Fact Sheet

Who is involved?

MIT Undergrads. The "**MIT Undergrads**" are Zack Anderson, RJ Ryan, and Alessandro Chiesa

Professor Ron Rivest. Professor Rivest was the MIT Undergrads' professor in the course at issue. Rivest specializes in cryptography; computer and network security; and algorithms. Professor Rivest is an inventor of the RSA public-key cryptosystem, and a founder of RSA Data Security. He is "well known and respected." ("**Rivest**"). Rivest gave the MIT Undergrads an "A" on the paper in which they purport to first disclose their "hack" of the AFC system.

DEFCON Conference. According to information published by DEFCON, the DEFCON Conference, which took place this year at the Riviera Hotel & Casino in Las Vegas, Nevada, is "one of the oldest continuous hacker conventions around, and also one of the largest." The Conference was anticipated to draw 5,000 to 7,000 attendees. According to organizers, "technology and hacking is the core" of the Conference. ("**DEFCON**").

EFF. The Electronic Frontier Foundation is representing the MIT Undergrads. The EFF (the "**EFF**"). The EFF describes itself as follows: "[w]hen our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990 — well before the Internet was on most people's radar — and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights. Blending the expertise of lawyers, policy analysts, activists, and technologists, EFF achieves significant victories on behalf of consumers and the general public. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 50,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public. EFF is a donor-funded nonprofit and depends on your support to continue successfully defending your digital rights. Litigation is particularly expensive; because two-thirds of our budget comes from individual donors, every contribution is critical to helping EFF fight —and win—more cases." *See http://www.eff.org/about*.

What data potentially relevant to AFC is involved?

There are three categories of data involved: (i) public domain materials ("**Universal Public Domain Materials**"); (ii) materials relevant to the AFC System that became public domain in connection with the DEFCON conference ("**Recent AFC-Related Public Domain Materials**"); and (iii) non-public materials that relate to the AFC system and potential security vulnerabilities ("**Non-Public Vulnerability Materials**").

The category "Recent AFC-Related Public Domain Materials" consists of two elements: (i) a four page Report that the MIT Undergrads provided to the MBTA on Friday evening, August 8, just before the initial TRO hearing was to take place (the "**Report**") and (ii) an 87 page powerpoint slide presentation that the MIT Undergrads' EFF counsel refused to provide to the

MBTA until 4:38 am on Saturday morning, August 9, hours before the 11:00 AM Court hearing (the "**Presentation**").

The sensitivity of the three overall categories of materials is as follows:

Category	**Illustrative Materials**	**Sensitivity**
Universal Public Domain Materials	Kostin Nohls, a UVA PhD candidate : information regarding weaknesses in MIFARE card Industry known-magnetic stripe vulnerabilities.	None.
Recent AFC-Related Public Domain Materials	DEFCON Presentation and 4 page Report	None/Low
Non-Public Vulnerability Materials	???	**High**, if the MIT Undergrads have such Materials.

Data on the Report and Presentation can be summarized as follows:

Document	**First Discloser**	**Recipients**	**Date of first receipt**
Presentation	MIT Undergrads	DEFCON Administrators	Approx. 7/5/2008
		DEFCON Attendees	Thursday, 8/7/2008
		MBTA	Saturday, 8/9/2008 at 4:38 AM
Report	MBTA	MBTA	Friday, 8/8/2008 at approx. 5:00 PM
		Court hearing attendees	Saturday 8/9/2008 at 11:00 AM
		Public (through docket)	Saturday 8/9/2008 at 2:00 PM

MBTA Discovers the Threat

On July 30, NXP, one of the MBTA's vendors (responsible for components of the Automated Fare Collection System) notified the MBTA of its discovery of an Internet posting that advertised a Presentation at the upcoming DEFCON "hacking" conference.

This presentation said, in relevant part:

> Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. … We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

The MBTA took this situation seriously, and proceeded to notify the MBTA Transit Police of this situation.

Meetings and Discussions with MIT

Professor Rivest called Joe Kelley on 7/31/2008 about having the MIT Undergrads meet with the MBTA. The MBTA informed him of the MIT Undergrads' giving a presentation regarding free subway rides at the DEFCON Conference, which he was unaware of. We also informed him that we had told the MBTA Police that this hacking conference was going on, and the Undergrads were talking about giving free rides. The MBTA Police then contacted Professor Rivest about a meeting with the Undergrads.

Sergeant Detective Richard Sullivan, of the Transit Police, worked with Professor Rivest to schedule this meeting. The meeting was originally scheduled for Monday, August 4, but Professor Rivest requested that the meeting move to Tuesday August 5 due to his travel schedule. However, Professor Rivest's secretary called and emailed Sgt. Sullivan to request that the meeting take place at MIT on August 4th

The following individuals attended this meeting: (i) Zack Anderson, (ii) RJ Russell; (iii) Professor Rivest; (iv) Jay Wilcoxson, MIT Associate General Counsel; (v) Transit Police Detective Sgt. Sullivan; and (vi) local FBI agent Jacob Shaver. The MIT Undergrads did promise Sgt. Sullivan that they would provide a report to him, but stated that it would not be available for a couple of weeks. On Tuesday, August 5, Sgt. Sullivan had several telephone/email communications with Prof. Rivest.

Non-Disclosure to the MBTA; Disclosure to DEFCON

It is our understanding that the MIT Undergrads did not disclose at the August 4 meeting (i) that they had already prepared the Presentation; or (ii) that they had already sent the Presentation to DEFCON for inclusion in a CD to be distributed to all attendees. Additionally, neither MIT Counsel Jay Wilcoxson nor Professor Rivest disclosed at the August 4 meeting or during the subsequent on phone conversations on August 5 that MIT knew of the Presentation.

After the August 4th meeting, Joe Kelley contacted Professor Rivest about (i) getting a copy of the Presentation, and (ii) having the Undergrads come in to talk about the information. Professor Rivest said he would work on this. The MIT Undergrads were unavailable because they were traveling to the DEFCON Conference, but promised to call the MBTA on Thursday and to provide the MBTA with a copy of the Presentation. When no call or information was forthcoming, the MBTA instructed its legal counsel to begin drafting Court papers, so that the MBTA could obtain this information. Joe Kelley via phone on Friday morning again asked Professor Rivest to obtain the presentation materials.

The MBTA filed the Court papers by the filing deadline of 4:00 on Friday. The MIT Undergrads sent then us the Report at approximately 4:30, after we had informed MIT that we were seeking a TRO. The materials we received consisted of the Report, which did not appear to constitute the presentation materials. At the hearing, Judge Woodlock requested a copy of this Report, which we were unable to provide due to our late receipt of this information, while we physically were in the Courthouse. The Judge ordered a hearing for Saturday morning at 11:00, and ordered us to file a supplemental declaration concerning the Report. The Supplemental Declaration we filed was from Scott Henderson of AFC concerning the Report. Outside legal counsel also filed a Declaration, informing the Court of the EFF's delaying tactics, and earlier disclosure of the Presentation.

The Presentation was not provided until after the court papers were filed. Even then, the MIT Undergrads (on the advice of their new EFF counsel) withheld it from the MBTA until 4:38 AM on Saturday morning. In order to review this Presentation before the hearing, outside counsel and MBTA counsel met with Scott Henderson from AFC, and personnel from S&B at Logan Airport at 6:00 am on Saturday, before these individuals' planned 8:00 flight to Las Vegas to attend the DEFCON Conference. This was to prepare for the 111:00 hearing that morning.

The delay in providing the Presentation and Report directly conflicts with the EFF's claims that the MIT Undergrads "always wanted to help."

The Core Principle of Responsible Disclosure

The MBTA seeks to preserve the integrity and security of its Fare Media System. The MBTA does not wish to detract from the MIT Undergrads First Amendment Rights or academic freedom. The principle that the MBTA seeks to enforce here is the principle of "**responsible disclosure**." Responsible disclosure is an industry accepted practice, which functions as follows: when an expert or other evaluator discovers a vulnerability (or a perceived vulnerability) in another vendor's system, he or she does NOT promptly go public with this information. Instead, he or she first (a) informs the vendor, and (b) gives the vendor a good opportunity to repair the vulnerability. Only then, after repair (and after confirmation that the vulnerability does indeed exist), does the expert go public, and receive appropriate credit for discovering the flaw.

The MBTA believes that responsible disclosure should apply here. The EFF Counsel disagrees, and claims that any restriction on the MIT Undergrads constitutes a violation of their First Amendment Rights.

Mediation Proposal

To implement a "responsible disclosure" solution, the MBTA has offered to mediate the parties' disputes -- without pre-conditions. As of 3:30 on Monday, August 11, 2008, despite two requests, the MIT Undergrads' EFF Counsel declined to agree to mediate.

Mediation is non-binding. A third party neutral, usually a respected former judge, or a experienced, mediation-specialized attorney, will preside over the sessions, which are completely confidential BY STATUTE. If a party does not like how mediation is progressing, he or she is free to "leave the table." The only drive that keeps parties at the table is a strong understanding of what they may face if they fail to reach a negotiated solution.

There is thus **no downside** to mediation for a party, provided that party is acting in good faith, and seriously seeks a solution, rather that a media blitz, or more "prank" material.

Motion to Modify TRO

On Monday, August 11, 2008 the MBTA filed a Motion to Modify the TRO to add the term "non-public" to the Order. The Court had issued Findings and Rulings orally from the bench during the emergency hearing on Saturday, and in the context of these Findings and Rulings the MBTA believed the TRO was clear. The EFF's press statements over the weekend, however, coupled with the EFF's failure to respond to the proposed mediation, in the MBTA's view jeopardized this clarity. The MBTA, accordingly, moved to restrict the TRO, as a further effort to demonstrate to the MIT Undergrads and their EFF counsel that the MBTA's goal in this case is simply **responsible disclosure**, and no more.

5533212_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08 CA 11364 GAO RBC

COMPLAINT

Introduction

1. The plaintiff, Massachusetts Bay Transportation Authority ("MBTA") brings this action against three undergraduate students at the Massachusetts Institute of Technology ("MIT"), and against MIT.

2. As demonstrated below, the undergraduate students, Zack Anderson, RJ Ryan, and Alessandro Chiesa (collectively the "MIT Undergrads") (i) claim to have circumvented the security features of the MBTA's computerized CharlieTicket and CharlieCard fare media systems; (ii) publicly offered "free subway rides for life" to interested parties over the Internet; and (iii) plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving demonstrations at the DEFCON hackers convention this Sunday, August 10, in Las Vegas.

3. Despite the MBTA's requests, MIT has been unwilling to set limits on the MIT Undergrads' activities.

4. The MIT Undergrads have declined to provide the MBTA or its system vendors with information concerning the claimed security flaws in the system.

5. If what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws – before the MBTA and its system vendors have an opportunity to correct the flaws – will cause significant damage to the MBTA's transit system.

Parties

6. The plaintiff, Massachusetts Bay Transportation Authority ("MBTA") is a legislatively created entity, under Massachusetts General Laws, Chapter 161A, with a principle place of business at the State Transportation Building, 10 Park Plaza, Boston, MA 02116.

7. The defendant, Zack Anderson ("Anderson"), upon information and belief, is an electrical engineering and computer science undergraduate studying at MIT, with a residential address of East Campus, 3 Ames St., Hall 2W, Room W210, Cambridge, Massachusetts 02142.

8. The defendant, RJ Ryan ("Ryan"), upon information and belief, is an undergraduate researcher in computer security at MIT, with a residential address of East Campus, 3 Ames St., Hall 2W, Room W214 Cambridge, Massachusetts 02142.

9. The defendant, Alessandro Chiesa ("Chiesa") upon information and belief, is a junior majoring in Theoretical Mathematics and Electrical Engineering and Computer Science at MIT, with a residential address of East Campus, 3 Ames St., Hall 4W, Room 409, Cambridge, Massachusetts 02142.

10. The defendant, Massachusetts Institute of Technology ("MIT"), is a Massachusetts non-profit educational institution having a usual place of business at 77 Massachusetts Avenue, Cambridge, Massachusetts 02139.

11. The term "MIT Undergrads" is used to refer to Anderson, Ryan, and Chiesa.

Jurisdiction And Venue

12. This Court has subject matter jurisdiction over the MBTA's claims under the provisions of 18 U.S.C. §1030(g) and 28 U.S.C. § 1331.

13. This Court has supplemental jurisdiction over MBTA's state, statutory and common law claims under 28 U.S. C. § 1367(a), because these claims are so related to the federal claims in this action that they form part of the same case or controversy.

14. Venue is appropriate in this District pursuant to 28 U.S.C. §§ 1391(b).

Factual Allegations Common To All Counts

The MBTA's Transit System

15. The MBTA is the nation's 5th largest mass transit system. The MBTA serves a population of 4,667,555 (based on the 2000 census) in 175 cities and towns with an area of 3,244 square miles.

16. To provide these transit services, the MBTA maintains 183 bus routes, 2 of which are Bus Rapid Transit lines, 3 rapid transit lines, 5 streetcar (Central Subway/Green Line) routes, 4 trackless trolley lines and 13 commuter rail routes. The MBTA's transit equipment includes of 927 diesel and CNG buses, 32 dual mode buses, 28 ETB's (electric trolley buses), 408 heavy rail vehicles, 200 light rail vehicles, 10 PCC's streetcars, 83 commuter rail locomotives, 410 commuter rail coaches and 298 MBTA-owned specially equipped vans and sedans, and an additional 235 contractor-supplied specially equipped vans and sedans.

17. The average weekday ridership for the entire system is approximately 1.4 million passenger trips. The approximate average weekday revenue of the MBTA is $700,000.00.

18. The MBTA directly services Rhode Island as well as Massachusetts, via its commuter rail service.

19. The MBTA is the recipient of significant funding from the United States Department of Transportation, through the Urban Mass Transportation Administration ("UMTA"). Since the mid-1960's, the MBTA has received over $3.5 billion in such funding, for its capital improvement projects and its yearly operating programs.

20. In addition to this funding, the MBTA receives funds from the Department of Homeland Security, to implement various security, anti-terrorism, and other security initiatives. For example, in 2007 the MBTA received $4 million from the Department of Homeland Security and the Federal Transit Administration, for use in emergency communications initiatives.

The MBTA Undertakes Considerable Improvements To The System, Including The Introduction of An Automated Fare Collection System

21. The MBTA has recently undertaken significant system improvements. A central improvement consisted of the procurement and installation of an automated fare collection system (the "Automated Fare Collection System" or "AFC System"). The Automated Fare Collection System replaces the MBTA's old "token" system, and is comprised of the following general, high-level system components:

(a) Computerized fare gates in each station, that read fare media and permit (or deny) users access to MBTA transit services ("Fare Gates");

(b) Computerized fare vending machines in each station (and elsewhere), that accept payment and issue or load value to fare media ("Fare Vending Machines");

(c) Fare media that communicate with the Fare Gates and the Fare Vending Machines to store and transfer "value" – the equivalent of the old token -- and that allow paying patrons to access the MBTA's transit services ("Fare Media");

(d) A central computing facility that controls and exchanges data with Fare Gates, with Fare Vending Machines, with servers and other devices connected to the AFC System network, with remote retail sales outlets, and with dial-in and other connections to the AFC System; and

(e) Complex sets of software applications that are resident on servers at the central computing facility, on the Fare Gates, on the Fare Vending Machines, and on certain Fare Media. These software applications (among other tasks) manage and control the issuance of fare media, payments for transit services, rate schedules, ridership volumes, and a wide range of other tasks and information.

22. The AFC System, accordingly, is highly automated, and is comprised of high speed data processing devices that perform logical, arithmetic, and storage functions.

23. The procurement and installation of the Automated Fare Collection System cost in excess of $180 million.

Through Outside Vendors, The MBTA Implements Its "CharlieCard pass" and "CharlieTicket pass" System

24. Fare Media are broken into two categories: (i) so-called "CharlieCard" passes and (ii) so-called "CharlieTicket passes". These Fare Media each employ slightly different technology.

25. A CharlieTicket pass uses a so-called a "magnetic stripe" or "magstrip" to convey information to the Automated Fare Collection System. CharlieTicket passes are paper-based media, and to employ a CharlieTicket pass, a user brings the Ticket's magstrip into physical contact with a reader in fare gate, by "swiping" the Ticket past the designated reading head. A user can "store value" on his or her CharlieTicket pass, or can store a monthly pass (or other pass) on the CharlieTicket pass.

26. CharlieCard passes, in contrast, are plastic media, and are so-called "smart cards." Each CharlieCard pass contains an integrated circuit – a computer chip – that processes information. This chip allows a user to store value for single or multiple rides and/or a T-pass. In addition, the smart card features of the CharlieCard pass allow for online account management, and other services that are not compatible with the CharlieTicket pass technology.

27. The user loads a CharlieTicket pass or a CharlieCard pass with value or a T-Pass using cash, credit or debit cards, at in-station fare vending machines, at retail sales terminals, at MBTA ticket offices, or online via the MBTA's website at www.mbta.com.

The CharlieCard Pass Becomes Centrally Important To The MBTA's Overall Transit System

28. The MBTA has implemented both CharlieTicket passes and CharlieCard passes in its Automated Fare Collection System. CharlieCard passes, for example, began to be used in January 2007.

29. The CharlieCard has become the preferred fare media of MBTA riders.

30. Currently, over eighty percent (68%) of riders use the CharlieCard pass, with ninety percent (90%) receiving the best value by using monthly magnetic stripe cards and CharlieCards. Accordingly, CharlieCards account for approximately $475,000.00 per weekday in revenues.

31. The CharlieCard is employed in the MBTA's corporate pass program, whereby employers provide MBTA fare media to their employees. As of the spring of 2008, this program had grown to include over 1,300 companies with offices in the Boston area.

32. Although CharlieCards are not currently employed on the MBTA's commuter rail system, a pilot program for such use is scheduled to commence in 2009.

The MBTA Learns That The MIT Undergrads (i) Purport To Have Discovered Security Flaws In The MBTA's CharlieTicket And CharlieCard Systems And (ii) Have Publicly Promised To Provide Others With "Free Subway Rides For Life"

33. On July 30, a vendor responsible for components of the Automated Fare Collection System notified the MBTA of its discovery of an Internet posting that advertised a presentation at the upcoming DEFCON 16 "hacking" conference.

34. The Internet posting read, in relevant part, as follows:

> Anatomy of a Subway Hack: Breaking Crypto RFID's and Magstripes of Ticketing Systems
>
> Zack Anderson Student, MIT
> RJ Ryan Student, MIT
> Alessandro Chiesa Student, MIT
>
> Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

35. The three MIT students identified in this announcement (for convenience, the "Initial Announcement") are the MIT Undergrads who are defendants in this matter. .

36. This Initial Announcement raised a number of concerns.

37. First, the Initial Announcement specifically targets the MBTA and its computerized Fare Media systems. The Announcement reads, for example: "[w]e focus *on the Boston T subway*, and show how we reverse engineered the data on *magstripe card* [apparently referring to the CharlieTicket], we present several attacks to completely break *the CharlieCard.*" (emphasis added).

38. Second, the Initial Announcement suggests that the MIT Undergrads have wholly compromised the CharlieCard system. The Announcement states, for example, that " we present several attacks to *completely break* the CharlieCard." (emphasis added)

39. Third, in the Initial Announcement, the MIT Undergrads promise to provide to attendees at their presentation "*free subway rides for life.*" (emphasis added).

40. Fourth, the Initial Announcement advertises the connection between the authors and MIT. This use of the MIT name suggests an endorsement or other approval of the presentation.

41. Finally, the MIT Undergrads claim that they will provide software tools to allow others to "break" the MBTA's CharlieCard and CharlieTicket system. Specifically, the Initial Announcement states that "[w]e will release *several open source tools* we wrote to perform these attacks. With live demos, *we will demonstrate how we broke these systems*."

42. Accordingly, the MIT Undergrads promised, in the Initial Announcement, to instruct and enable others to "break" the MBTA's computerized Fare Media system.

43. The Initial Announcement presented concerns, in addition, due to the forum the MIT Undergrads had chosen. The Announcement indicated that the MIT Undergrads would present this information at DEFCON 16.

44. According to information published by DEFCON, the DEFCON Conference, taking place this year at the Riviera Hotel & Casino in Las Vegas, Nevada, is "one of the oldest continuous hacker conventions around, and also one of the largest. *See* https://www.defcon.org/html/links/dc-faq/dc-faq.html.

45. Organizers state that the Conference is anticipated to draw 5,000 to 7,000 attendees.

46. According to organizers, "technology and hacking is the core" of the Conference. *See id.*

47. The 2008 DEFCON Conference begins on Friday, August 8, and the MIT Undergrads are scheduled to give their "The Anatomy of a Subway Hack" presentation at 1:00 on Sunday, August 10, 2008.

The MBTA Contacts The MIT Undergrads, Through Law Enforcement, And Communicates Its Concerns To Them, To Professor Rivest, And To MIT

48. After discovering the Initial Announcement and the threat it posed, the MBTA and law enforcement promptly arranged a meeting with the MIT Undergrads to discuss their intentions, and to present the MBTA's concerns.

49. This meeting took place on August 5, 2008. The MIT Undergrads attended, as did Rivest and MIT counsel.

50. The MIT Undergrads stated that they did not intend to harm the MBTA.

51. Despite this statement, and the MBTA's requests, the defendants have not provided the MBTA with a copy of the materials the MIT Undergrads plan to present.

52. After this August 5 meeting, the Initial Announcement was revised to read in relevant part as follows (for convenience, the "Revised Announcement"):

> The Anatomy of a Subway Hack:
> Breaking Crypto RFID's and Magstripes of Ticketing Systems
>
> Zack Anderson Student, MIT
> RJ Ryan Student, MIT
> Alessandro Chiesa Student, MIT
>
> In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

53. A comparison of (a) the Initial Announcement to (b) the Revised Announcement reveals the following changes (underlines signify additions, strike-outs signify deletions from the):

> ~~Want free subway rides for life?~~ In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We ~~go over social engineering attacks we executed on employees~~survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote ~~to perform~~in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

54. The Revised Announcement does not remove the MBTA's concerns.

55. Like the Initial Announcement, the Revised Announcement (i) targets the MBTA and its specific Fare Media systems by name; (ii) claims that the CharlieCard system has been "completely" broken by the authors' attacks; (iii) continues to suggest endorsement and approval by MIT; and (iv) continues to promise the release of software tools and demonstrations to allow others to duplicate the attacks.

56. Disclosure of this information – if what the MIT Undergrads claim is true – will significantly compromise the CharlieCard and CharlieTicket systems. This in turn will harm the overall functioning of the MBTA's transit services.

57. The MBTA does not demand that the MIT Undergrads forever refrain from disclosing information that will compromise or threaten to compromise the security of its Fare Media systems. Instead, under industry-accepted principles of "responsible disclosure", the

MBTA demands that the MIT Undergrads refrain from such disclosure until the MBTA's system vendors have remedied the security flaw the MIT Undergrads have identified.

The Role of MIT

58. Professor Rivest specializes in cryptography; computer and network security; and algorithms. Professor Rivest, on information and belief, is an inventor of the RSA public-key cryptosystem, and a founder of RSA Data Security.

59. Upon information and belief, Rivest was aware of, and supervised the MIT Undergrads in their work attacking and "breaking" the MBTA's Fare Media system.

60. MIT publishes explicit policies prohibiting attacks on the security and integrity of MIT systems. For example, the MITnet Rules of Use provide as follows:

> Don't violate the intended use of MITnet.
> The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:
>
> Don't try to interfere with or alter the integrity of the system at large, by doing any of the following:
> ...
> attempting to capture or crack passwords or encryption
> destroying or altering data or programs belonging to other users
> ...
> Appropriate use of MITnet resources includes maintaining the security of the system. *See* http://web.mit.edu/olh/Rules/#rule_1

61. Rivest and MIT are bound to respect and enforce these rules with respect to MIT's own network security. Upon information and belief, the MIT Undergrads have been permitted to disregard these rules with respect to key systems in the Commonwealth, such as the MBTA's computerized Fare Media systems.

62. The defendants' actions and omissions have caused the MBTA to expend substantial funds to respond to the threat the defendants have posed. Due to the defendants'

failure to provide information reasonably requested by the MBTA, the MBTA is unaware currently of the level of improper ridership due to the defendants' wrongdoing. This wrongdoing, if allowed to continue -- and if what the MIT Undergrads claim is true -- threatens to inflict significant additional damage, unless the requested relief is granted.

Count I
Violation Of The Computer Fraud And Abuse Act: 18 U.S.C. §1030

63. MBTA restates and re-alleges the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

64. A CharlieTicket standing alone constitutes a "computer" within the meaning of 18 U.S.C. §1030(e)(1).

65. A CharlieCard standing alone constitutes a "computer" within the meaning of 18 U.S.C. §1030(e)(1).

66. The system for storing value and processing payments via CharlieTickets and CharlieCards, including the Fare Gate and the Fare Vending Machine, constitutes a "computer" within the meaning of 18 U.S.C. §1030(e)(1).

67. The "computers" identified above were used in interstate commerce or communication and were protected computers within the meaning of 18 U.S.C. §1030(e)(2)(B).

68. The MIT Undergrads knowingly caused the transmission of a program, information, code, or command targeted at MBTA protected computers.

69. As a result of such conduct, the MIT Undergrads intentionally caused damage without authorization, to these protected computers.

70. The MIT Undergrads intentionally accessed MBTA protected computers without authorization, and as a result of such conduct, have caused damage.

71. The damage caused includes a loss aggregating substantially more than the $5,000 amount required under 18 U.S.C. §1030(a)(5)(B)(i).

72. In addition, the damage constitutes a threat to public health or safety, within the meaning of 18 U.S.C. §1030(a)(5)(B)(iv).

73. The damage, moreover, affects a computer system used by a government entity for national security purposes, within the meaning of 18 U.S.C. §1030(a)(5)(B)(v).

74. The MBTA has been damaged, and has suffered losses, due to these past wrongs by the defendants.

75. More importantly, the MBTA will suffer irreparable harm if the MIT Undergrads are allowed to give their presentation at DEFCON without limitations, based on the Initial and Revised Announcements.

Count II
Liability for Attempt under 18 U.S.C. §1030

76. MBTA restates and re-alleges the allegations contained in Paragraphs 1 through 75 as if fully set forth herein.

77. The conduct described above, if it does not rise to the level of a direct violation of 18 U.S.C. §1030, at a minimum constitutes an illegal attempt, actionable under the statute.

78. In light of this attempt, the MBTA will suffer irreparable harm if the MIT Undergrads are allowed to give their presentation at DEFCON without limitations, based on the Initial and Revised Announcements.

Count III
Conversion

79. MBTA restates and re-alleges all of the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

80. MBTA owns and has immediate right to possession of fares from passengers traveling on the MBTA lines.

81. The MIT Undergrads exerted dominion over MBTA's property by traveling on the MBTA lines without paying fares.

82. The MIT Undergrads have no right to enjoy the MBTA's transit services without paying requisite fares.

83. By engaging in the conduct described above, the MIT Undergrads have converted the MBTA's property.

84. Upon information and belief, the MIT Undergrads have instructed others in converting, have provided the means to allow others to convert, or have otherwise facilitated the conversion by others of the MBTA's property.

85. As a result, the MBTA has suffered damages.

Count IV
Trespass To Chattels

86. MBTA restates and re-alleges all of the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

87. The MBTA consented to the MIT Undergrads' use of, and access to, its computerized Fare Media systems, including CharlieTickets and CharlieCards.

88. By the conduct described herein, these defendants knowingly and intentionally exceeded that consent, and have trespassed on the MBTA's computing facilities.

89. The MBTA has been damaged as a result of these defendants' trespass. .

Count V
For Imposition Of A Constructive Trust Upon Illegal Profits

90. MBTA restates and re-alleges all of the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

91. The MIT Undergrads' conduct is wrongful.

92. By virtue of these defendants' wrongful conduct, they have illegally received or will illegally receive money and profits that rightfully belong to MBTA, in the form of lost transit fares.

93. MBTA is entitled to have the MIT Undergrads hold the money and profits that they illegally received as constructive trustee for the benefit of MBTA.

Count VI
Negligent Supervision Against MIT

94. The MBTA restates and re-alleges all of the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

95. Based on MIT's policies, industry practice, and other sources, MIT understood the importance of network integrity and security.

96. MIT owed a duty to the MBTA to properly supervise and guide the MIT Undergraduates.

97. This duty included a duty to instruct and guide the MIT Undergraduates to responsibly disclose information concerning perceived security flaws.

98. MIT knew or should have know of the MIT Undergrads' activities evidenced by the Initial and Revised Announcements. MIT knew or should have know of the MIT Undergrad's decision to decline to provide the MBTA with any written information concerning their presentation.

99. Harm to the MBTA was foreseeable by MIT in the event MIT failed to fulfill these duties.

100. MIT breached these duties.

101. This breach has caused the MBTA significant harm.

COUNT VII
Violations of M.G.L. c. 93, §11

102. The MBTA restates and re-alleges all of the allegations contained in Paragraphs 1 through 62 as if fully set forth herein.

103. Each of the defendants is engaged in trade or commerce in the Commonwealth of Massachusetts.

104. The actions of the defendants, as aforesaid, constitute unfair and deceptive acts and practices in violation of G.L. c. 93A, §11.

Requested Relief

WHEREFORE, the MBTA respectfully requests that the Court:

1. Grant it Judgment in an amount to be set at trial on Counts I through VI;

2. Grant it Judgment in an amount to be set at trial on Count VII, trebled, plus costs and attorneys' fees;

3. Grant preliminary injunctive relief, pursuant to 18 U.S.C. §1030(g) and extending through DEFCON and until the MBTA's vendors have had sufficient time to correct defects, enjoining the MIT Undergrads:

(a) From offering to provide software tools or demonstrations to allow others to duplicate the attacks referenced in the Initial and Revised Announcements;

(b) From providing information or materials that would assist another in any material way to circumvent the security of the Fare Media system;

(c) From publicly stating or indicating that the security or integrity of the CharlieCard pass, the CharlieTicket pass, or the MBTA's Fare Media systems has been compromised;

(d) From further circulating the Initial Announcement and Revised Announcement, and from declining to promptly remove access to these Announcements;

(e) From suggesting that MIT endorses or approves of the activities outlined in the Initial or Revised Announcement;

(f) From suggesting they can provide or assist others in obtaining "free subway rides" on the MBTA's transit system; and

(g) From declining to provide the MBTA and its vendors with information sufficient to replicate, test, and repair the purported security flaws in the Fare Media system.

4. Enter an order declaring that the MIT Undergrads hold in trust, as constructive trustees for the benefit of MBTA, any revenues obtained from the use of compromised Fare Media;

5. Award the MBTA its costs, including attorneys' fees; and

6. Grant the MBTA such other relief as is just and proper.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO #667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building, 7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August __, 2008
Boston, Massachusetts

5526720_v3

JS 44 (Rev 12/07)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS

Massachusetts Bay Transportation Authority

(b) County of Residence of First Listed Plaintiff Suffolk
(EXCEPT IN U.S PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)
Ieuan Mahony, Esquire, Holland & Knight, LLP 10 St. James Avenue, Boston, MA 02106

DEFENDANTS

Zack Anderson, et al

County of Residence of First Listed Defendant Middlesex
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED

Attorneys (If Known)

08 CA 11364 GAO

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury

PERSONAL INJURY
- ☐ 362 Personal Injury - Med. Malpractice
- ☐ 365 Personal Injury - Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 444 Welfare
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence

Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE/PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R. & Truck
- ☐ 650 Airline Regs.
- ☐ 660 Occupational Safety/Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt.Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus - Alien Detainee
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Information Act
- ☐ 900Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing **(Do not cite jurisdictional statutes unless diversity)**:
18 U.S.C. § 1030

Brief description of cause.
Defendants have breached or threaten to breach computer security

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☐ Yes ☐ No

VIII. RELATED CASE(S) IF ANY (See instructions). JUDGE _____ DOCKET NUMBER _____

DATE
8-8-08

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

1. Title of case (name of first party on each side only) Massachusetts Bay Transportation Authority v. Zack Anderson, et al

2. Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).

☐	I.	160, 410, 470, 535, R.23, REGARDLESS OF NATURE OF SUIT.	
☒	II.	195, 196, 368, 400, 440, 441-446, 540, 550, 555, 625, 710, 720, 730, 740, 790, 791, 820*, 830*, 840*, 850, 890, 892-894, 895, 950.	*Also complete AO 120 or AO 121 for patent, trademark or copyright cases
☐	III.	110, 120, 130, 140, 151, 190, 210, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 370, 371, 380, 365, 450, 891.	
☐	IV.	220, 422, 423, 430, 460, 462, 463, 465, 480, 490, 510, 530, 610, 620, 630, 640, 650, 660, 690, 810, 861-865, 870, 871, 875, 900.	
☐	V.	150, 152, 153.	

3. Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.

4. Has a prior action between the same parties and based on the same claim ever been filed in this court?
YES ☐ NO ☒

5. Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)
YES ☐ NO ☒

If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?
YES ☐ NO ☐

6. Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?
YES ☐ NO ☒

7. Do all of the parties in this action, excluding governmental agencies of the united states and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).
YES ☒ NO ☐

A. If yes, in which division do all of the non-governmental parties reside?
Eastern Division ☒ Central Division ☐ Western Division ☐

B. If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?
Eastern Division ☐ Central Division ☐ Western Division ☐

8. If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)
YES ☐ NO ☐

(PLEASE TYPE OR PRINT)

ATTORNEY'S NAME Ieuan Mahony
ADDRESS Holland & Knight, LLP, 10 St. James Avenue, Boston, MA 02116
TELEPHONE NO. 617-573-2700

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, SUSAN HOCKFIELD, PHILLIP L. CLAY, and the MIT CORPORATION

Defendants

Civil Action No. _____

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER

Introduction

The plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), seeks a temporary restraining order enjoining the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (collectively the "MIT Undergrads") (a) from exploiting security flaws they claim to have discovered in the MBTA's Fare Media System; and (b) from publicizing these flaws in the presentation they are scheduled to give two days from today, on Sunday August 10 at the DEFCON hackers convention in Las Vegas.

Facts

The MBTA's automated fare collection system (the "AFC System" or the "Automated Fare Collection System") relies on so-called CharlieCard passes and CharlieTicket passes for the payment of MBTA fares (among other purposes). Declaration of Joseph Kelley ("Kelley Decl.") ¶¶13-16. The fare media system (the "Fare Media System") contains security features, designed

to prevent unauthorized personnel from manipulating the system, and obtaining free MBTA transit services or causing other harm. Declaration of G. Foster ("Foster Decl.") ¶¶4-5.

The MIT Undergrads (i) claim to have circumvented the security features of the MBTA's computerized CharlieTicket and CharlieCard fare media systems; (ii) publicly offered "free subway rides for life" to interested parties over the Internet; and (iii) plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving demonstrations at the DEFCON hackers convention this Sunday, August 10, in Las Vegas. Foster Decl. ¶¶10-23.

Despite the MBTA's requests, the MIT Undergrads have declined to provide the MBTA or its system vendors with information concerning the claimed security flaws in the system. Kelley Decl. ¶¶23-26.

If what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws – before the MBTA and its system vendors have an opportunity to correct the flaw – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25.

Argument

I. The MBTA Is Entitled To Immediate Relief

The MBTA is entitled to a temporary restraining order because it has shown: (1) a likelihood that it will prevail on the merits; (2) irreparable harm unless the restraining order is issued; (3) greater harm to it than the adversary's harm resulting from issuance of a temporary restraining order; and (4) the absence of an adverse impact on the public interest. *Esso Standard Oil Co. (Puerto Rico) v. Monroig-Zayas,* 445 F.3d 13, 18 (1st Cir.2006); *McGuire v. Reilly*, 260 F.3d 36. 42 (1st Cir. 2001). Injunctive relief should issue to "prevent a real threat of harm." *Matos ex rel. Matos v. Clinton School District*, 367 F.3d 68, 73 (1st Cir. 2004). As demonstrated

below, if the MIT Undergrads truly have broken the security of the MBTA's Fare Media system, the MBTA will suffer immediate, real harm.

II. The MBTA Has A High Likelihood Of Success On Its Claims Under The Computer Fraud And Abuse Act.

The MBTA is likely to success on the merits of its claims under 18 U.S.C. §1030, the Computer Fraud and Abuse Act (the "CFAA"). First, the systems for storing value and processing payments via CharlieTickets and CharlieCards, including the Fare Gate and the Fare Vending Machine, constitute "computers" within the meaning of 18 U.S.C. §1030(e)(1). These "computers," moreover, are used in interstate commerce or communication due, for example, to the MBTA's services in Rhode Island and Massachusetts. *See* Kelley Decl. ¶7. Accordingly, these are protected computers within the meaning of 18 U.S.C. §1030(e)(2)(B).

Second, based on the Initial and Revised Announcements, it appears the MIT Undergrads knowingly caused the transmission of a program, information, code, or command targeted at MBTA protected computers and, as a result of such conduct, the MIT Undergrads intentionally caused damage without authorization, to these protected computers. Moreover, the MIT Undergrads intentionally accessed MBTA protected computers without authorization, and as a result of such conduct, have caused damage. These damages include a loss aggregating substantially more than the $5,000 amount required under 18 U.S.C. §1030(a)(5)(B)(i), particularly in light of the volume of traffic covered by the CharlieCard and CharlieTicket passes, and the costs of the overall Automated Fare Collection System that relies on the CharlieCard and CharlieTicket passes. *See* Kelley Decl. ¶¶12, 19.

Finally, the damage constitutes a threat to public health or safety, within the meaning of 18 U.S.C. §1030(a)(5)(B)(iv), and also affects a computer system used by a government entity for national security purposes, within the meaning of 18 U.S.C. §1030(a)(5)(B)(v), due to the

role of the MBTA in Homeland Security efforts, and transit services generally. *See* Kelley Decl. ¶¶6, 8-9.

III. Irreparable Harm

"Irreparable injury' in the preliminary injunction context means an injury that cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005). The loss of a trade secret is generally found to constitute irreparable harm. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F.Supp.2d 23, 32 (D.Mass. 2004). That is in recognition of the fact that, "once the trade secret is lost, it is gone forever." *Id. (citing FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir.1984)).

Here, if what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws in the Fare Media System – before the MBTA and its system vendors have an opportunity to correct the flaws – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25. The requested relief, therefore, is necessary to preserve the status quo until a full hearing. *See CMM Cable Rep., Inc. v. Ocean Coast Properties, Inc.*, 48 F.3d 618, 620 (1st Cir.1995)

IV. Reliance On Industry-Recognized "Responsible Disclosure" Practices, There Will Be No Cognizable Harm To The MIT Undergrads.

The temporary halt on the MIT Undergrad's disclosures will not create cognizable harm to the defendants. This is particularly true in light of industry practices, and the so-called "responsible disclosure" doctrine.

The term "responsible disclosure" refers to the method of disclosing a technological vulnerability to the developer so that the developer can fix the vulnerability before the general

public finds out about it. Making a disclosure of the vulnerability to the developer is necessary to obtain a fix. If the discoverer discloses the vulnerability to a broader audience, hackers and other malicious users may be able to exploit the vulnerability before the developer implements a fix. The term "responsible disclosure" is generally used to refer to the process by which (i) the discoverer discloses the vulnerability, (ii) the vulnerability is corrected, and (iii) hackers are prevented from exploiting the vulnerability in the interim.

Microsoft defines the term "responsible disclosure" as follows:

> In a responsible disclosure scenario, the researcher who discovers the vulnerability reports the findings directly to the appropriate vendor, providing a reasonable amount of time for the vendor to investigate, create, and test the necessary update. Only when the update is made available are actual details of the vulnerability made public, with due credit given to the original reporter. (emphasis added).[1]

Google states that "responsible disclosure" is an "industry best practice." Specifically, Google defines the term, and elaborates on the term in its "Security and Product Safety" as follows:

> This process of notifying a vendor before publicly releasing information is an industry-standard best practice known as responsible disclosure. Responsible disclosure is important to the ecology of the Internet. It allows companies like Google to keep users safe by fixing vulnerabilities and resolving security concerns before they are brought to the attention of the bad guys. We strongly encourage anyone who is interested in researching and reporting security issues to observe the simple courtesies and protocols of responsible disclosure. (emphasis added).[2]

---

[1] See Malware Revolution: A Change in Target (published: March 14, 2007), Microsoft Website, located at http://www.microsoft.com/technet/community/columns/secmgmt/sm0307.mspx .

[2] Google Security and Product Safety, located at http://www.google.com/corporate/security.html; see, Symantec Responsible Disclosure Policy (January 2006) (listing 5 steps Symantec commits to follow as part of its "responsible disclosure" procedures), located at http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf.

A number of industry groups have proposed various "uniform" policies relating to these disclosure issues.[3]

V. The Requested Relief Furthers The Public Interest.

The final factor is the public interest. This factor requires the Court to "inquire whether there are public interests beyond the private interests of the litigants that would be affected by the issuance or denial of injunctive relief." *Friends of Magurrewock, Inc. v. U.S. Army Corps of Engineers*, 498 F.Supp.2d 365, 379 (D.Me.,2007) (quoting *Everett J. Prescott, Inc. v. Ross*, 383 F.Supp.2d 180, 193 (D.Me.2005))

The MBTA provides approximately 1.4 million passenger trips per weekday.[4] The Fare Media System threatened by the MIT Undergrads' conduct governs the majority of this system. It is strongly in the public interest to protect this system in the manner requested, particularly in light of the steps the MBTA has taken to avoid the necessity of requesting relief from this Court.

[3] See, e.g., Rain Forest Puppy - Full Disclosure Policy (RFPolicy) v2.0. located at http://www.wiretrip.net/rfp/policy.html; Organization for Internet Safety Guidelines for Security Vulnerability Reporting and Response, V2.0 (2004) located at http://www.oisafety.org/index.html.

[4] Kelley Decl. ¶6.

Conclusion

THEREFORE, the plaintiff respectfully requests that this Court enter the attached proposed Order.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

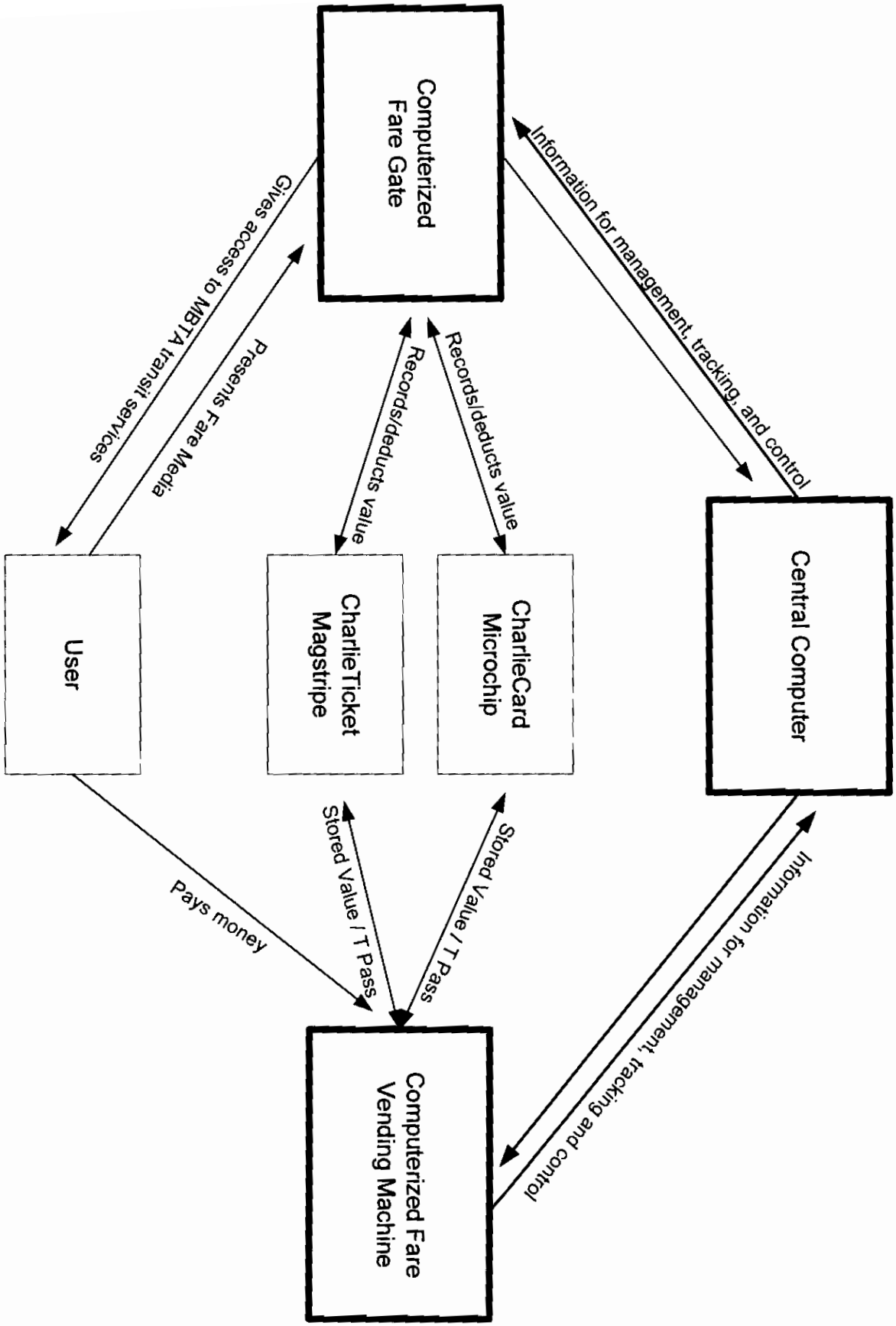
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August __, 2008
Boston, Massachusetts

5530567_v1

Schematic Illustrating the MBTA's Fare Media System



UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, SUSAN HOCKFIELD, PHILLIP L. CLAY, and the MIT CORPORATION

Defendants

Civil Action No. _____

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER

Introduction

The plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), seeks a temporary restraining order enjoining the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (collectively the "MIT Undergrads") (a) from exploiting security flaws they claim to have discovered in the MBTA's Fare Media System; and (b) from publicizing these flaws in the presentation they are scheduled to give two days from today, on Sunday August 10 at the DEFCON hackers convention in Las Vegas.

Facts

The MBTA's automated fare collection system (the "AFC System" or the "Automated Fare Collection System") relies on so-called CharlieCard passes and CharlieTicket passes for the payment of MBTA fares (among other purposes). Declaration of Joseph Kelley ("Kelley Decl.") ¶¶13-16. The fare media system (the "Fare Media System") contains security features, designed

to prevent unauthorized personnel from manipulating the system, and obtaining free MBTA transit services or causing other harm. Declaration of G. Foster ("Foster Decl.") ¶¶4-5.

The MIT Undergrads (i) claim to have circumvented the security features of the MBTA's computerized CharlieTicket and CharlieCard fare media systems; (ii) publicly offered "free subway rides for life" to interested parties over the Internet; and (iii) plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving demonstrations at the DEFCON hackers convention this Sunday, August 10, in Las Vegas. Foster Decl. ¶¶10-23.

Despite the MBTA's requests, the MIT Undergrads have declined to provide the MBTA or its system vendors with information concerning the claimed security flaws in the system. Kelley Decl. ¶¶23-26.

If what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws – before the MBTA and its system vendors have an opportunity to correct the flaw – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25.

Argument

I. The MBTA Is Entitled To Immediate Relief

The MBTA is entitled to a temporary restraining order because it has shown: (1) a likelihood that it will prevail on the merits; (2) irreparable harm unless the restraining order is issued; (3) greater harm to it than the adversary's harm resulting from issuance of a temporary restraining order; and (4) the absence of an adverse impact on the public interest. *Esso Standard Oil Co. (Puerto Rico) v. Monroig-Zayas,* 445 F.3d 13, 18 (1st Cir.2006); *McGuire v. Reilly*, 260 F.3d 36. 42 (1st Cir. 2001). Injunctive relief should issue to "prevent a real threat of harm." *Matos ex rel. Matos v. Clinton School District*, 367 F.3d 68, 73 (1st Cir. 2004). As demonstrated

below, if the MIT Undergrads truly have broken the security of the MBTA's Fare Media system, the MBTA will suffer immediate, real harm.

II. The MBTA Has A High Likelihood Of Success On Its Claims Under The Computer Fraud And Abuse Act.

The MBTA is likely to success on the merits of its claims under 18 U.S.C. §1030, the Computer Fraud and Abuse Act (the "CFAA"). First, the systems for storing value and processing payments via CharlieTickets and CharlieCards, including the Fare Gate and the Fare Vending Machine, constitute "computers" within the meaning of 18 U.S.C. §1030(e)(1). These "computers," moreover, are used in interstate commerce or communication due, for example, to the MBTA's services in Rhode Island and Massachusetts. *See* Kelley Decl. ¶7. Accordingly, these are protected computers within the meaning of 18 U.S.C. §1030(e)(2)(B).

Second, based on the Initial and Revised Announcements, it appears the MIT Undergrads knowingly caused the transmission of a program, information, code, or command targeted at MBTA protected computers and, as a result of such conduct, the MIT Undergrads intentionally caused damage without authorization, to these protected computers. Moreover, the MIT Undergrads intentionally accessed MBTA protected computers without authorization, and as a result of such conduct, have caused damage. These damages include a loss aggregating substantially more than the $5,000 amount required under 18 U.S.C. §1030(a)(5)(B)(i), particularly in light of the volume of traffic covered by the CharlieCard and CharlieTicket passes, and the costs of the overall Automated Fare Collection System that relies on the CharlieCard and CharlieTicket passes. *See* Kelley Decl. ¶¶12, 19.

Finally, the damage constitutes a threat to public health or safety, within the meaning of 18 U.S.C. §1030(a)(5)(B)(iv), and also affects a computer system used by a government entity for national security purposes, within the meaning of 18 U.S.C. §1030(a)(5)(B)(v), due to the

role of the MBTA in Homeland Security efforts, and transit services generally. *See* Kelley Decl. ¶¶6, 8-9.

III. Irreparable Harm

"Irreparable injury' in the preliminary injunction context means an injury that cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005). The loss of a trade secret is generally found to constitute irreparable harm. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F.Supp.2d 23, 32 (D.Mass. 2004). That is in recognition of the fact that, "once the trade secret is lost, it is gone forever." *Id. (citing FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir.1984)).

Here, if what the MIT Undergrads claim in their public announcements is true, public disclosure of the security flaws in the Fare Media System – before the MBTA and its system vendors have an opportunity to correct the flaws – will cause significant damage to the MBTA's transit system. Kelley Decl. ¶27; Foster Decl. ¶25. The requested relief, therefore, is necessary to preserve the status quo until a full hearing. *See CMM Cable Rep., Inc. v. Ocean Coast Properties, Inc.*, 48 F.3d 618, 620 (1st Cir.1995)

IV. Reliance On Industry-Recognized "Responsible Disclosure" Practices, There Will Be No Cognizable Harm To The MIT Undergrads.

The temporary halt on the MIT Undergrad's disclosures will not create cognizable harm to the defendants. This is particularly true in light of industry practices, and the so-called "responsible disclosure" doctrine.

The term "responsible disclosure" refers to the method of disclosing a technological vulnerability to the developer so that the developer can fix the vulnerability before the general

public finds out about it. Making a disclosure of the vulnerability to the developer is necessary to obtain a fix. If the discoverer discloses the vulnerability to a broader audience, hackers and other malicious users may be able to exploit the vulnerability before the developer implements a fix. The term "responsible disclosure" is generally used to refer to the process by which (i) the discoverer discloses the vulnerability, (ii) the vulnerability is corrected, and (iii) hackers are prevented from exploiting the vulnerability in the interim.

Microsoft defines the term "responsible disclosure" as follows:

> In a responsible disclosure scenario, the researcher who discovers the vulnerability reports the findings directly to the appropriate vendor, providing a reasonable amount of time for the vendor to investigate, create, and test the necessary update. Only when the update is made available are actual details of the vulnerability made public, with due credit given to the original reporter. (emphasis added).[1]

Google states that "responsible disclosure" is an "industry best practice." Specifically, Google defines the term, and elaborates on the term in its "Security and Product Safety" as follows:

> This process of notifying a vendor before publicly releasing information is an industry-standard best practice known as responsible disclosure. Responsible disclosure is important to the ecology of the Internet. It allows companies like Google to keep users safe by fixing vulnerabilities and resolving security concerns before they are brought to the attention of the bad guys. We strongly encourage anyone who is interested in researching and reporting security issues to observe the simple courtesies and protocols of responsible disclosure. (emphasis added).[2]

---

[1] See Malware Revolution: A Change in Target (published: March 14, 2007), Microsoft Website, located at http://www.microsoft.com/technet/community/columns/secmgmt/sm0307.mspx .

[2] Google Security and Product Safety, located at http://www.google.com/corporate/security.html; see, Symantec Responsible Disclosure Policy (January 2006) (listing 5 steps Symantec commits to follow as part of its "responsible disclosure" procedures), located at http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf.

A number of industry groups have proposed various "uniform" policies relating to these disclosure issues.[3]

V. The Requested Relief Furthers The Public Interest.

The final factor is the public interest. This factor requires the Court to "inquire whether there are public interests beyond the private interests of the litigants that would be affected by the issuance or denial of injunctive relief." *Friends of Magurrewock, Inc. v. U.S. Army Corps of Engineers*, 498 F.Supp.2d 365, 379 (D.Me.,2007) (quoting *Everett J. Prescott, Inc. v. Ross*, 383 F.Supp.2d 180, 193 (D.Me.2005))

The MBTA provides approximately 1.4 million passenger trips per weekday.[4] The Fare Media System threatened by the MIT Undergrads' conduct governs the majority of this system. It is strongly in the public interest to protect this system in the manner requested, particularly in light of the steps the MBTA has taken to avoid the necessity of requesting relief from this Court.

[3] See, e.g., Rain Forest Puppy - Full Disclosure Policy (RFPolicy) v2.0. located at http://www.wiretrip.net/rfp/policy.html; Organization for Internet Safety Guidelines for Security Vulnerability Reporting and Response, V2.0 (2004) located at http://www.oisafety.org/index.html.

[4] Kelley Decl. ¶6.

Conclusion

THEREFORE, the plaintiff respectfully requests that this Court enter the attached proposed Order.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

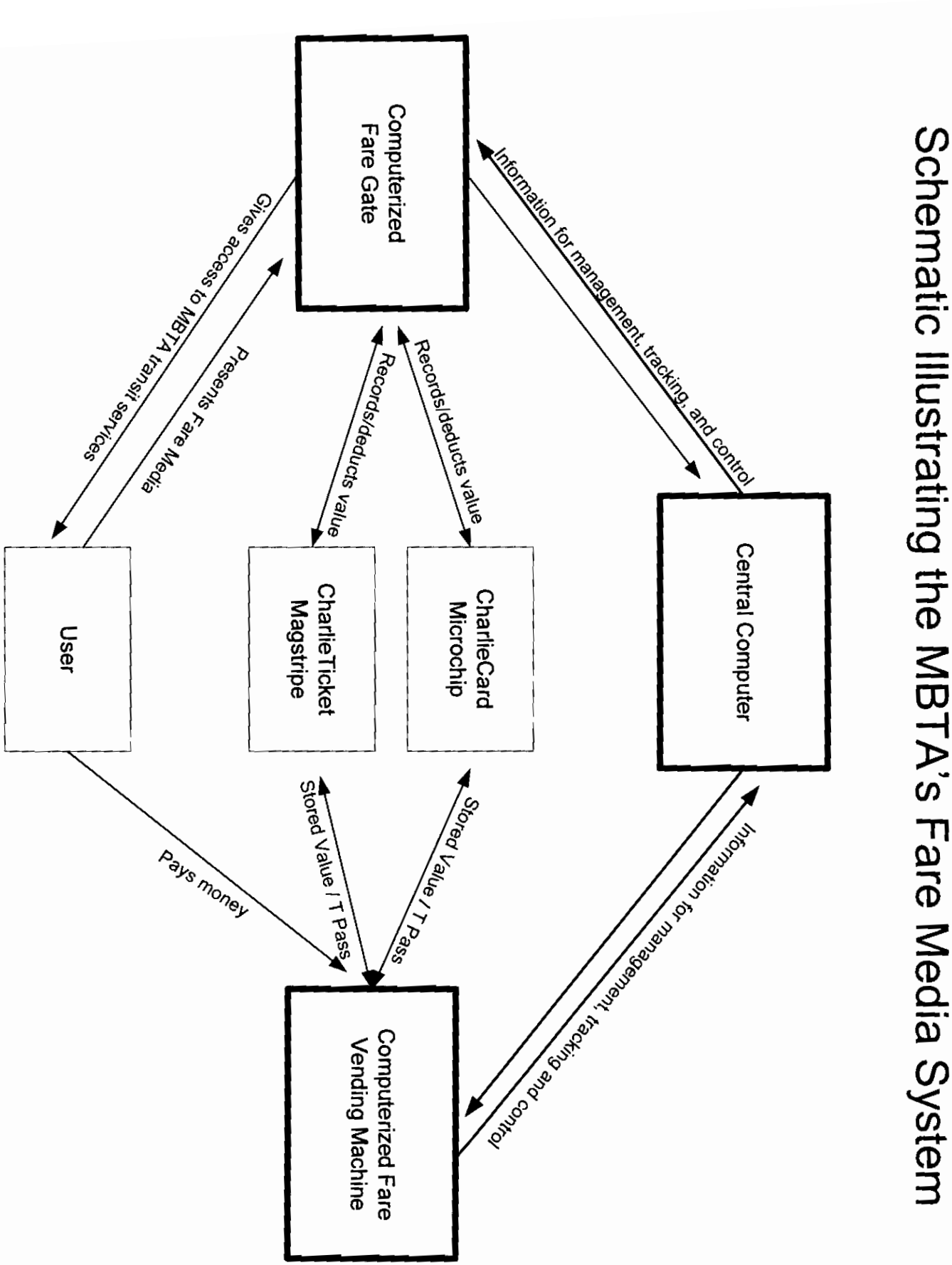
By its attorneys,

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August __, 2008
Boston, Massachusetts

5530567_v1


Schematic Illustrating the MBTA's Fare Media System
Computerized Fare Gate
Central Computer
User
CharlieTicket Magstripe
CharlieCard Microchip
Computerized Fare Vending Machine
Information for management, tracking, and control
Gives access to MBTA transit services
Presents Fare Media
Records/deducts value
Records/deducts value
Pays money
Stored Value / T Pass
Stored Value / T Pass
Information for management, tracking and control

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, SUSAN HOCKFIELD, PHILLIP L. CLAY, and the MIT CORPORATION

Defendants

Civil Action No. _____

DECLARATION OF RICHARD SULLIVAN

1. I am a Sergeant Detective in the Transit Police of the plaintiff, Massachusetts Bay Transportation Authority ("MBTA"). I am the Transit Police liaison to the Federal Bureau of Investigation (the "FBI").

2. I have held this position since April 2002.

3. I make this declaration based on my personal knowledge.

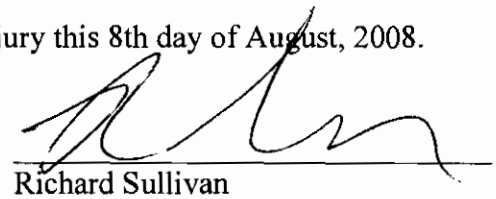
4. Some time after July 30, 2008, I was informed that the MBTA had learned of statements, purportedly made by the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads"), that related to the security of fare media used on the MBTA transit system.

5. I worked with the MIT Professor Ron Rivest and the FBI to arrange a meeting with the MIT Undergrads to discuss the issues.

6. This meeting took place on August 5, 2008 at MIT. I attended the meeting with a local FBI agent, Jacob Shaver.

7. This meeting was attended by the MIT Undergrads, with the exception of Alessandro Chiesa, by their Professor, Ron Rivest, and by an individual, Jay Wilcox, who identified himself as MIT counsel.

Signed under the penalties of perjury this 8th day of August, 2008.



Richard Sullivan
MBTA Transit Police

5530793_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY
TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, et al.

Defendants

Civil Action No. _____

DECLARATION OF GARY FOSTER

1. I am the Chief Technology Officer for the plaintiff, Massachusetts Bay Transportation Authority ("MBTA").

2. I have held this position since January 28, 2008. My duties include responsibility for the network and system software and hardware employed in the Automated Fare Collection System, including the CharlieTicket and CharlieCard systems. My duties also include collaboration with business partners to assure security measures, encryption structures, and other safeguards employed in these Fare Media systems are operationally.

3. I make this declaration based on my personal knowledge and a review of MBTA business records concerning the matters set out below.

Security Features Of The CharlieTicket And CharlieCard Passes

4. The Fare Media system contains features to preserve system integrity and security.

5. For example, the CharlieCard chip contains both open and MBTA proprietary encryption.

6. The MBTA CharlieCard pass is built upon a so-called "MIFARE Classic 1K" card. There have been attacks on the security of MIFARE Classic cards, that have been publicized and that purport to be successful.

7. The MBTA, through its vendors, has commissioned, developed, and included MBTA proprietary security systems and technology on the CharlieCard, to substantially enhance existing security present on the out-of-the-box MIFARE Classic 1K card. Therefore, issues with underlying MIFARE Classic cards are not at issue.

8. It is extremely important to maintain the security and integrity of the Fare Media systems. With an insecure, compromised system, even basic revenue controls, to name one example, become significantly challenging.

9. Included in the Exhibits, as Exhibit 5, is a document entitled "Schematic Illustrating the MBTA's Fare Media System." This Schematic provides a fair and accurate general description of the components of the MBTA's in-station Automated Fare Collection System, including the MBTA's CharlieCard and CharlieTicket Fare Media.

The Initial Announcement

10. On July 30, a vendor responsible for components of the Automated Fare Collection System notified the MBTA of its discovery of an Internet posting that advertised a presentation at the upcoming DEFCON 16 "hackers" conference. This email included a copy of the "Initial Announcement" identified in the Complaint. A true and accurate copy of the email provided to me with this notice is included as Exhibit 1.

11. This Initial Announcement raised a number of concerns.

12. First, the Initial Announcement specifically targets the MBTA and its computerized Fare Media systems. Second, the Initial Announcement suggests that MIT Undergrads have wholly compromised the CharlieCard system. Third, in the Initial

Announcement, the MIT Undergrads promise to provide to attendees at their presentation "free subway rides for life." Fourth, the Initial Announcement advertises the connection between the authors and MIT, and suggests an endorsement or other approval of the presentation. Finally, the MIT Undergrads claim that they will provide software tools to allow others to "break" the MBTA's CharlieCard and CharlieTicket system.

The DEFCON Conference

13. The Initial Announcement presented concerns, in addition, due to the forum the MIT Undergrads had chosen. The Announcement indicated that the MIT Undergrads would present this information at DEFCON 16.

14. According to information published by DEFCON, the DEFCON Conference, taking place this year at the Riviera Hotel & Casino in Las Vegas, Nevada, is "one of the oldest continuous hacker conventions around, and also one of the largest." I have included as Exhibit 2 a true and accurate copy of the FAQs that contain this information. *See* https://www.defcon.org/html/links/dc-faq/dc-faq.html.

15. Organizers state that the Conference is anticipated to draw 5,000 to 7,000 attendees, and that "technology and hacking is the core" of the Conference. *See id.*

16. The 2008 DEFCON Conference begins on Friday, August 8, and the MIT Undergrads are scheduled to give their "The Anatomy of a Subway Hack" presentation at 1:00 on Sunday, August 10, 2008. I have included as Exhibit 3 a copy of the DEFCON schedule, available at the DEFCON site, showing this timing.

The MIT Undergrads' Response To The MBTA's Requests

17. After discovering the Initial Announcement and the threat it posed, we worked with law enforcement to arrange a meeting with the MIT Undergrads to discuss their intentions, and to present our concerns.

18. This meeting took place on August 5, 2008. I understand from the MBTA's representative at this meeting, Sergeant Sullivan, that the meeting was attended by the MIT Undergrads, by their Professor, Ron Rivest, and MIT counsel.

19. The MBTA has requested through MIT Professor Ron Rivest that the MIT Undergrads provided a copy of the materials the MIT Undergrads plan to present at the DEFCON Conference.

20. The MIT Undergrads have not provided this information.

21. After this August 5 meeting, the Initial Announcement was revised to read in relevant part as follows (for convenience, the "Revised Announcement"). I have included as Exhibit 4 a copy of this Revised Annoucement.

22. The Revised Announcement does not alleviate the MBTA's concerns.

23. Like the Initial Announcement, the Revised Announcement (i) targets the MBTA and its specific Fare Media systems by name; (ii) claims that the CharlieCard system has been "completely" broken by the authors' attacks; (iii) continues to suggest endorsement and approval by MIT; and (iv) continues to promise the release of software tools and demonstrations to allow others to duplicate the attacks.

24. The MIT Undergrads' actions have caused the MBTA to expend substantial funds to respond to the threat they present. Due to the defendants' failure to provide information reasonably requested by the MBTA, the MBTA is concerned about improper ridership based on the defendants' activities. In addition, the MBTA is uncertain as to the level of threat the MIT Undergrads' activities in fact pose.

25. If what the MIT Undergrads claim is true, then their presentation at DEFCON – or indeed any disclosure before the MBTA and its vendors have had an opportunity to correct the alleged flaws -- will inflict significant damage, unless the requested relief is granted.

Signed under the penalties of perjury this 8th day of August, 2008.

Gary Foster

5529716_v3

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON et al.

Defendants

Civil Action No. _____

DECLARATION OF JOSEPH KELLEY

1. I am the Deputy General Manager for Systemwide Modernization for the plaintiff, Massachusetts Bay Transportation Authority ("MBTA").

2. I have held this position since August 8, 2005. My duties include the management and oversight of systemwide improvements and modernization. Part of my duties consisted of supervision and overall responsibility for the implementation and operations of the Automated Fare Collection System.

3. I make this declaration based on my personal knowledge and a review of MBTA business records concerning the matters set out below.

The MBTA's Transit System

4. The MBTA is the nation's 5th largest mass transit system. The MBTA serves a population of 4,667,555 (based on the 2000 census) in 175 cities and towns with an area of 3,244 square miles.

5. To provide these transit services, the MBTA maintains 183 bus routes, 2 of which are Bus Rapid Transit lines, 3 rapid transit lines, 5 streetcar (Central Subway/Green Line) routes, 4 trackless trolley lines and 13 commuter rail routes. The MBTA's transit equipment includes of

JAK

927 diesel and CNG buses, 32 dual mode buses, 28 ETB's (electric trolley buses), 408 heavy rail vehicles, 200 light rail vehicles, 10 PCC's streetcars, 83 commuter rail locomotives, 410 commuter rail coaches and 298 MBTA-owned specially equipped vans and sedans, and an additional 235 contractor-supplied specially equipped vans and sedans.

6. The average weekday ridership for the entire system is approximately 1.4 million passenger trips. The approximate average weekday revenue of the MBTA is $700,000.00.

7. The MBTA directly services Rhode Island as well as Massachusetts, via its commuter rail service.

8. The MBTA is the recipient of significant funding from the United States Department of Transportation, through the Urban Mass Transportation Administration ("UMTA"). Since the mid-1960's, the MBTA has received over $3.5 billion in such funding, for its capital improvement projects and its yearly operating programs.

9. In addition to this funding, the MBTA receives funds from the Department of Homeland Security, to implement various security, anti-terrorism, and other security initiatives. For example, in 2007 the MBTA received $4 million from the Department of Homeland Security and the Federal Transit Administration, for use in emergency communications initiatives.

The Procurement And Implementation Of The MBTA's Automated Fare Collection System

10. The MBTA has recently undertaken significant system improvements. A central improvement consisted of the procurement and installation of an automated fare collection system (the "Automated Fare Collection System" or "AFC System"). The Automated Fare Collection System replaces the MBTA's old "token" system, and is comprised of the following general, high-level system components:

(a) Computerized fare gates in each station, that read fare media and permit (or deny) users access to MBTA transit services ("Fare Gates");

JDK

(b) Computerized fare vending machines in each station (and elsewhere), that accept payment and issue or load value to fare media ("Fare Vending Machines");

(c) Fare media that communicate with the Fare Gates and the Fare Vending Machines to store and transfer "value" – the equivalent of the old token -- and that allow paying patrons to access the MBTA's transit services ("Fare Media");

(d) A central computing facility that controls and exchanges data with Fare Gates, with Fare Vending Machines, with servers and other devices connected to the AFC System network, with remote retail sales outlets, and with dial-in and other connections to the AFC System; and

(e) Complex sets of software applications that are resident on servers at the central computing facility, on the Fare Gates, on the Fare Vending Machines, and on certain Fare Media. These software applications (among other tasks) manage and control the issuance of fare media, payments for transit services, rate schedules, ridership volumes, and a wide range of other tasks and information.

11. The AFC System, accordingly, is highly automated, and is comprised of high speed data processing devices that perform logical, arithmetic, and storage functions.

12. The procurement and installation of the Automated Fare Collection System cost in excess of $180 million.

The CharlieCard and CharlieTicket Systems

13. Fare Media are broken into two categories: (i) so-called "CharlieCard" passes and (ii) so-called "CharlieTicket passes". These Fare Media each employ slightly different technology.

14. A CharlieTicket pass uses a so-called a "magnetic stripe" or "magstrip" to convey information to the Automated Fare Collection System. CharlieTicket passes are paper-based media, and to employ a CharlieTicket pass, a user brings the Ticket's magstrip into physical contact with a reader in fare gate, by "swiping" the Ticket past the designated reading head. A

user can "store value" on his or her CharlieTicket pass, or can store a monthly pass (or other pass) on the CharlieTicket pass.

15. CharlieCard passes, in contrast, are plastic media, and are so-called "smart cards." Each CharlieCard pass contains an integrated circuit – a computer chip – that processes information. This chip allows a user to store value for single or multiple rides and/or a T-pass. In addition, the smart card features of the CharlieCard pass allow for online account management, and other services that are not compatible with the CharlieTicket pass technology.

16. The user loads a CharlieTicket pass or a CharlieCard pass with value or a T-Pass using cash, credit or debit cards, at in-station fare vending machines, at retail sales terminals, at MBTA ticket offices, or online via the MBTA's website at www.mbta.com.

The Importance Of The CharlieCard Pass

17. The MBTA has implemented both CharlieTicket passes and CharlieCard passes in its Automated Fare Collection System. CharlieCard passes, for example, began to be used in January 2007.

18. The CharlieCard has become the preferred fare media of MBTA riders.

19. Currently, over eighty percent (68%) of riders use the CharlieCard pass, with ninety percent (90%) receiving the best value by using monthly magnetic stripe cards and CharlieCards. Accordingly, CharlieCards account for approximately $475,000.00 per weekday in revenues.

20. The CharlieCard is employed in the MBTA's corporate pass program, whereby employers provide MBTA fare media to their employees. As of the spring of 2008, this program had grown to include over 1,300 companies with offices in the Boston area.

21. Although CharlieCards are not currently employed on the MBTA's commuter rail system, a pilot program for such use is scheduled to commence in 2009.

JPK

Harm To The MBTA System

22. I have reviewed the documents referred to in the Complaint as the " Initial Announcement" and the "Revised Announcement".

23. Since the August 5, 2008 meeting with the MIT Undergrads and their professor, Ron Rivest , I have spoken to Professor Rivest on several occasions. I continued to explain the MBTA's concerns, and asked that he arrange to have the MIT Undergrads forward a copy of their proposed DEFCON presentation to the MBTA.

24. The MBTA has not received a copy of these materials.

25. I had understood that the MIT Undergrads were willing to engage in a conference call on Thursday, August 7, 2008, while they were en route to the DEFCON Conference. We did not hear from the Undergrads and were unable to contact them.

26. I spoke with Professor Rivest most recently this morning, Friday August 8, 2008. I again informed him that the MBTA had not received the MIT Undergrads' presentation materials.

27. If what the MIT Undergrads claim in these Announcements is true, disclosure of this information will significantly compromise the CharlieCard and CharlieTicket systems. This in turn will harm the overall functioning of the MBTA's transit services.

28. The MBTA demands that the MIT Undergrads refrain from disclosure until the MBTA's system vendors have remedied the security flaw the MIT Undergrads claim to have identified. The MBTA does not demand that the MIT Undergrads forever refrain from disclosing this information.

Signed under the penalties of perjury this 8th day of August, 2008.

Joseph Kelley

5529633_v2

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. _____

DECLARATION OF IEUAN G. MAHONY

1. I am a partner at Holland & Knight, LLP, representing the Massachusetts Bay Transportation Authority ("MBTA") in this matter.

2. I certify to the following efforts made to notify the defendants of the present Motion for Temporary Restraining Order ("TRO"):

(a) On Friday August 8, 2008, Joseph Kelley spoke with the MIT Undergrads' professor, Ron Rivest, to again request presentation materials.

(b) On Friday August 8, 2008, after the decision was made to proceed, William A. Mitchell, Jr., General Counsel for the MBTA contacted R. Gregory Morgan, Vice President and General Counsel of MIT to inform him of the planned Motion.

(c) On Friday August 8, 2008, once the papers were ready to be brought to court, Daniel Grabouskus, General Manager of the MBTA, made efforts to contact the President of MIT.

3. The document included in the Exhibit Binder as Exhibit 6 is a true and accurate comparison of the Initial Announcement (Exhibit 1) and the Revised Announcement (Exhibit 4), using the software application Deltaview.

4. The documents included in the Exhibit Binder as Exhibit 7 are true and accurate copies of (i) a July 14, 2008 CNET New.com posting by R. Vamosi entitled "Column: The Man Who Changed Internet Security", located at http://news.cnet.com/8301-10789_3-9989292-57.html?tag=st.nl; and (ii) an August 7, 2008 CNET News.com posting by R. Vamosi entitled "Kaminsky Provides the Why of Attacking DNS", located at http://news.cnet.com/8301-1009_3-10009951-83.html?tag=st.nl .

5. The document included in the Exhibit Binder as Exhibit 8 is a true and accurate copy of the Athena Rules of Use (including MITnet Rules of Use), located at http://web.mit.edu/olh/Rules/.

Signed under the penalties of perjury this 8th day of August, 2008.

Ieuan G. Mahony

5530574_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON et al

Defendants

Civil Action No. _____

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. Rules of Civ. P., Local Rule 7.1, Plaintiff, Massachusetts Bay Transportation Authority ("MBTA) files this Corporate Disclosure Statement:

1. The MBTA is a state, governmental agency governed by, inter alia, Chapter 16IA of the Massachusetts General Laws.

1. Plaintiff MBTA has no parent company.

2. No publicly held company owns more than a 10% interest in MBTA.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

Ieuan G. Mahony (BBO #552349)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Dated: August 8, 2008

5531221_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08-11364-GAO

SUPPLEMENTAL DECLARATION OF IEUAN G. MAHONY

1. I am a partner at Holland & Knight, LLP, representing the Massachusetts Bay Transportation Authority ("MBTA") in this matter. The following supplements my earlier Declaration in this matter.

The Defendants' Delay In Providing The Actual DEFCON Presentation Materials

2. By email dated Friday, August 8 at 8:13 PM I notified counsel for the MIT Undergrads and counsel for MIT (collectively, "Defendants' Counsel") of the hearing scheduled for today. I stated to the MIT Undergrads' counsel that "I urge you strongly to advise your clients to provide us with all presentation material and al other materials they may with to circulate concerning the MBTA's Fare Media Systems." I noted that the August 8 Undergrad-to-MBTA Report (attached as Exhibit 1 to the Declaration of Scott Henderson) "does not appear to comprise all (or perhaps any) DEFCON presentation materials." *See* attached Exhibit 1 (emphasis added).

3. By email dated Friday, August 8 at 8:17 PM I provided a copy Defendants' Counsel with a copy of the Court's Order of yesterday. *See* Exhibit 2. I had previously left

FILED
In Open Court
USDC, Mass.
Date 8/9/08
By JARRETT LOVETT
Deputy Clerk

detailed voice-mail messages with Defendants' Counsel, in order to begin attorney-to-attorney discussions in this matter.

4. By email dated Friday, August 8 at 8:31 PM, I asked Defendants' Counsel, Marcia Hofman (for the MIT Undergrads) and Jay Wilcoxson (in-house counsel for MIT) to confirm whether they had received my voice-mail messages and email, and whether they planned to attend the hearing. *See* Exhibit 3.

5. Shortly after I sent Exhibit 3, at approximately 8:35, I reached Attorney Wilcoxson. During our discussion, among other points, I urged Attorney Wilcoxson to do what he could to convince the MIT Undergrads to immediately provide us with any materials they intended to disclose or present concerning the MBTA's systems at issue.

6. After our discussion, by email dated Friday, August 8 at 8:52 PM, Attorney Wilcoxson confirmed that MIT would be represented by counsel at this hearing. *See* Exhibit 4.

7. Shortly after my discussion with Attorney Wilcoxson, at approximately 9:00, I reached Marcia Hofman, from the Washington DC office of the Electronic Frontier Foundation (the "EFF"). Attorney Hofman confirmed that she was representing the MIT Undergrads. Attorney Hofman's colleague from the San Franscico office of the EFF, Kurt Opsahl, also participated in this call.

8. During our discussion, among other points, I urged Attorney Hofman and Attorney Opsahl to provide us with any materials their clients intended to disclose or present at the DEFCON Conference concerning the MBTA's systems at issue. During this call, we also discussed a proposed Order in this matter, revised as suggested by the Court during the Friday hearing.

9. Shortly after this call, by email dated Friday, August 8 at 9:55 PM, I forwarded a revised Order, and indicated further interest in discussing a negotiated solution. *See* Exhibit 5.

10. Counsel for the MIT Undergrads then called me, at approximately 11:30, to discuss the MBTA's position, the MBTA's view of the "responsible disclosure" doctrine, and possible discussions toward a negotiated solution. Counsel also indicated an interest in postponing today's hearing.

11. By email dated Saturday, August 9 at 1:30 AM, I reminded Counsel for the MIT Undergrads that the MBTA still had not received any presentation materials. I noted that "the decision to continue to withhold these materials makes me concerned." *See* Exhibit 6.

12. By email dated Saturday, August 9 at 4:38 AM, Counsel for the MIT Undergrads forwarded to me an 87 page set of slides, that purports to constitute the DEFCON presentation of the MIT Undergrads. A copy of this slide deck is attached as Exhibit 7. I have hand-numbered the pages, as the formatting of the document does not allow the addition of page numbers. I provide a color copy to the Court, and black and white copies to Defendants' Counsel.

13. In their email of Saturday, August 9 at 4:38 am (Exhibit 8), Counsel for the MIT Undergrads informed the MBTA that this slide deck had already been distributed at the DEFCON Conference.

14. By emails dated Saturday, August 9 at 5:15 and 5:26 AM, I asked Defendants' Counsel to state when these materials had been provided to DEFCON, when they had been distributed, and whether the defendants' knew of the MBTA's requests to review these materials before they were distributed at DEFCON. *See* Exhibit 9.

15. I met with Scott Henderson of the MBTA and Daniel Terryn, Technical Software Manager of Scheidt & Bachmann this morning at Logan Airport at 6:00 to seek to review these

Presentation Materials (Ex. 7) before they flew to Las Vegas on an 8:00 flight. There was insufficient time to prepare Declarations concerning these materials, and the MBTA will rely on oral argument.

Signed under the penalties of perjury this 9th day of August, 2008.

Ieuan G. Mahony

5533212_v1

Exhibit 1

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:13 PM
To: 'marcia@eff.org'
Cc: 'jaren@mit.edu'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: FW: Pleadings

Attachments: MahonyDeclaration.pdf; Complaint.pdf; Disclosure.pdf; Fosterdeclarataion.pdf; KelleyDeclaration.pdf; MemoinSupport.pdf; Order.pdf; SullivanDec.pdf; SullivanDeclaration.pdf; TROMotion.pdf

Marcia:
Per my recent voice-mail to you, I understand from your communications with Bill Mitchell, and from Mr. Anderson's voice-mail to Scott Henderson, that you are representing the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa. This matter presents the following issues from our end:

(1) Pleadings Filed

I have attached the pleadings filed today. An email will follow with the exhibits, and the Order that issued in the case.

(2) Hearing Tomorrow

The Order sets a further hearing for tomorrow at 11:00 on the Seventh floor, Courtroom 20, at the John Joseph Moakley U.S. Courthouse, 1 Courthouse Way, Boston 02210.

(3) DEFCON Presentation Materials.

As you may know, the MBTA has requested that your clients present a complete set of materials they intend to present at the DEFCON Conference. Late today, the MBTA received a 4 page (excluding the cover sheet) document entitled "Prepared for the Massachusetts Bay Transit Authority: Fare Collection Vulnerability Assessment Report" dated August 8, 2008. We have reviewed this document and it does not appear to comprise all (or perhaps any) DEFCON presentation materials.

In a voice-mail to Scott Henderson this evening, Mr. Anderson suggested that he had distributed a CD of materials at the DEFCON Conference for this presentation. Mr. Anderson stated, however, that he was unable to send these materials due to poor internet. Mr. Anderson later called and left a message for Mr. Henderson informing him that, on the advice of counsel, Mr. Anderson was not providing further information to the MBTA on the presentation.

I urge you strongly to advise your clients to provide us with all presentation materials and all other materials they may wish to circulate concerning the MBTA's Fare Media Systems. I see no basis for withholding this information.

(4) Negotiated Order

The papers I have attached include a proposed Order. The Judge discussed revisions to this Order with us this afternoon. If you believe that the Order, with revisions, may provide a basis for discussing a negotiated resolution, by way of a form of consent judgment, please let me know. I left with your voice-mail my cell and work numbers. I have included them below as well.

I will call again later this evening to answer any questions you may have. I will also again urge you to immediately provide all presentation materials.

Thank you

Ieuan Mahony

Holland Knight

Ieuan G. Mahony
Partner

Holland & Knight LLP

10 St. James Ave.
Boston, MA 02116-3889

Main 617-523-2700
Direct 617 573-5835
Cell 781-789-4230
Fax 617-523-6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect it to hold in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney client or work product privilege that may be available to protect confidentiality.


MahonyDeclaration.pdf (13 KB)


Complaint.pdf (106 KB)


Disclosure.pdf (19 KB)


Fosterdeclaratai on.pdf (19 KB)...


KelleyDeclaratio n.pdf (78 KB)


MemoinSupport. pdf (26 KB)


Order.pdf (13 KB)


SullivanDec.pdf (14 KB)


SullivanDeclarati on.pdf (13 KB...


TROMotion.pdf (14 KB)

Exhibit 2

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:17 PM
To: 'marcia@eff.org'; 'jaren@mit.edu'
Cc: William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: FW: Activity in Case 1:08-cv-11364-GAO Massachusetts Bay Transportation Authority v. Anderson et al Motion Hearing

Counsel:
Below is the Order that entered this evening. Again, the hearing is set for **tomorrow, Saturday, August 9, at 11:00.**

Ieuan Mahony

From: ECFnotice@mad.uscourts.gov [mailto:ECFnotice@mad.uscourts.gov]
Sent: Friday, August 08, 2008 6:21 PM
To: CourtCopy@mad.uscourts.gov
Subject: Activity in Case 1:08-cv-11364-GAO Massachusetts Bay Transportation Authority v. Anderson et al Motion Hearing

This is an automatic e-mail message generated by the CM/ECF system. Please DO NOT RESPOND to this e-mail because the mail box is unattended.
*****NOTE TO PUBLIC ACCESS USERS*** Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy each document during this first viewing. However, if the referenced document is a transcript, the free copy and 30 page limit do not apply.**

United States District Court

District of Massachusetts

Notice of Electronic Filing

The following transaction was entered on 8/8/2008 at 6:21 PM EDT and filed on 8/8/2008

Case Name: Massachusetts Bay Transportation Authority v. Anderson et al
Case Number: 1:08-cv-11364
Filer:
Document Number: No document attached

Docket Text:
Electronic Clerk's Notes for proceedings held before Judge Douglas P. Woodlock: Motion Hearing held on 8/8/2008 in courtroom 20 re [2] MOTION for Temporary Restraining Order filed by Massachusetts Bay Transportation Authority: Pltff informs the Court that the parties are aware of today's proceedings; Court hears initial argument; a Further Hearing as to [2]

MOTION for Temporary Restraining Order is set for 8/9/2008 11:00 AM in Courtroom 20 before Judge Douglas P. Woodlock. The pltff is to inform the deft's of said hearing and advise them to have counsel present; pltff is further Ordered to file a supplemental affidavit by 8/9/08. (Digital Recording)(Interpreter: Mahoney and Darling for the pltff)(Attorneys present: Mahoney and Darling for the pltff) (Lovett, Jarrett)

1:08-cv-11364 Notice has been electronically mailed to:

Ieuan-Gael Mahony ieuan.mahony@hklaw.com, yvette.cooks@hklaw.com

Maximillian J. Bodoin max.bodoin@hklaw.com

1:08-cv-11364 Notice will not be electronically mailed to:

Exhibit 3

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:31 PM
To: 'jaren@mit.edu'
Cc: 'marcia@eff.org'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: RE: Pleadings

Jay and Marcia:
Judge Woodlock was interested in (i) knowing whether parties planned to attend the hearing tomorrow, and (ii) receiving assurance that counsel in fact received notice concerning this hearing. I have left you each voice-mail and a number of email in this regard.

I will try you again this evening, and tomorrow morning before the hearing, but I would appreciate a confirmation (a) that you have received my communications; and (b) as to whether you plan to attend the hearing. Marcia, we would have no objection to your attending and being heard telephonically, in light of your presence at the DEFCON Conference.

Let me know
Thanks
Ieuan

Holland · Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP

10 St. James Ave.
Boston, MA 02116-3889

Main 617-523-2700
Direct 617-573-5835
Fax 617-523-6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect to be held in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney-client or work product privilege that may be available to protect confidentiality.

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:13 PM
To: 'marcia@eff.org'
Cc: 'jaren@mit.edu'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: FW: Pleadings

Marcia:
Per my recent voice-mail to you, I understand from your communications with Bill Mitchell, and from Mr. Anderson's voice-mail to Scott Henderson, that you are representing the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa. This matter presents the following issues from our end:

(1) Pleadings Filed

I have attached the pleadings filed today. An email will follow with the exhibits, and the Order that issued in the case.

(2) Hearing Tomorrow

The Order sets a further hearing for tomorrow at 11:00 on the Seventh floor, Courtroom 20, at the John Joseph Moakley U.S. Courthouse, 1 Courthouse Way, Boston 02210.

(3) DEFCON Presentation Materials.

As you may know, the MBTA has requested that your clients present a complete set of materials they intend to present at the DEFCON Conference. Late today, the MBTA received a 4 page (excluding the cover sheet) document entitled "Prepared for the Massachusetts Bay Transit Authority: Fare Collection Vulnerability Assessment Report" dated August 8, 2008. We have reviewed this document and it does not appear to comprise all (or perhaps any) DEFCON presentation materials.

In a voice-mail to Scott Henderson this evening, Mr. Anderson suggested that he had distributed a CD of materials at the DEFCON Conference for this presentation. Mr. Anderson stated, however, that he was unable to send these materials due to poor internet. Mr. Anderson later called and left a message for Mr. Henderson informing him that, on the advice of counsel, Mr. Anderson was not providing further information to the MBTA on the presentation.

I urge you strongly to advise your clients to provide us with all presentation materials and all other materials they may wish to circulate concerning the MBTA's Fare Media Systems. I see no basis for withholding this information.

(4) Negotiated Order

The papers I have attached include a proposed Order. The Judge discussed revisions to this Order with us this afternoon. If you believe that the Order, with revisions, may provide a basis for discussing a negotiated resolution, by way of a form of consent judgment, please let me know. I left with your voice-mail my cell and work numbers. I have included them below as well.

I will call again later this evening to answer any questions you may have. I will also again urge you to immediately provide all presentation materials.

Thank you

Ieuan Mahony

Holland Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP

10 St. James Ave
Boston, MA 02116-3889

Main 617-523-2700
Direct 617-523-5835
Cell 781-789-4230
Fax 617-523-6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect to be held in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney-client or work product privilege that may be available to protect confidentiality.

<< File: MahonyDeclaration.pdf >> << File: Complaint.pdf >> << File: Disclosure.pdf >> << File: Fosterdeclarataion.pdf >> << File: KelleyDeclaration.pdf >> << File: MemoinSupport.pdf >> << File: Order.pdf >> << File: SullivanDec.pdf >> << File: SullivanDeclaration.pdf >> << File: TROMotion.pdf >>

Exhibit 4

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:52 PM
To: 'jaren@mit.edu'
Cc: marcia@eff.org; WMitchell@mbta.com; SDarling@mbta.com; rgmorgan@mit.edu; Mahony, Ieuan (BOS - X75835)
Subject: RE: Pleadings

Thanks Jay.

From: Jaren D. Wilcoxson [mailto:jaren@mit.edu]
Sent: Friday, August 08, 2008 8:52 PM
To: Mahony, Ieuan (BOS - X75835)
Cc: marcia@eff.org; WMitchell@mbta.com; SDarling@mbta.com; rgmorgan@mit.edu
Subject: Re: Pleadings

Reveived and MIT plans to attend.

Jaren D. Wilcoxson
Counsel
Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Room 12-090
Cambridge, MA 02139
tel: 617-253-7724
fax: 617-258-0267
jaren@mit.edu

This message and any attached documents contain information which may be confidential, subject to privilege, or exempt from disclosure under applicable law. These materials are intended only for the use of the intended recipient. Delivery of this message to any person other than the intended recipient shall not compromise or waive such confidentiality, privilege, or exemption from disclosure as to this communication.

Sent from my Verizon Wireless BlackBerry

From: <ieuan.mahony@hklaw.com>
Date: Fri, 8 Aug 2008 20:31:06 -0400
To: <jaren@mit.edu>
CC: <marcia@eff.org>; <WMitchell@mbta.com>; <SDarling@mbta.com>; <ieuan.mahony@hklaw.com>
Subject: RE: Pleadings

Jay and Marcia:

Judge Woodlock was interested in (i) knowing whether parties planned to attend the hearing tomorrow, and (ii) receiving assurance that counsel in fact received notice concerning this hearing. I have left you each voice-mail and a number of email in this regard.

I will try you again this evening, and tomorrow morning before the hearing, but I would appreciate a confirmation (a) that you have received my communications; and (b) as to whether you plan to attend the hearing. Marcia, we would have no objection to your attending and being heard telephonically, in light of your presence at the DEFCON Conference.

Let me know
Thanks
Ieuan

Holland Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP

10 St. James Ave.
Boston, MA 02116-3889

Main 617 523 2700
Direct 617 573-5835
Fax 617-523-6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect it to hold in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney-client or work product privilege that may be available to protect confidentiality.

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 8:13 PM
To: 'marcia@eff.org'
Cc: 'jaren@mit.edu'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: FW: Pleadings

Marcia:
Per my recent voice-mail to you, I understand from your communications with Bill Mitchell, and from Mr. Anderson's voice-mail to Scott Henderson, that you are representing the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa. This matter presents the following issues from our end:

(1) Pleadings Filed

I have attached the pleadings filed today. An email will follow with the exhibits, and the Order that issued in the case.

(2) Hearing Tomorrow

The Order sets a further hearing for tomorrow at 11:00 on the Seventh floor, Courtroom 20, at the John Joseph Moakley U.S. Courthouse, 1 Courthouse Way, Boston 02210.

(3) DEFCON Presentation Materials.

As you may know, the MBTA has requested that your clients present a complete set of materials they intend to present at the DEFCON Conference. Late today, the MBTA received a 4 page (excluding the cover sheet) document entitled "Prepared for the Massachusetts Bay Transit Authority: Fare Collection Vulnerability Assessment Report" dated August 8,

2008. We have reviewed this document and it does not appear to comprise all (or perhaps any) DEFCON presentation materials.

In a voice-mail to Scott Henderson this evening, Mr. Anderson suggested that he had distributed a CD of materials at the DEFCON Conference for this presentation. Mr. Anderson stated, however, that he was unable to send these materials due to poor internet. Mr. Anderson later called and left a message for Mr. Henderson informing him that, on the advice of counsel, Mr. Anderson was not providing further information to the MBTA on the presentation.

I urge you strongly to advise your clients to provide us with all presentation materials and all other materials they may wish to circulate concerning the MBTA's Fare Media Systems. I see no basis for withholding this information.

(4) Negotiated Order

The papers I have attached include a proposed Order. The Judge discussed revisions to this Order with us this afternoon. If you believe that the Order, with revisions, may provide a basis for discussing a negotiated resolution, by way of a form of consent judgment, please let me know. I left with your voice-mail my cell and work numbers. I have included them below as well.

I will call again later this evening to answer any questions you may have. I will also again urge you to immediately provide all presentation materials.

Thank you

Ieuan Mahony

Holland · Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP

10 St. James Ave.
Boston, MA 02116-3889

Main 617 523 2700
Direct 617 573 5835
Cell 781 789-4230
Fax 617-523 6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect it to hold in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney client or work product privilege that may be available to protect confidentiality.

<< File: MahonyDeclaration.pdf >> << File: Complaint.pdf >> << File: Disclosure.pdf >> << File: Fosterdeclarataion.pdf >> << File: KelleyDeclaration.pdf >> << File: MemoinSupport.pdf >> << File: Order.pdf >> << File: SullivanDec.pdf >> << File: SullivanDeclaration.pdf >> << File: TROMotion.pdf >>

Exhibit 5

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Friday, August 08, 2008 9:55 PM
To: 'marcia@eff.org'; 'kurt@eff.org'
Cc: 'jaren@mit.edu'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: MBTA, MIT Students, and MIT - Revised Proposed Order

Attachments: Redline.doc; #5530720v3_Active_ - MBTA - MIT Students - Propose.DOC

Redline.doc (69 KB) #5530720v3_Active_ - MBTA - MI.

Kurt and Marcia:

As we discussed, I have attached a proposed Order, that I've revised based on comments made by Judge Woodlock during the hearing today. I've included a clean version of this revised Order, and a redline showing the changes from the original proposed Order.

As we discussed, it may be that the parties have interests that are similar: both seeking to act within the CFAA, and resolve possible security issues. I think this proposed Order, particularly as revised, reflects these interests; I recognize, however, that certain elements of the Complaint may be incorrect from your perspective, or arise from misunderstandings. If the proposed Order sufficiently captures the parties' joint interests, but the specific language is off, we should work together to correct the language. Or if the tone or substance of the Complaint needs re-balancing through a joint solution, we should work on that as well. I understand, though, that our discussion was in the nature of "brainstorming," and that none of us is committing to a solution at this point.

Finally, I agreed to inform Judge Woodlock and his clerk of your wish to attend the hearing telephonically, and to state my recommendation that you be permitted to attend in that manner.

Let me know your thoughts. I'll be offline for 1.5 hours or so, then available until 12:30 or so. I'll be available tomorrow morning from 6:30 eastern until 10:30 for the hearing.

Thanks
Ieuan

Holland & Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP

10 St. James Ave.
Boston, MA 02116-3889

Main 617-523 2700
Direct 617-573-5835
Fax 617-523-6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to

whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect it to hold in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney client or work product privilege that may be available to protect confidentiality.

Exhibit 6

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 1:30 AM
To: 'marcia@eff.org'; 'kurt@eff.org'; 'jennifer@eff.org'
Cc: 'Swope, Jeffrey'; 'jaren@mit.edu'; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: MBTA v Anderson et al

Kurt, Marcia, and Jennifer:
Per our 11:30 call, I will be available for another hour or so tonight. I have not circulated your inquiry about possible willingness to postpone the hearing. Please let me know if you wish us formally to consider this as a request.

I note that we still do not have your clients' presentation materials. I am inclined to object to any discussion of a postponement, as the decision to continue to withhold these materials makes me concerned. As I stated during our 9:00, and 11:30 calls this evening, I see no basis for continuing to withhold this information.

With that said, we remain interested in discussing an amicable resolution. Once I have finished the Supplemental Declaration I discussed, I will begin work on a proposed Consent Judgment and format for your review.

Ieuan

Holland Knight

Ieuan G. Mahony
Partner
Holland & Knight LLP
10 St. James Avenue
Boston, MA 02118
Main 617 523 2700
Direct 617 573 5835

Cell 781-789 4230
Fax 617 523 6850
Email ieuan.mahony@hklaw.com

www.hklaw.com

NOTICE: This e-mail is from a law firm, Holland & Knight LLP ("H&K"), and is intended solely for the use of the individual(s) to whom it is addressed. If you believe you received this e-mail in error, please notify the sender immediately, delete the e-mail from your computer, and do not copy or disclose it to anyone else. If you are not an existing client of H&K, do not construe anything in this e-mail to make you a client unless it contains a specific statement to that effect and do not disclose anything to H&K in reply that you expect to be held in confidence. If you properly received this e-mail as a client, co-counsel or retained expert of H&K, you should maintain its contents in confidence in order to preserve the attorney client or work product privilege that may be available to protect confidentiality.

Exhibit 7

Anatomy of a Subway Hack

Russell Ryan

Zack Anderson

Alessandro Chiesa

For updated slides and code, see: http://web.mit.edu/zacka/www/subway/

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 2 of 97

what this talk is:

Pen-testing a subway system



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 3 of 97

what this talk is not:

evidence in court
(hopefully)

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 4 of 97

You'll learn how to

- Generate stored-value fare cards
- Reverse engineer magstripes
- Hack RFID cards
- Use software radio to sniff
- Use FPGAs to brute force
- Tap into the fare vending network
- Social engineer
- WARCART!

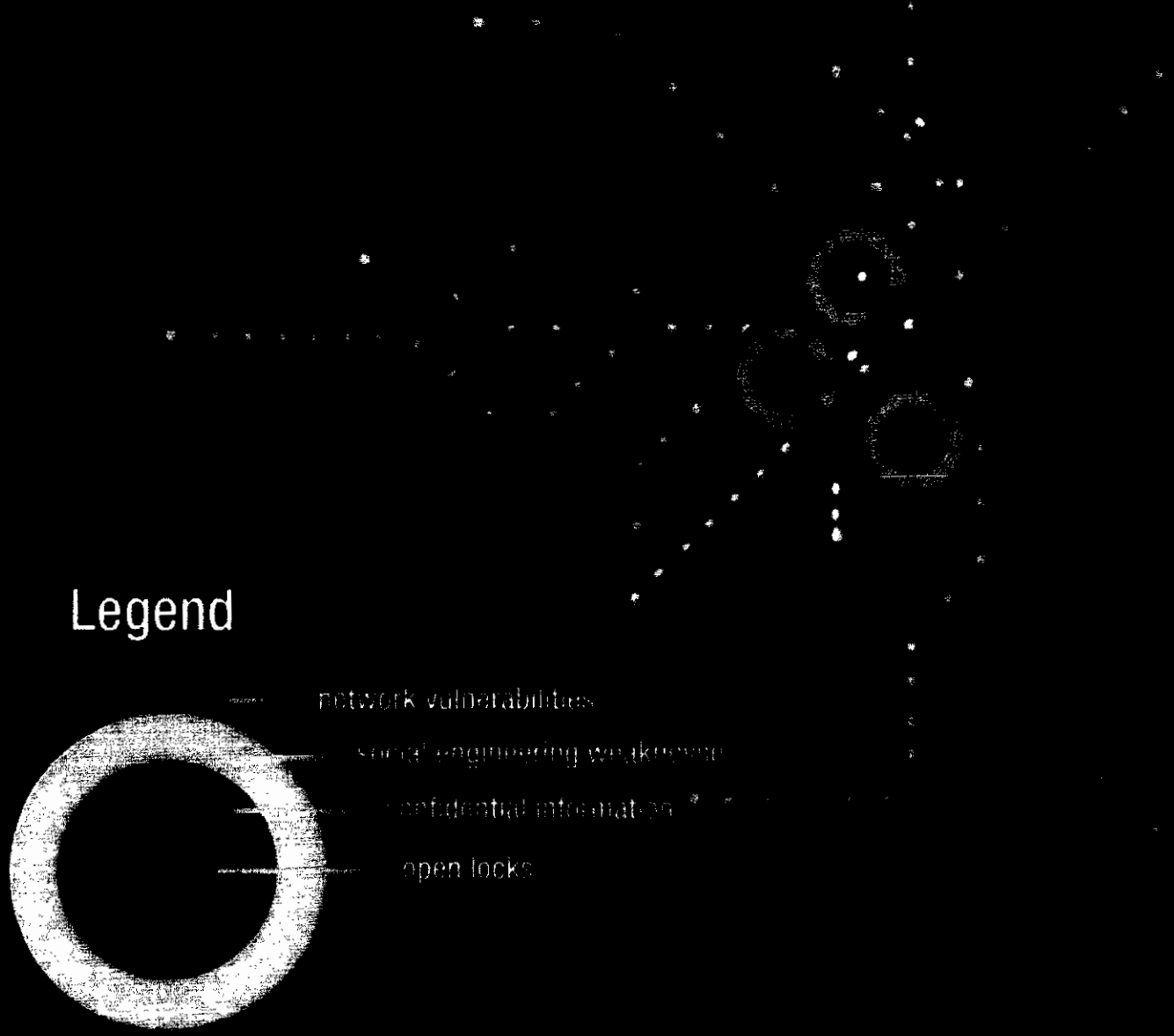
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 5 of 97

AND THIS IS VERY ILLEGAL!

So the following material is for educational use only.

(5)

Boston T System Vulnerabilities



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 7 of 97

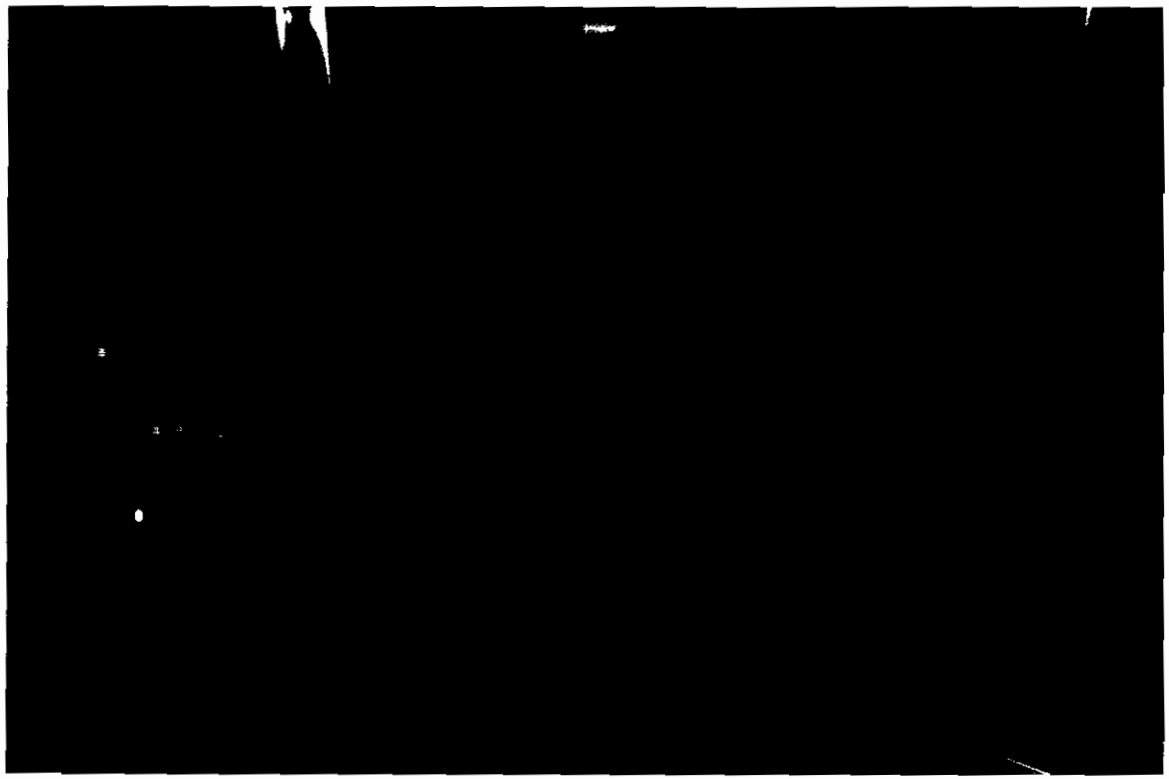


Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 8 of 97

there is almost always a free way to get in

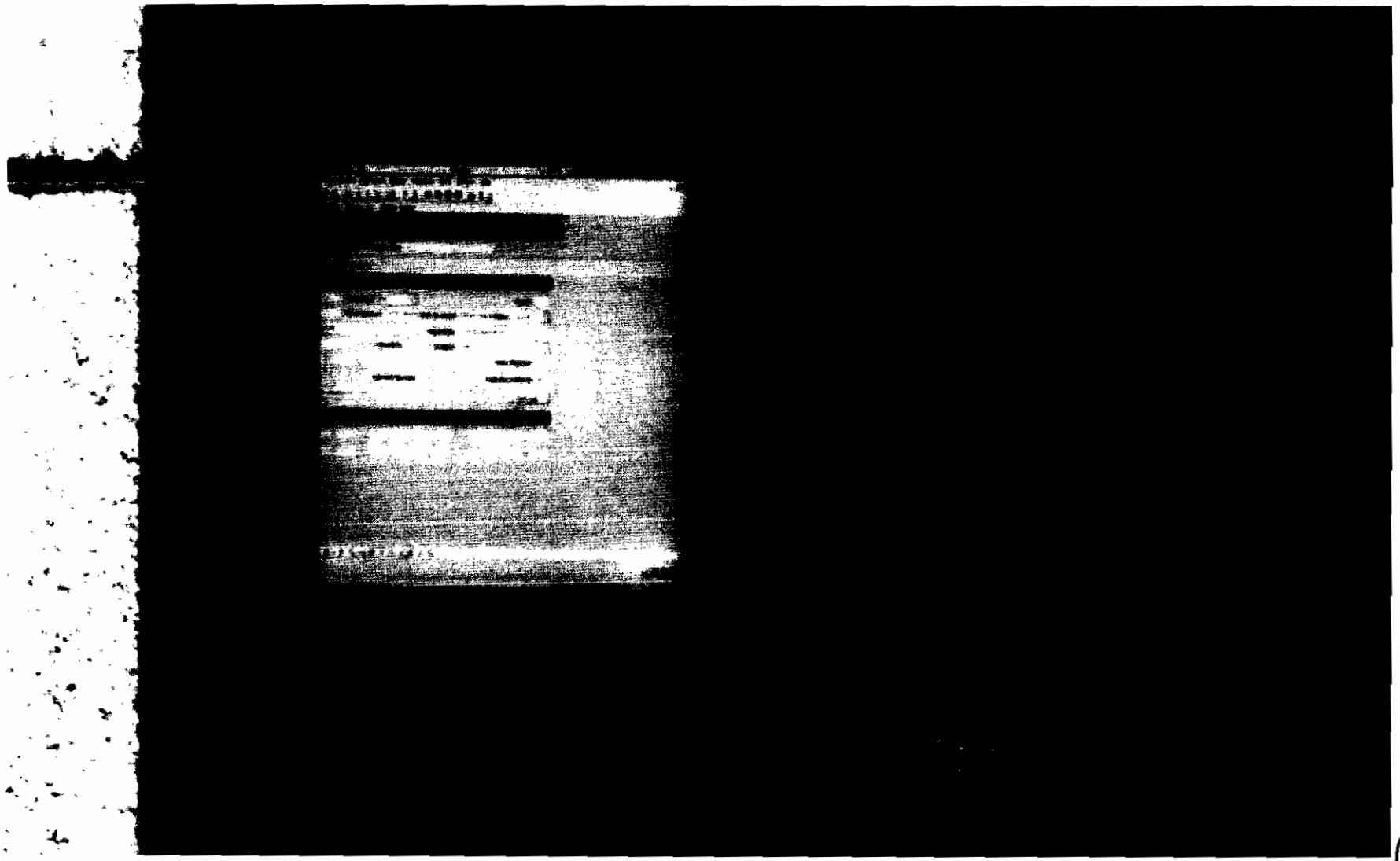
8

turnstile control boxes open... almost everywhere



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 10 of 97

computer screens visible through windows

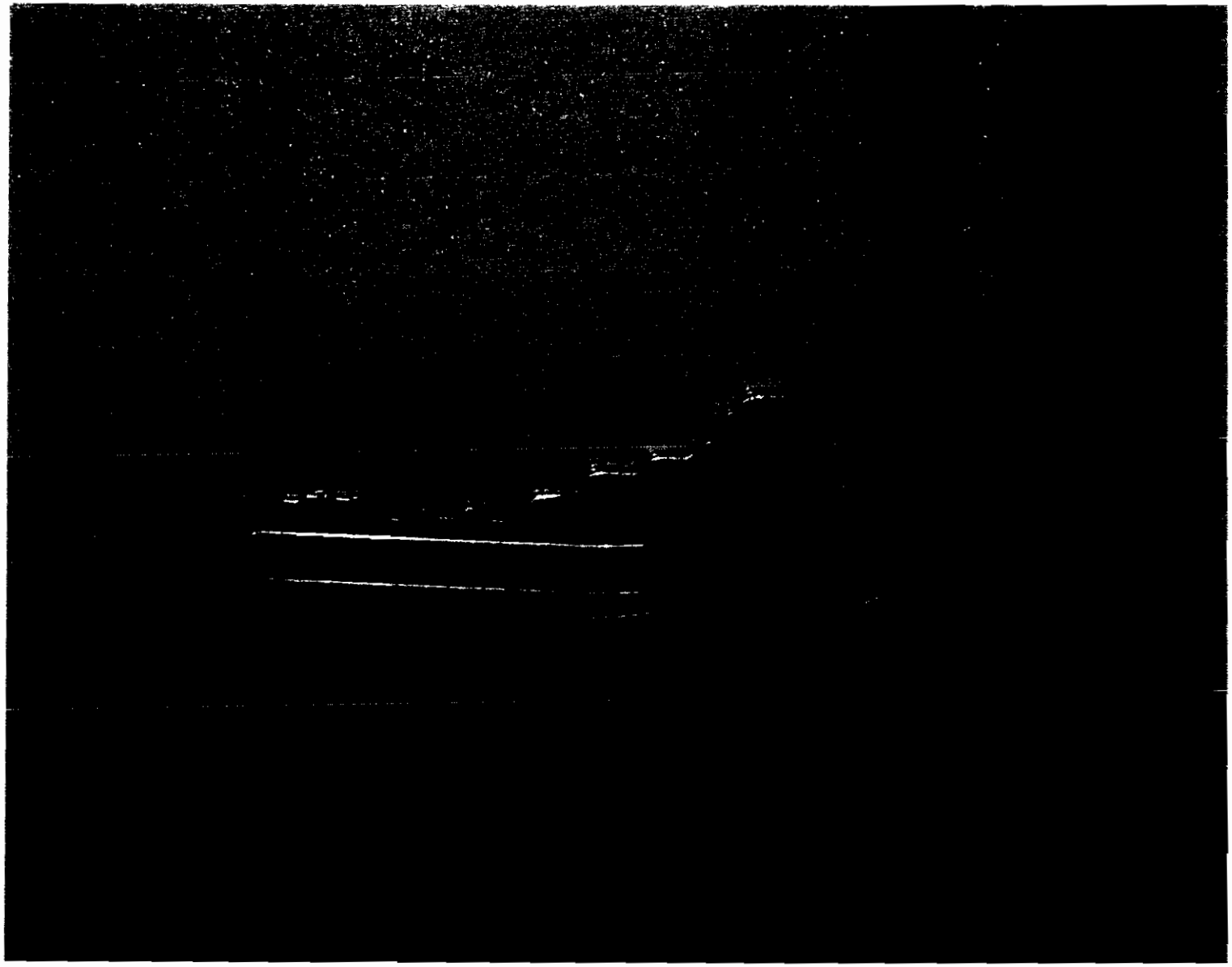


10

11

door keys left in open boxes

door keys left in open boxes



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 13 of 97

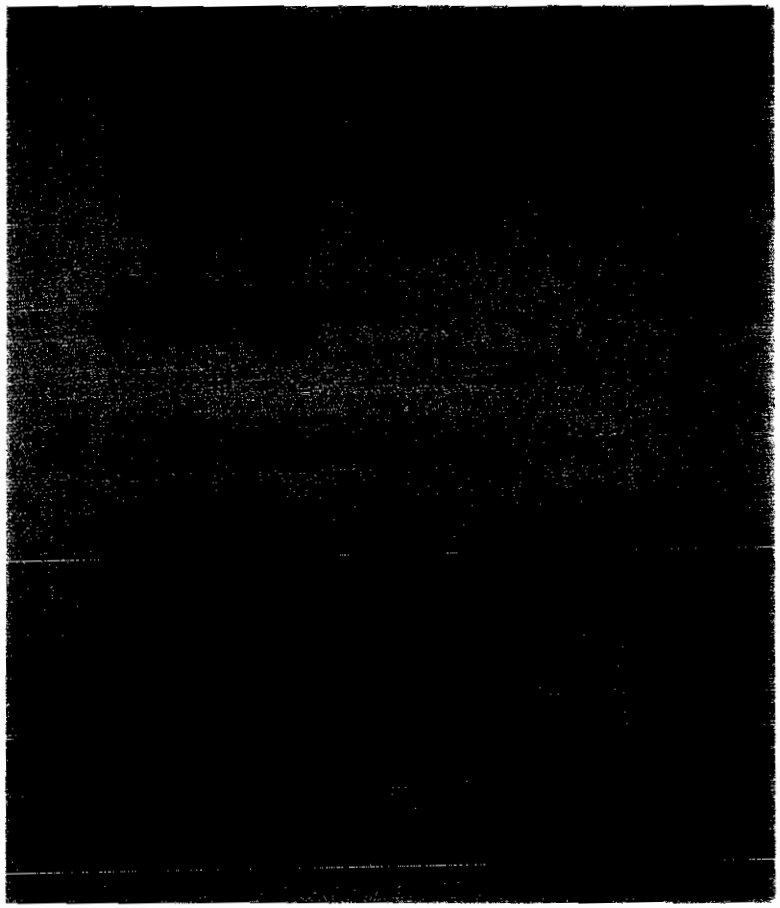
(12)

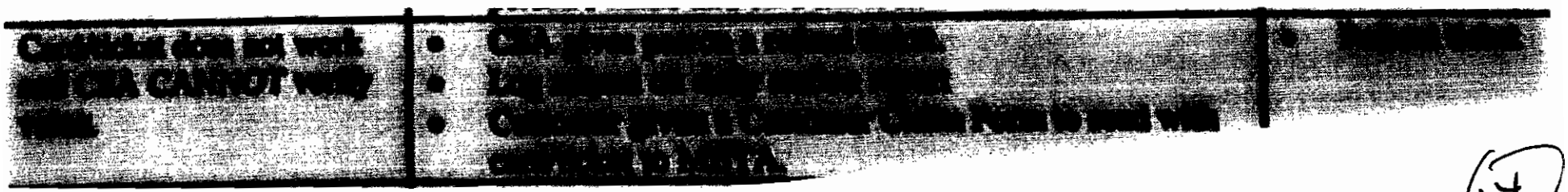
state-of-the-art surveillance... often unattended



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 14 of 97

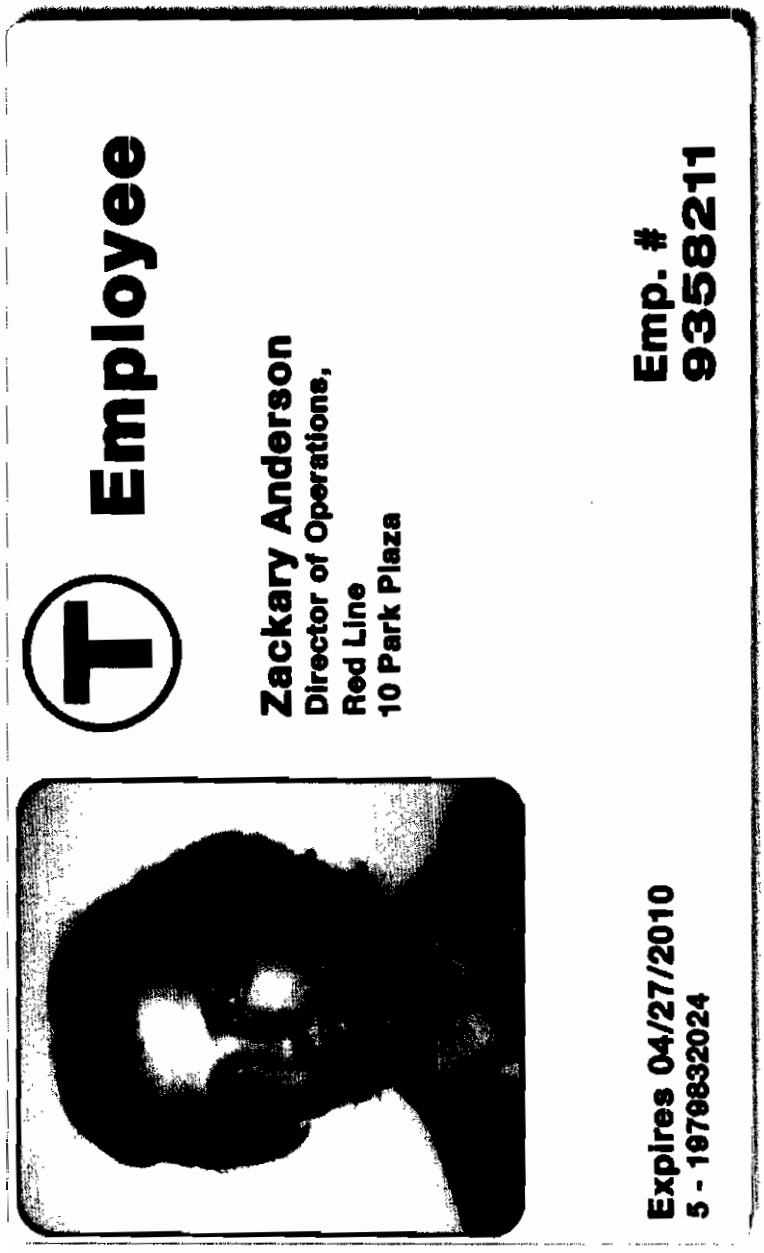
documents left in the open





Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 15 of 97

15


Employee
Zackary Anderson
Director of Operations,
Red Line
10 Park Plaza
Emp. #
9358211
Expires 04/27/2010
5 - 1978832024

ebY Sign in

Categories ▾ Motors Express Stores

Back to list of items Listed in category: Computers & Networking > Printers

Fargo DTC515 Thermal Card Printer

Bidder or seller of this item? Sign in for your status



1 of 2

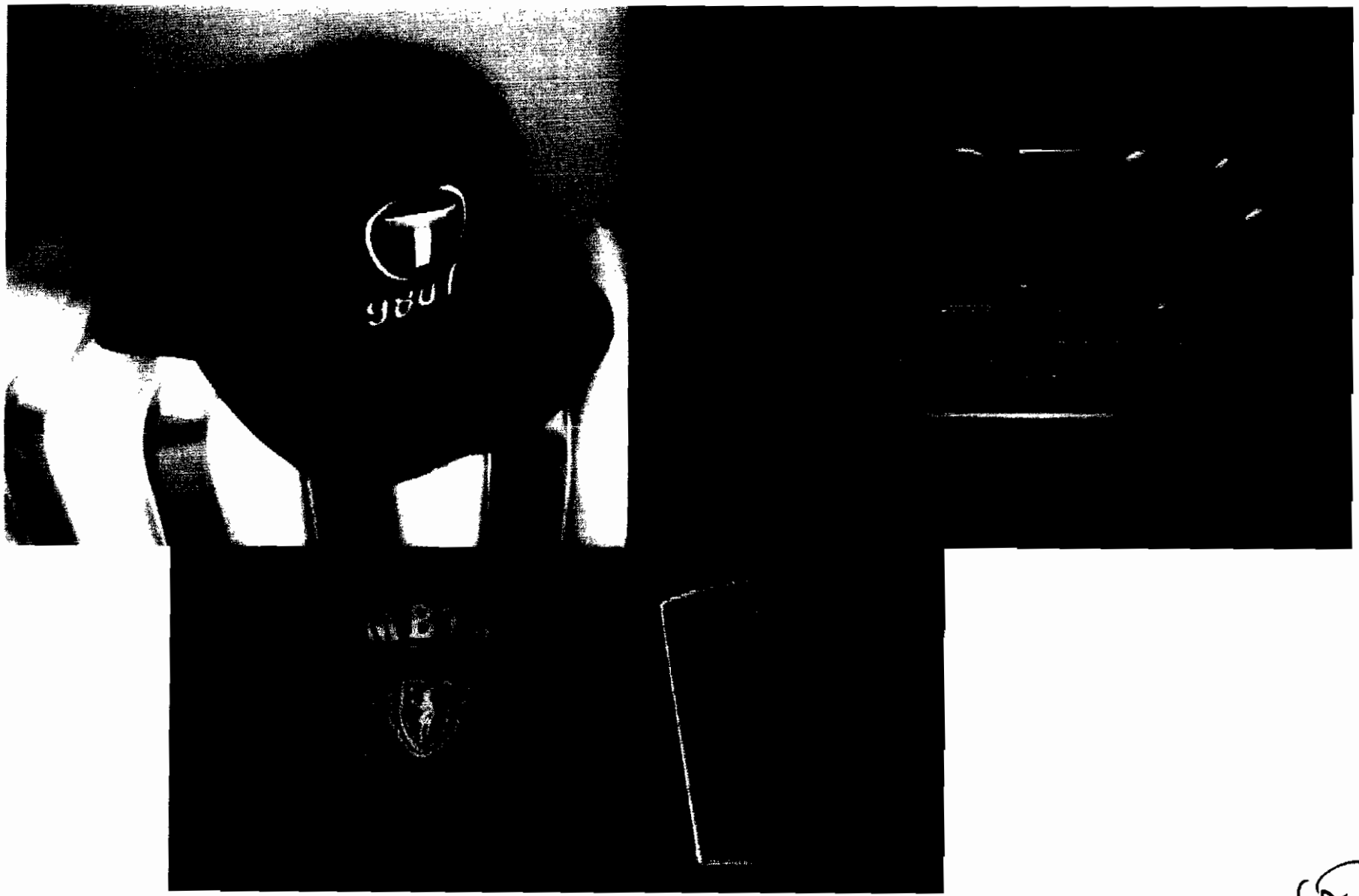
View larger picture

Current bid:	**US $79.99**
Your maximum bid:	**US $** [ ] Place Bid > (Enter US $80.99 or more)
End time:	**Jun-29-08 19:43:35 PDT** (2 days 1 hour)
Shipping costs:	**US $30.12** UPS Ground Service to 02142, United States
Ships to:	United States
Item location:	Minneapolis, Minnesota, United States
History:	1 bid
High bidder:	1***o (804 ★)
You can also:	Watch This Item Get SMS or IM alerts | Email to a friend

16

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 17 of 97

what we found on Ebay



17

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 18 of 97

ATTACK THE MAGCARD

pick the hardware

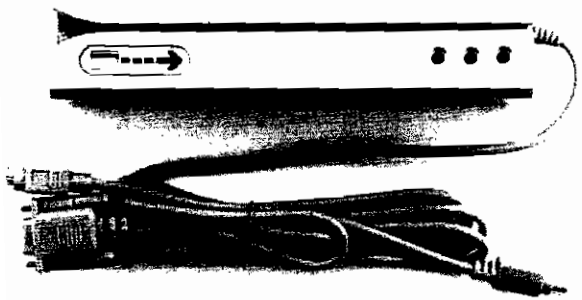


$5<

Homebrew reader

With inserts, can read 3-tracks

stripesnoop.sourceforge.net

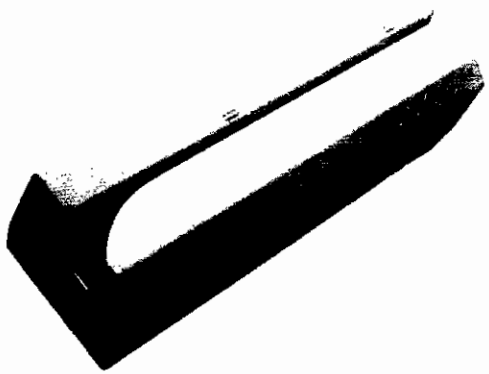


$139.95

Spark Fun Electronics

3-Track Lo-Co

Includes source code



$300

MSR206 or MAKStripe

3-Track Hi/Lo-Co

Works with our GPL'd software

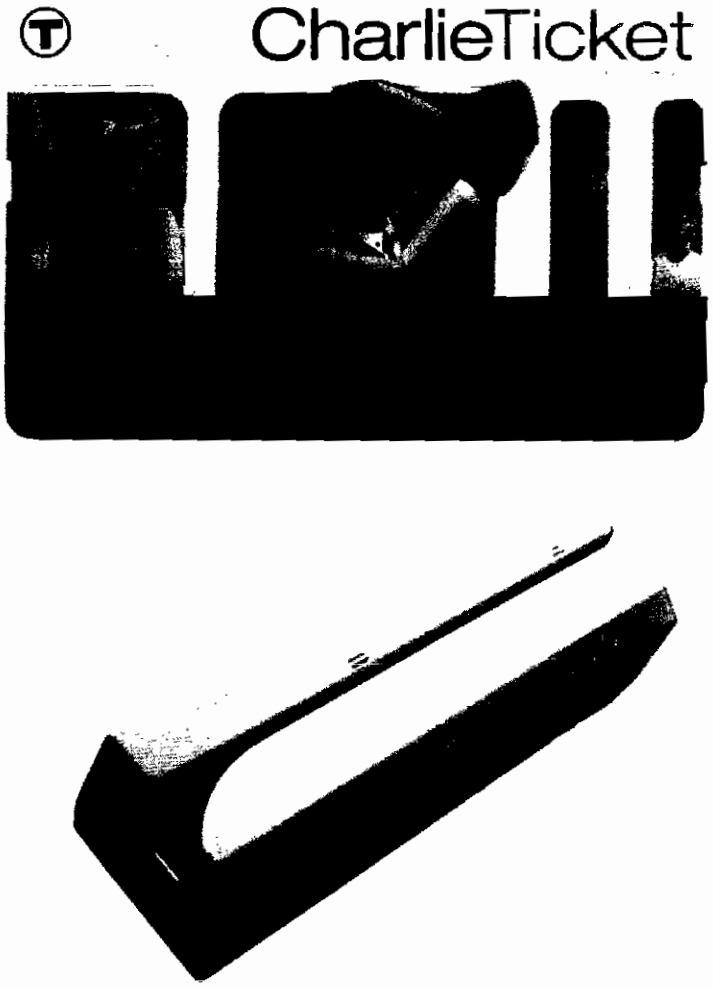
20

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 21 of 97

12



CharlieTicket



EC9010402AC9D000000005B800C80150342248A
84EBD132BE10280002000000002025D0000FD60

23

Is value stored on the card?

try a cloning attack

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 25 of 97

If yes, then

you now have free subway rides for life

24

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 26 of 97

Oh,

but you want more than that, eh?

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 27 of 97

reverse engineering

The Charlie Ticket

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 28 of 97

reverse engineering

Everybody talks about it,
But where do you start?

1) Make a guess about what's in the data
2) Change a single variable; see what changes
3) Repeat many times with varying data
4) Compare similar and dissimilar data
5) Ignore constant regions
6) Build/use tools

27

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 29 of 97

reverse engineering

Isolate Variables method

To locate a single variable:

- Group data by that variable
- Ignore global similarities (between different groups)
- Ignore differences within groups

Resulting locations are probably where the data is stored

28

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 30 of 97

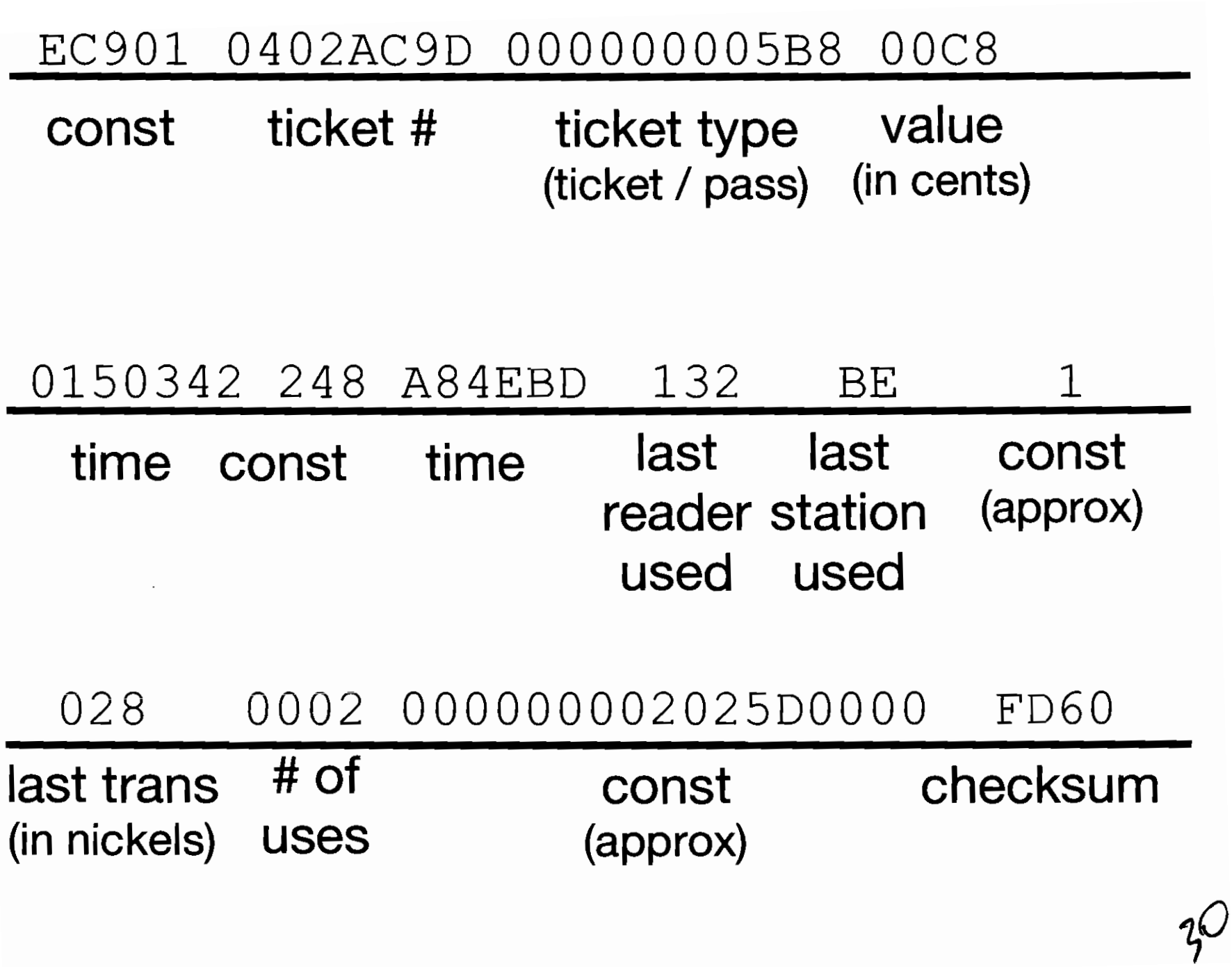
EC901 0402AC9D 000000005B8 00C8

0150342 248 A84EBD 132 BE 1

028 0002 000000002025D0000 FD60

29

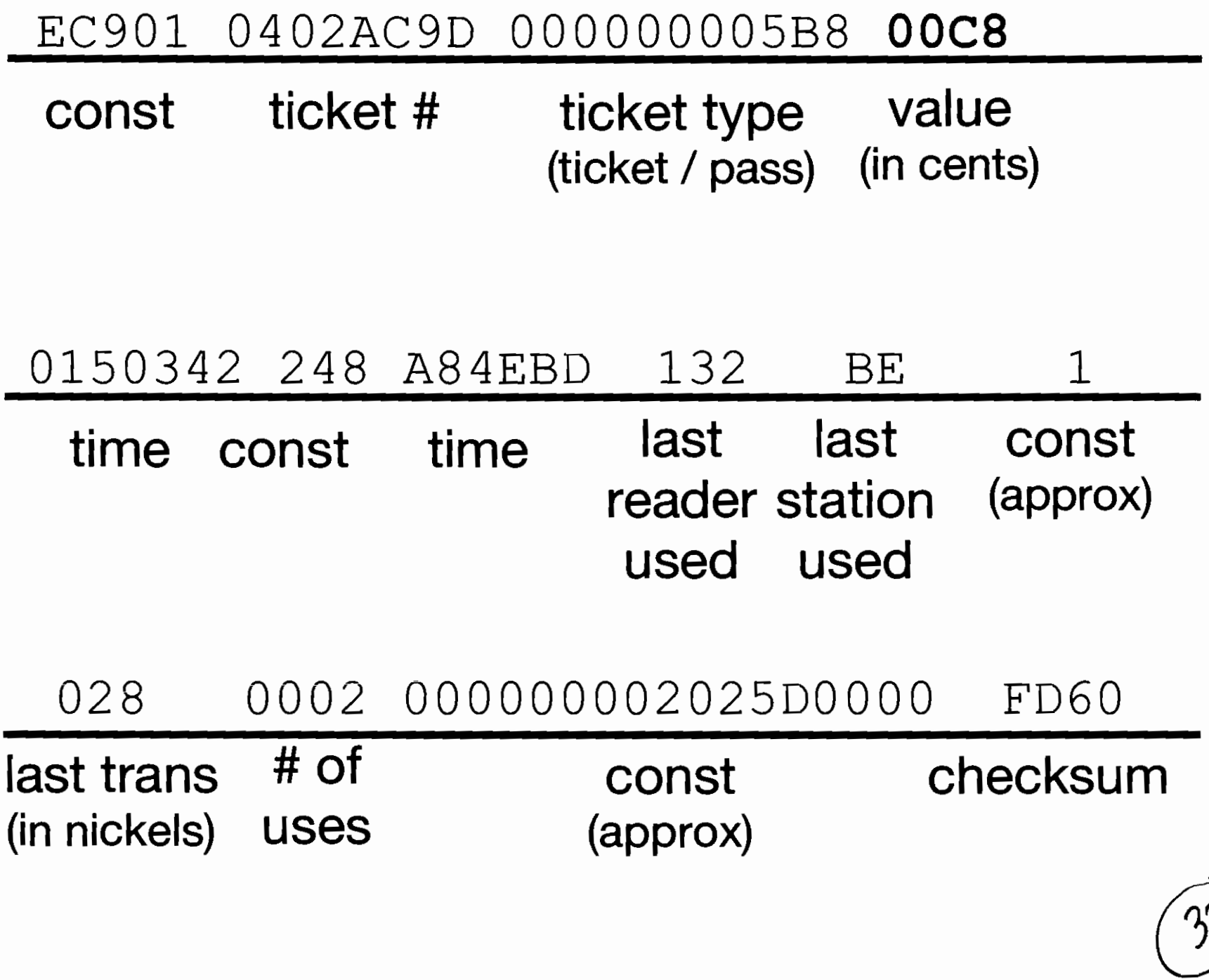
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 31 of 97



30

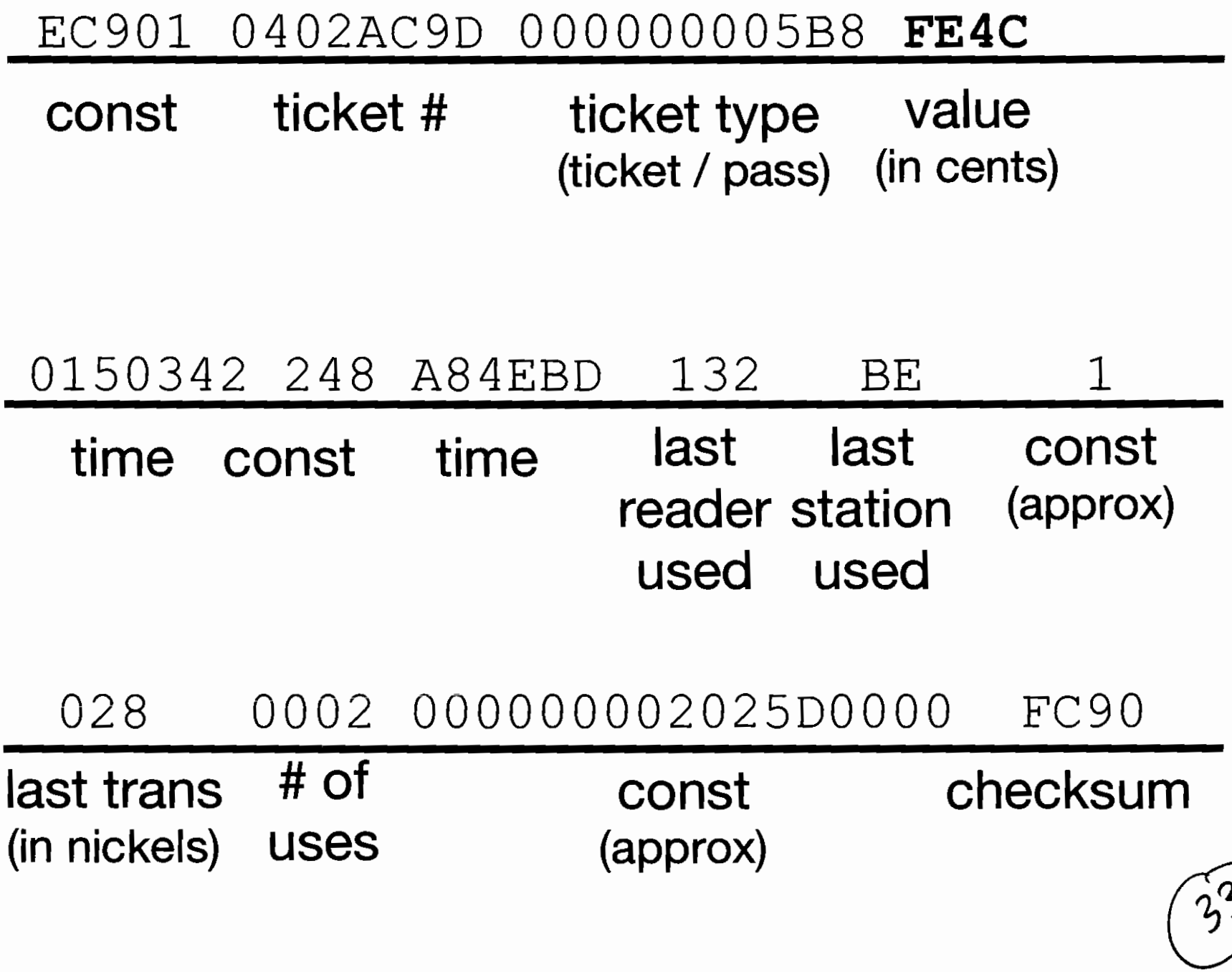
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 32 of 97

forging
The Charlie Ticket

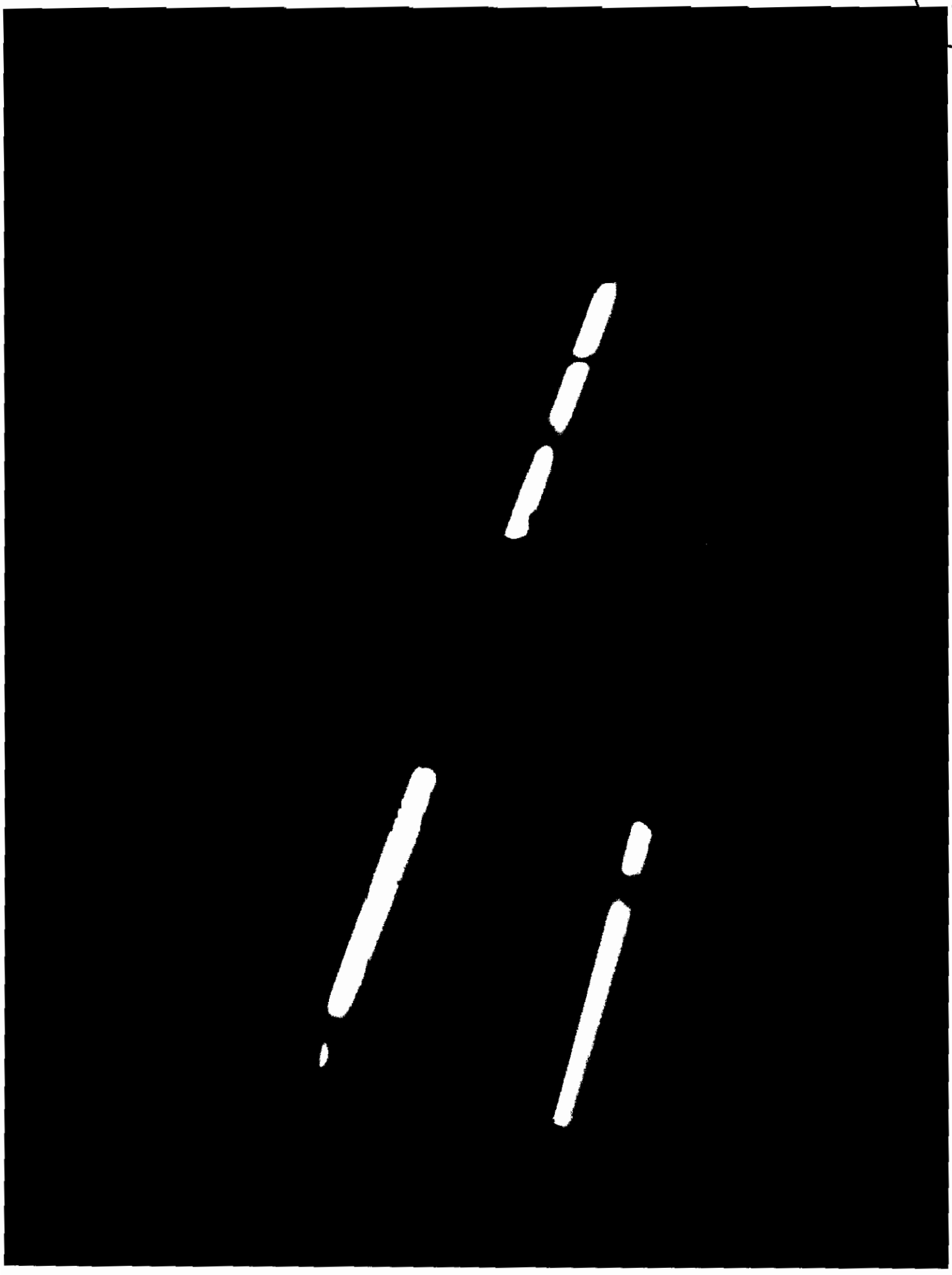


32

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 34 of 97



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 35 of 97



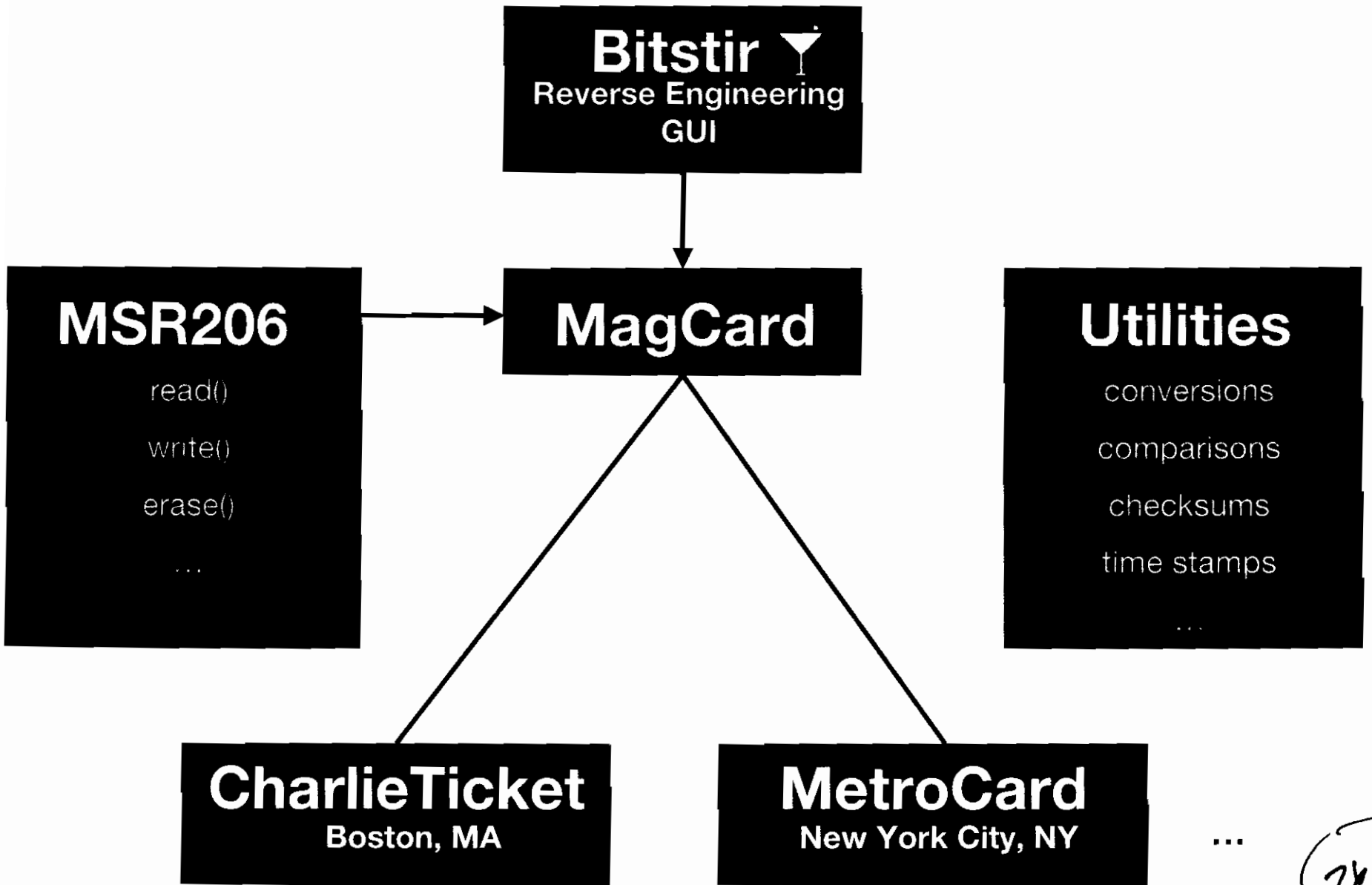
Stored Value
CharlieTicket
Hybrid the surcharge
a CharlieCard. Ask for
into or visit mbta.com
Initial Value = 100.00
Ticket-No: 1 - 07
Cash
06/29/2008 06:45 PM
Subject to applicable tariff regulations and conditions
of use. Ticket may be confiscated for misuse.
Not replaceable if lost or stolen. Non-refundable.
100.00
Kendall/ MIT
Dec/ice: 20114
Schedule & Fare Information: 617-222-3200 Website: www.mbta.com © MBTA
Massachusetts Bay Transportation Authority

=

+

E9
ADULT
Stored Value
NOT VALID
OR TRANSFER
Initial Value = 1.25
Ticket-No: 1 - 0342
Cash
08/25/2006 01:
Subject to applicable tariff regulations and conditions
of use. Ticket may be confiscated for misuse.
Not replaceable.
1.25
Kendall/ MIT
Dec/ice: 20114
Schedule & Fare Information: 617-222-3200 Website: www.mbta.com © MBTA
Massachusetts Bay Transportation Authority

MagCard Reverse-Engineering Framework



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 38 of 97

Demo: MagCard and Reverse Engineering Toolkit

- wrote Python libraries for analyzing magcards
- integrated with the MSR206 reader/writer
- GUI helps visualize and organize data



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 39 of 97

what about other subways?

- Most subway fare collection systems in US are made by two major integrators

- **Scheidt & Bachmann** made Boston T, San Francisco Bart, Long Island Railroad, Seattle Sound Transit, London Silverlink, etc. systems
- **Cubic Transportation** made NYC MTA, Washington DC WMATA, Chicago CTA, Shanghai Metro, etc. systems

Are they hackable? Yes!

38

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 40 of 97


ATTACK
THE
RFID

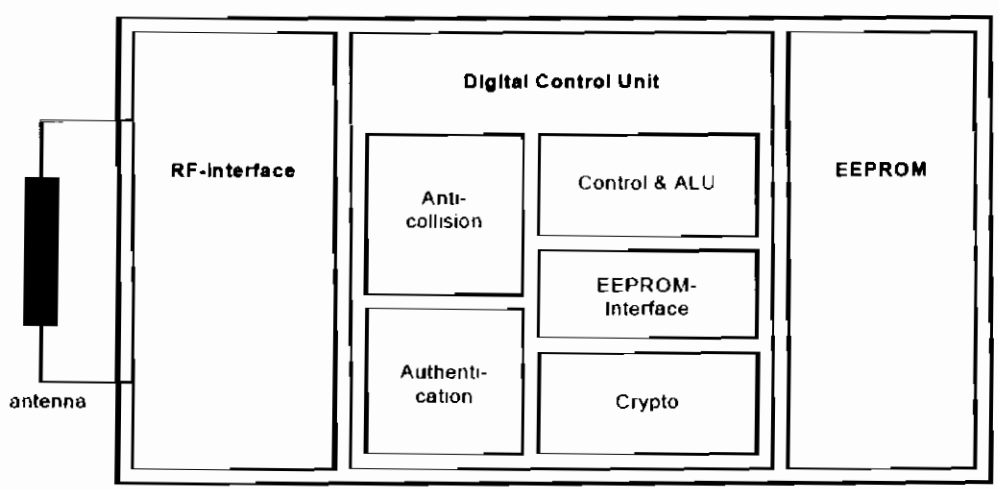
learn about your RFID card

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 42 of 97

40

MIFARE Classic

- 13.56MHz RFID smartcard
- End-to-end proprietary “crypto” (Crypto-1)
- 1K memory & unique identifier on card
- Over 500 million tags in use



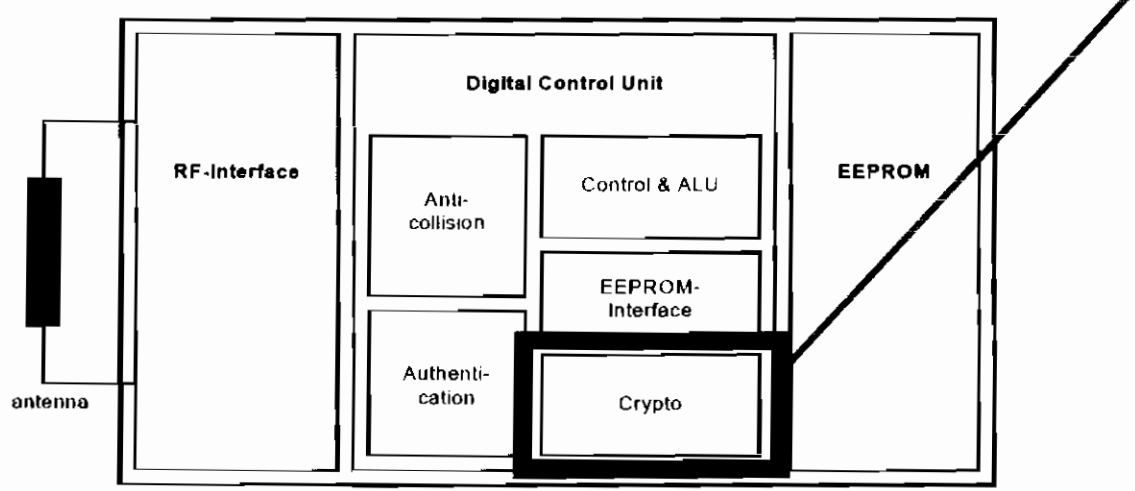
41

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 43 of 97

Crypto-1 Cryptanalysis

Crypto-1 reverse engineered by Karsten Nohl, University of Virginia, 2007:

- Etched and inspected silicon wafer using high-powered imagery.
- Found and reconstructed crypto portions from over 10k gates.
- Found vulnerabilities in the cipher and implementation

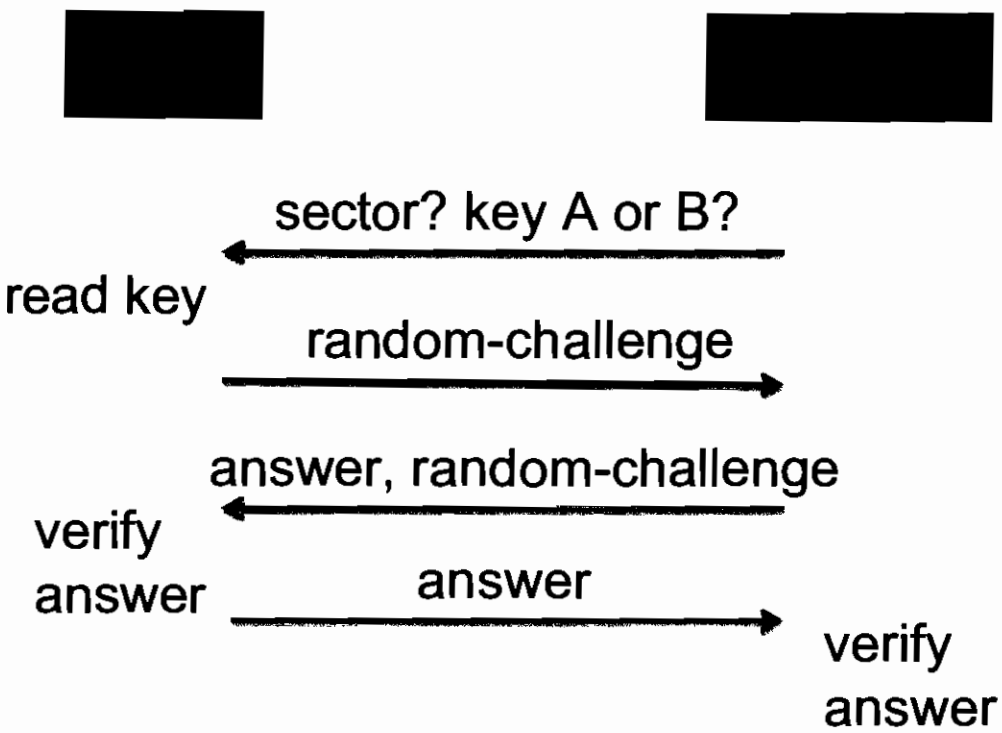


42

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 44 of 97

security of the MIFARE card

Mutual 3-pass authentication



Each sector two keys

Non-linear filter functions

43

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 45 of 97

security of the MIFARE card

Mutual 3-pass authentication

[redacted] [redacted]

sector? key A or B?

read key

random-challenge

answer, random-challenge

verify answer

answer

verify answer

[redacted]

Non-linear filter functions

44

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 46 of 97

security of the MIFARE card

[redacted]

[redacted]

[redacted]

Non-linear filter functions

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 47 of 97

security of the MIFARE card

[redacted]

[redacted]

[redacted]

[redacted]

46

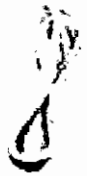
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 48 of 97

to execute these attacks we need to interact with the card

choose your hardware

47

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 49 of 97

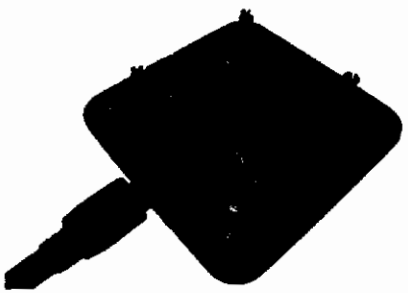


$50

MiFare RFID Reader/Writer

Comes with source code

Hard to hack, but doable

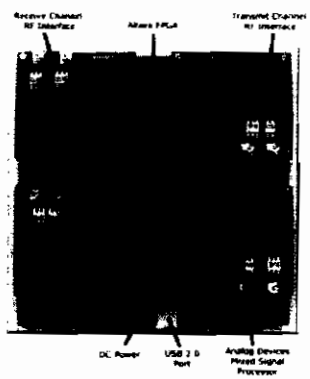


$220

OpenPCD + OpenPICC

Open design 13.56MHz RFID reader + emulator

Free schematics (www.openpcd.org)



$700

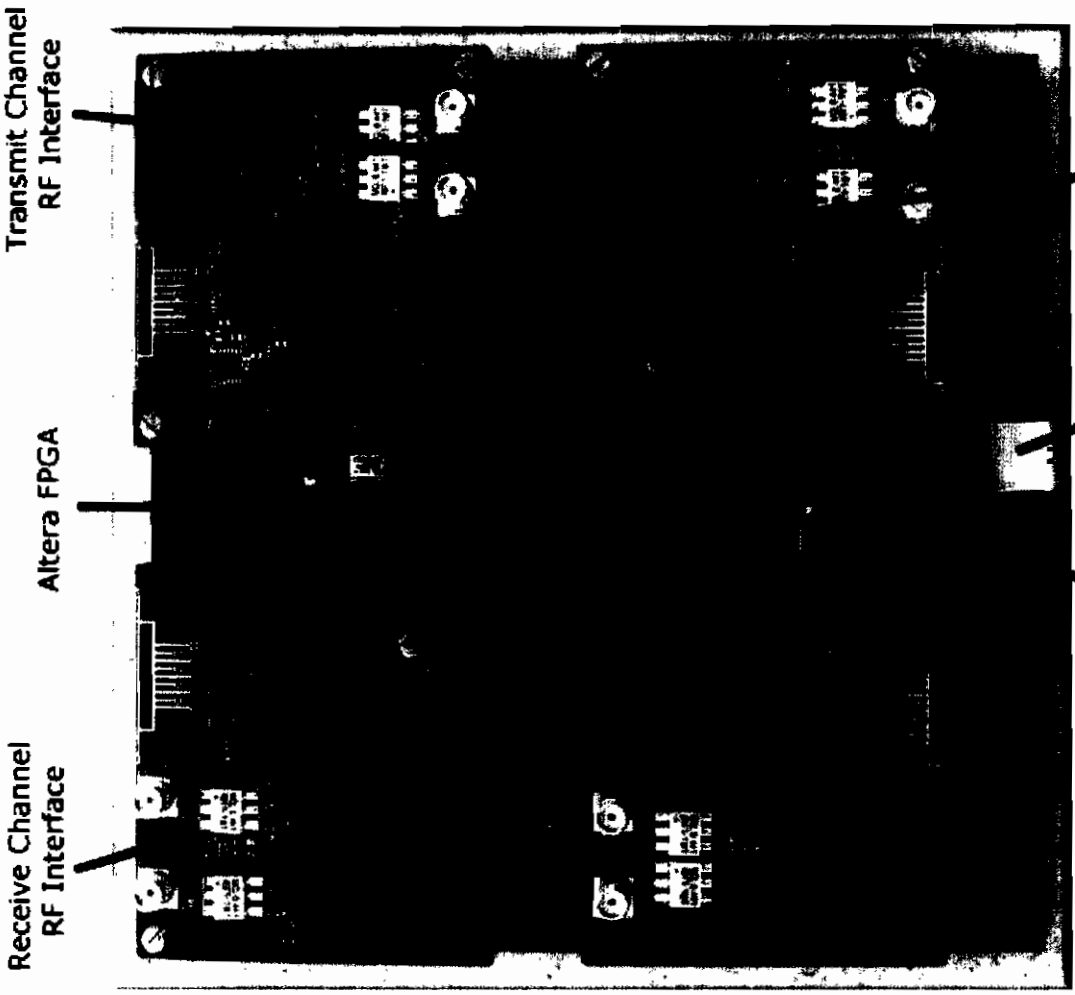
USRP

Full control over signal input/output

Works with GNU Radio + our plugin

48

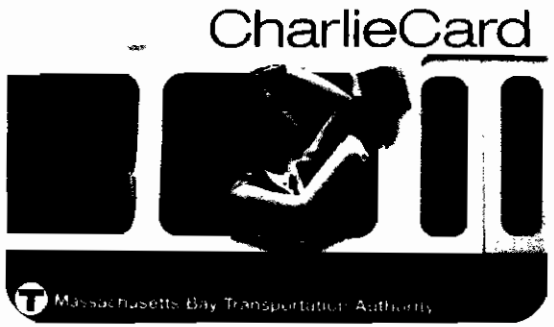
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 50 of 97


Transmit Channel
RF Interface
Altera FPGA
Receive Channel
RF Interface
Analog Devices
Mixed Signal
Processor
USB 2.0
Port
DC Power

USRP

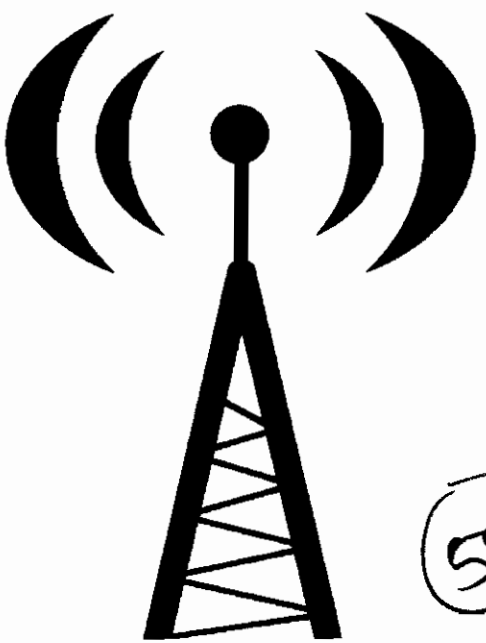
49

card/reader communication



13.56MHz
ASK modulation
Modified miller encoding

13.56MHz
+/- 847kHz
OOK modulation
Manchester encoding



50

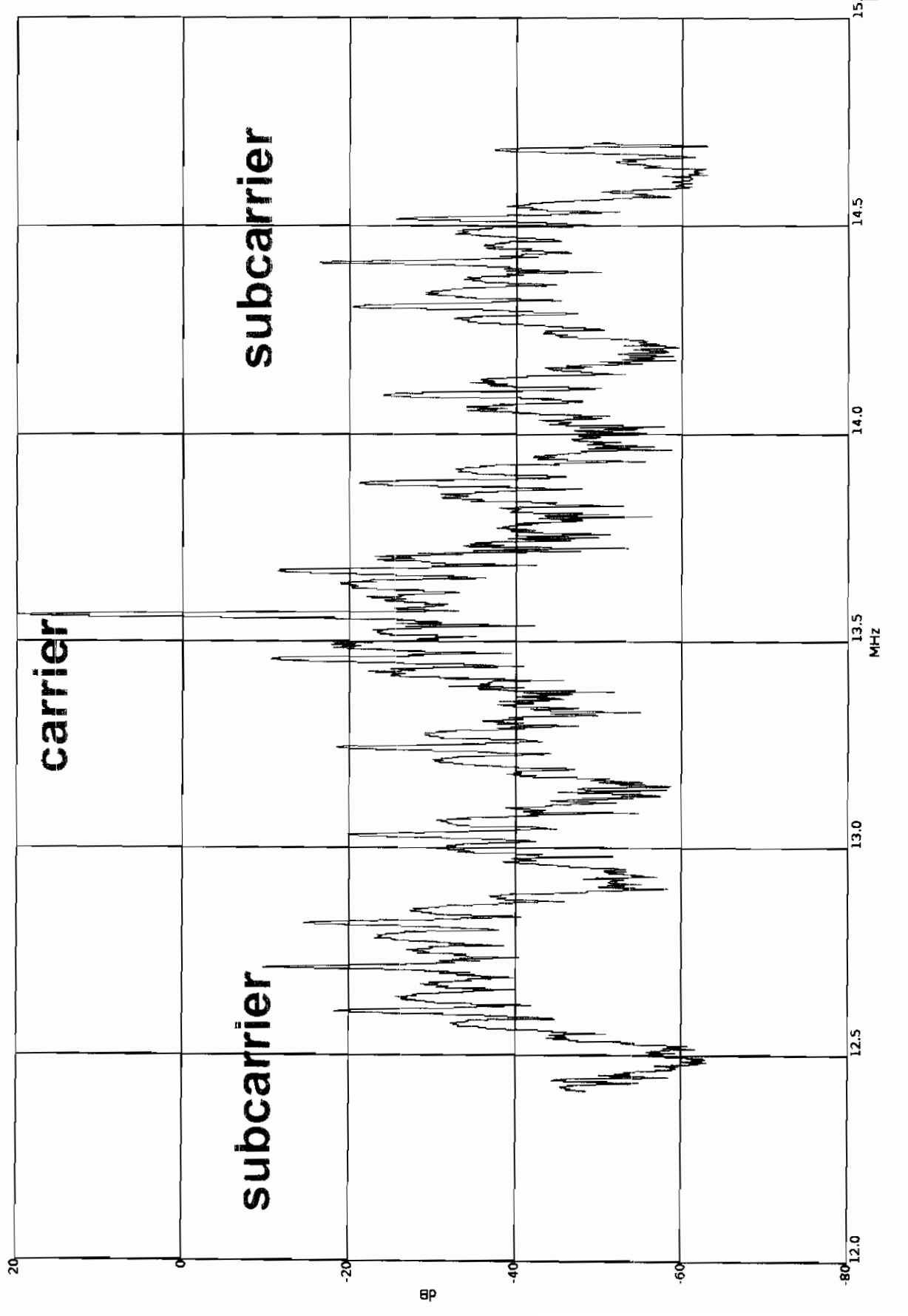
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 52 of 97

GNU radio RFID toolchain

Tune Radios

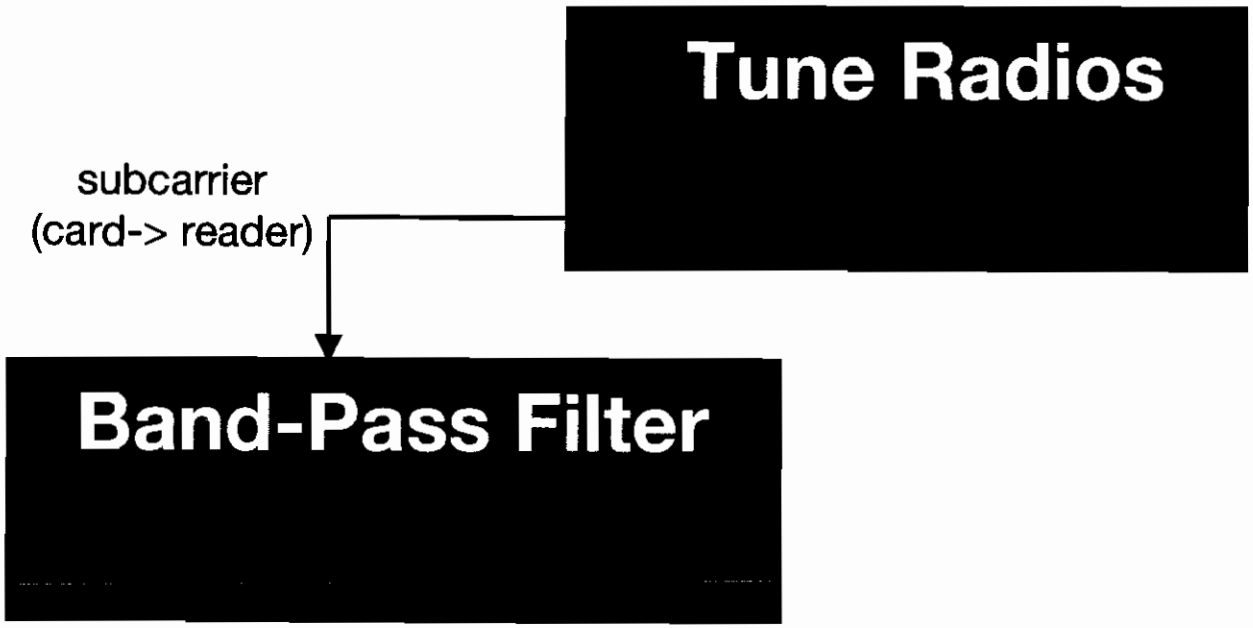
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 53 of 97

charlie card + reader FFT



52

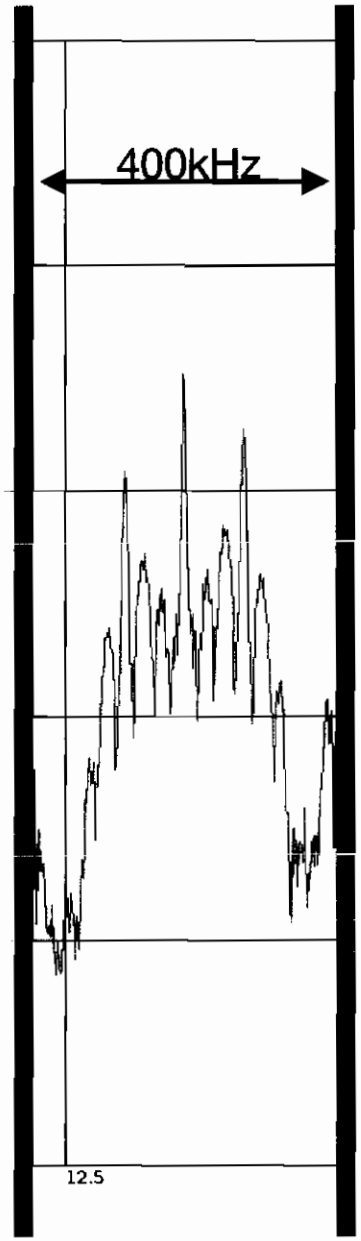
GNU radio RFID toolchain



53

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 55 of 97

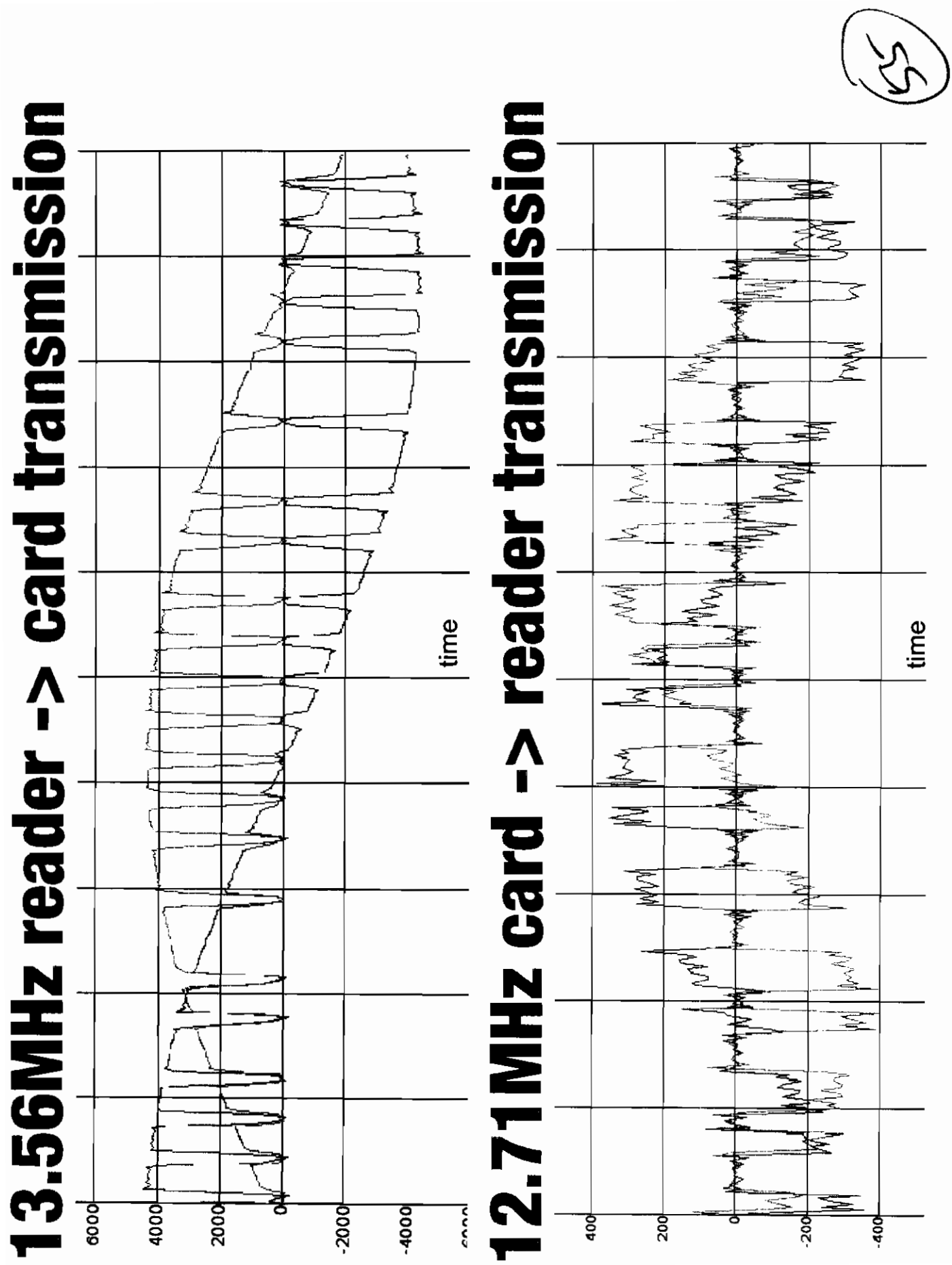
charlie card + reader FFT



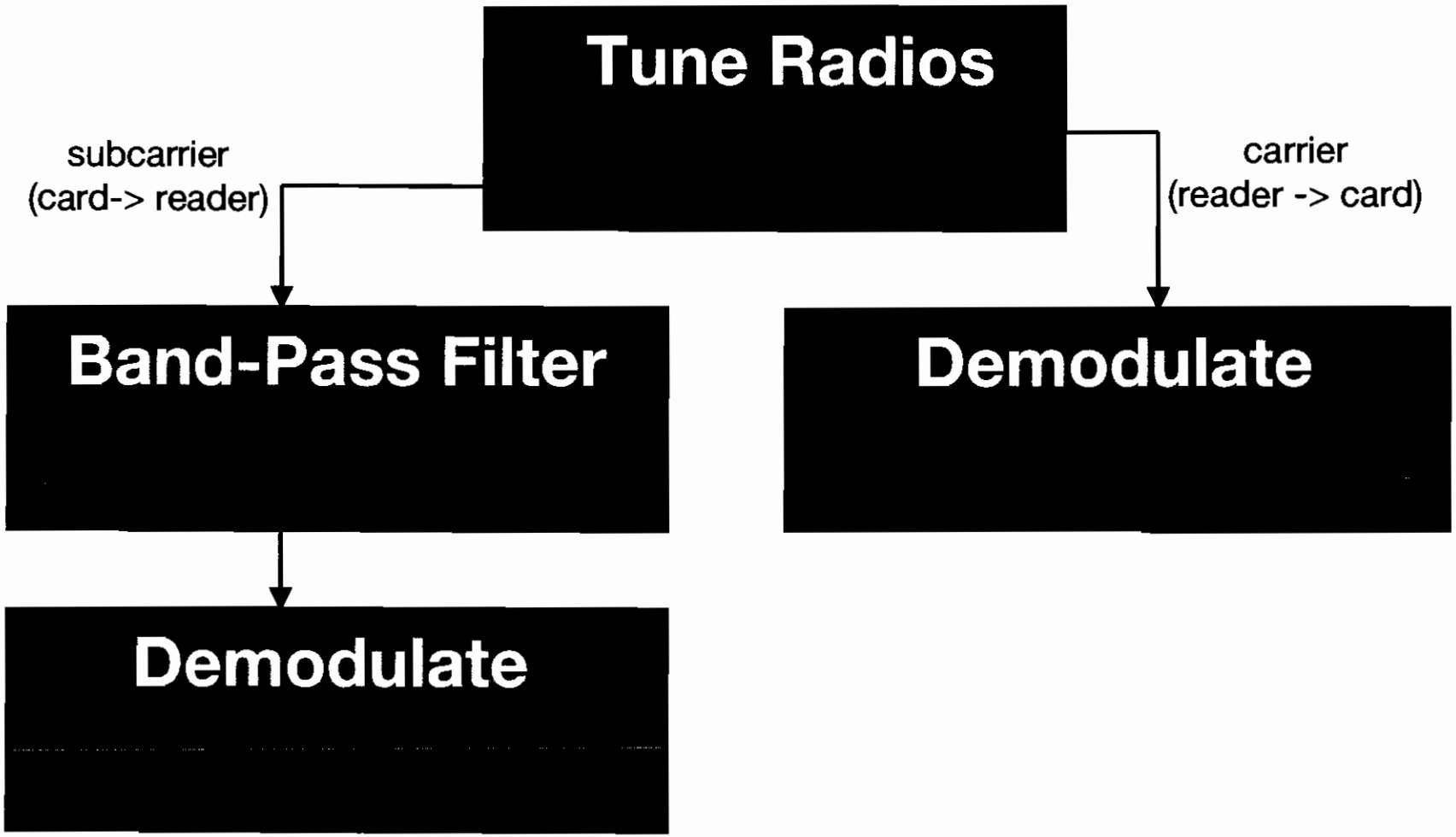
Band Pass Filter

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 56 of 97

54


13.56MHz reader -> card transmission
6000
4000
2000
0
-2000
-4000
time
12.71MHz card -> reader transmission
400
200
0
-200
-400
time

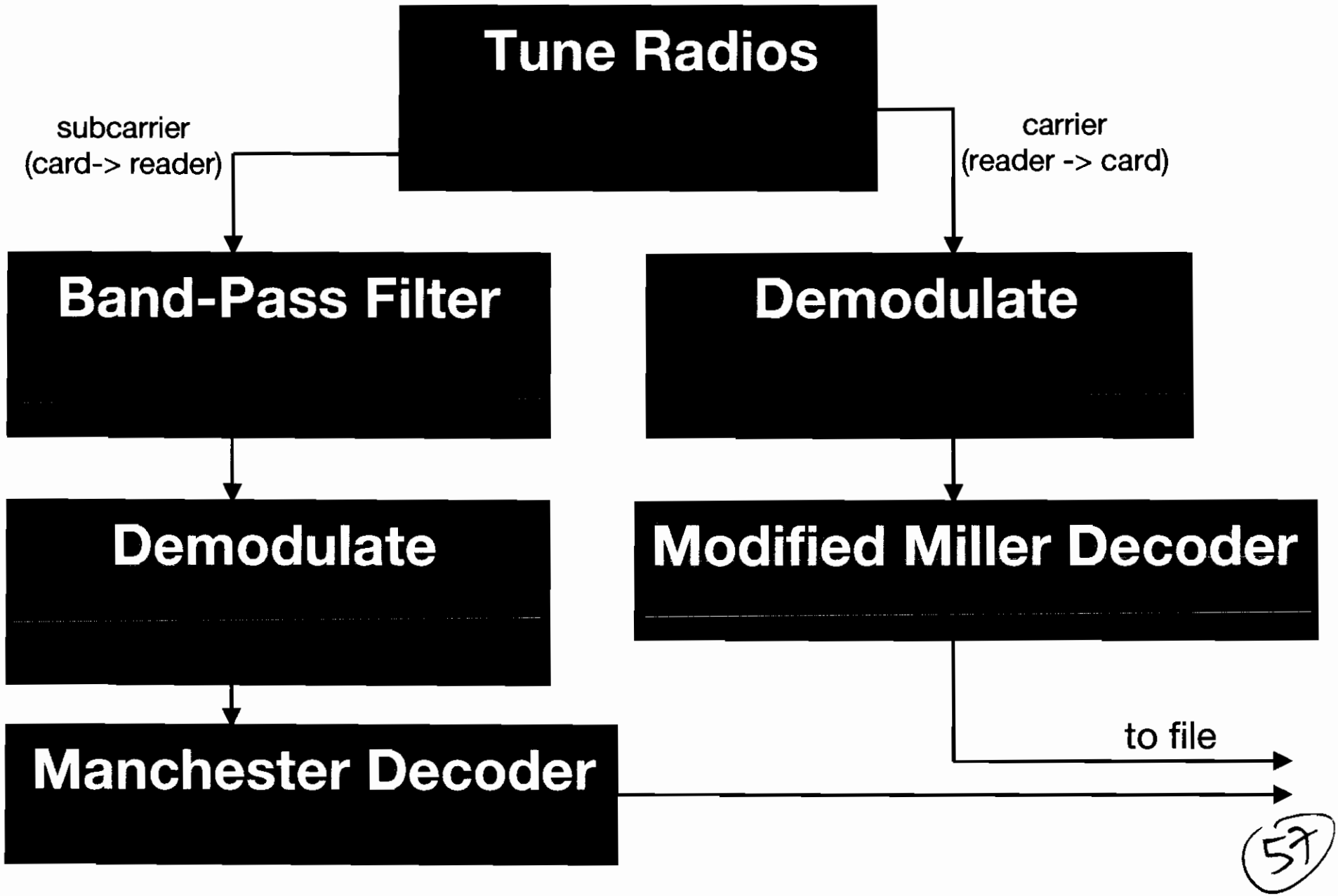
GNU radio RFID toolchain



56

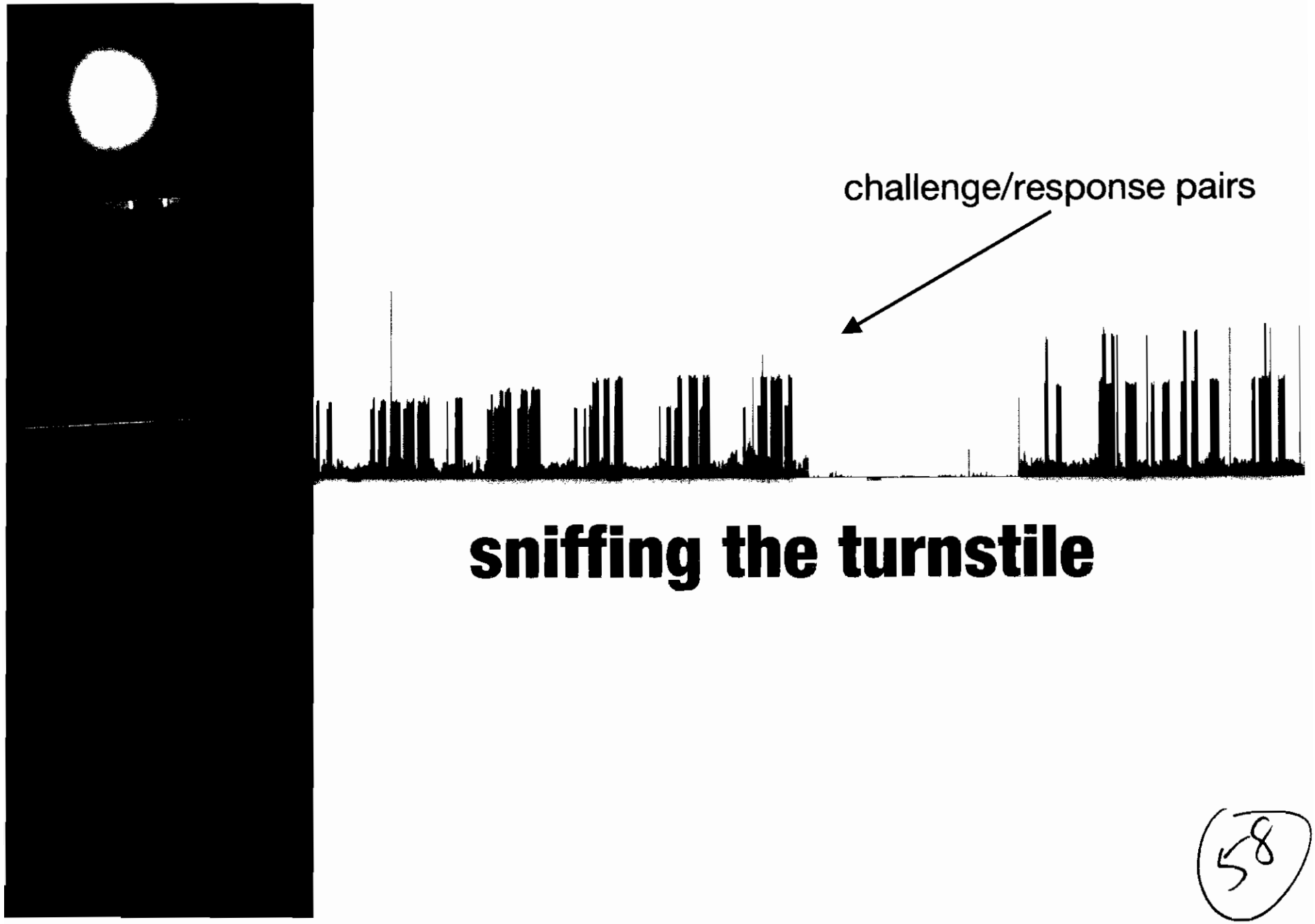
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 58 of 97

GNU radio RFID toolchain



57

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 59 of 97



sniffing the turnstile

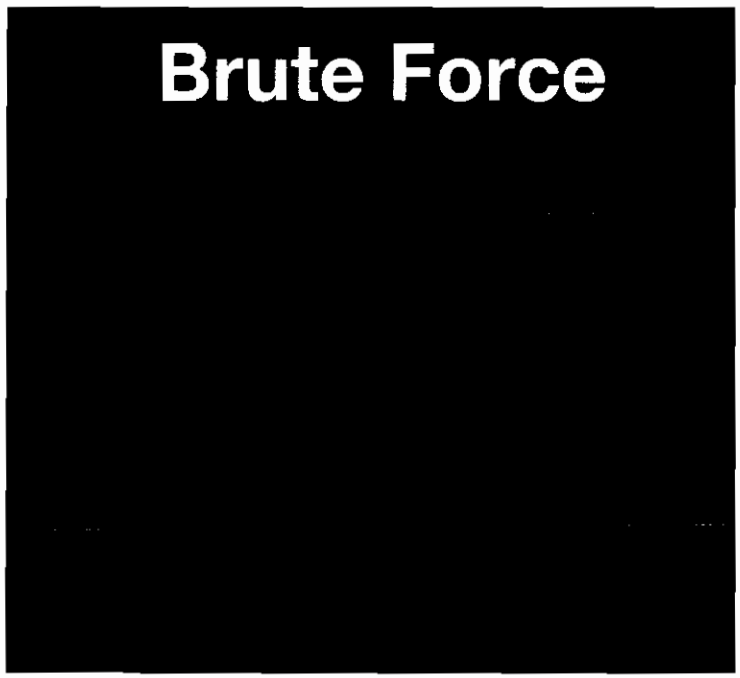
58

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 60 of 97

attacks on the MIFARE card

Goal: get secret key (can clone card with it)

Brute Force



59

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 61 of 97

attacks on the MIFARE card

Goal: get secret key (can clone card with it)

Brute Force

[redacted]

Manipulate PRG Timing

[redacted]

60

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 62 of 97

attacks on the MIFARE card

Goal: get secret key (can clone card with it)

Brute Force

Manipulate PRG Timing

Algebraic Attacks

61

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 63 of 97

when all else fails

brute force it

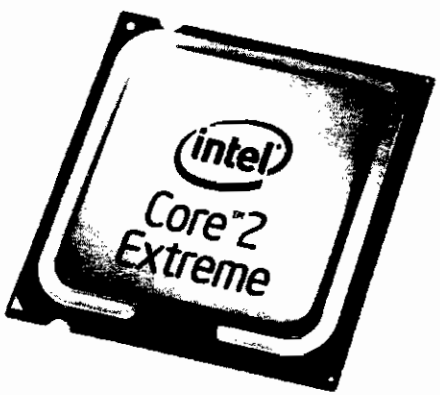


Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 64 of 97

Why Brute Force with an FPGA?

Because it's fast!

microprocessor



- General purpose device
- Finite instruction set
  (Uh, oh. Sounds RISCy)
- 1-8 parallelizations

FPGA



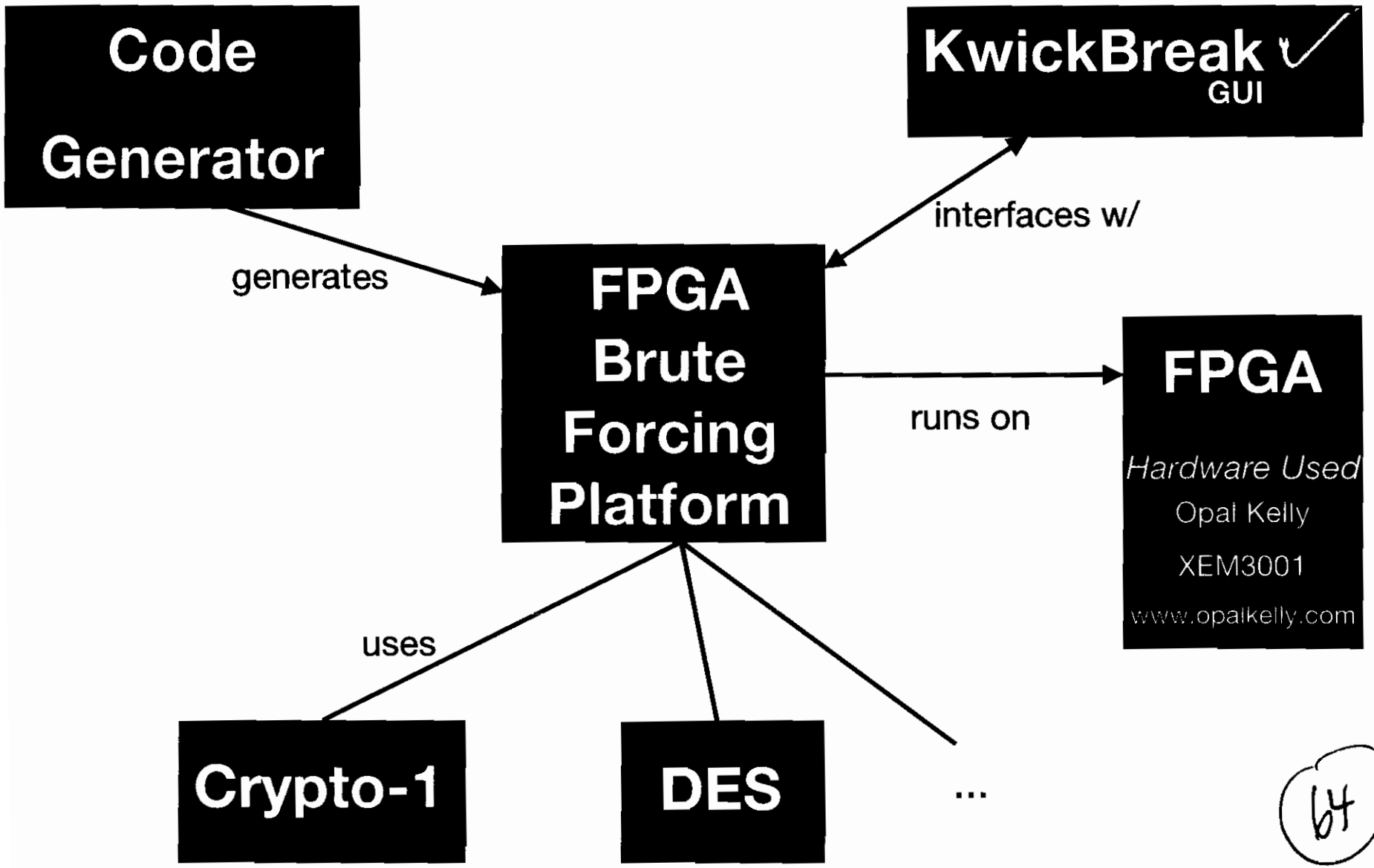
- Dedicated logic
- Hardware description language defines hardware
- Hundreds of parallelizations

63

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 65 of 97

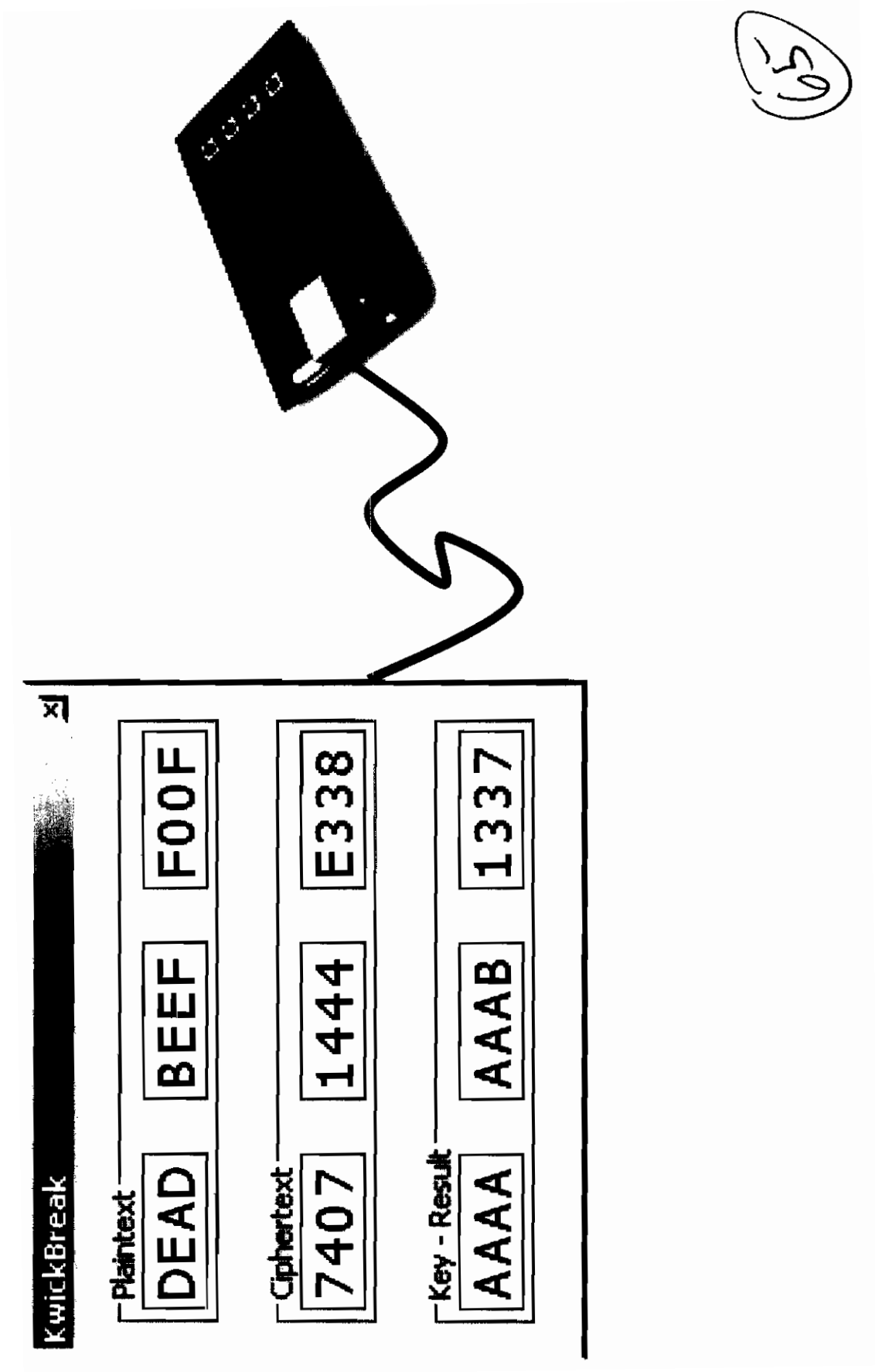
KwickBreak FPGA Brute-Forcer

Executes known plaintext attack to recover key



64

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 66 of 97


KwickBreak
Plaintext
DEAD
BEEF
F00F
Ciphertext
7407
1444
E338
Key - Result
AAAA
AAAB
1337

writing a (trivial) XOR module

```
module xorPlugin(
        input  wire clk,
        input  wire [47:0] key,
        input  wire [47:0] plaintext,
        output reg [47:0] encrypted,
        output reg ready);

always @(posedge clk) begin
        ready <= 1;
        encrypted <=  key ^ plaintext;
end
endmodule
```


Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 68 of 97

writing a (trivial) XOR module (cont)

./kwickbreakGenerator.py
>>>
Please enter your plugin module name, as written.
xorPlugin
Output filename (and path)
xorBruteForceUtil.v
How many cores would you like on the chip?
50
If you have a pipelined design, how many clock delays for valid data?
0
xorBruteForceUtil.v successfully written!

Now just create a new project in Xilinx ISE,
load the files, and synthesize

Done!

67

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 69 of 97

Subways using MiFare Classic

- Boston (CharlieCard)
- London (Oyster Card)
- Netherlands (OV-Chipkaart)
- Minneapolis
- South Korea (Upass)
- Hong Kong
- Beijing
- Madrid (Sube-T)
- Rio de Janeiro (RioCard)
- New Delhi
- Bangkok

and more

68

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 70 of 97



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 71 of 97

network security

- Performed site surveys of T stations and offices (no WiFi found)
- Performed wireless device audit
- Found unguarded network switches

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 72 of 97

fiber switches in unlocked room

connect fare vending machines to the internal network

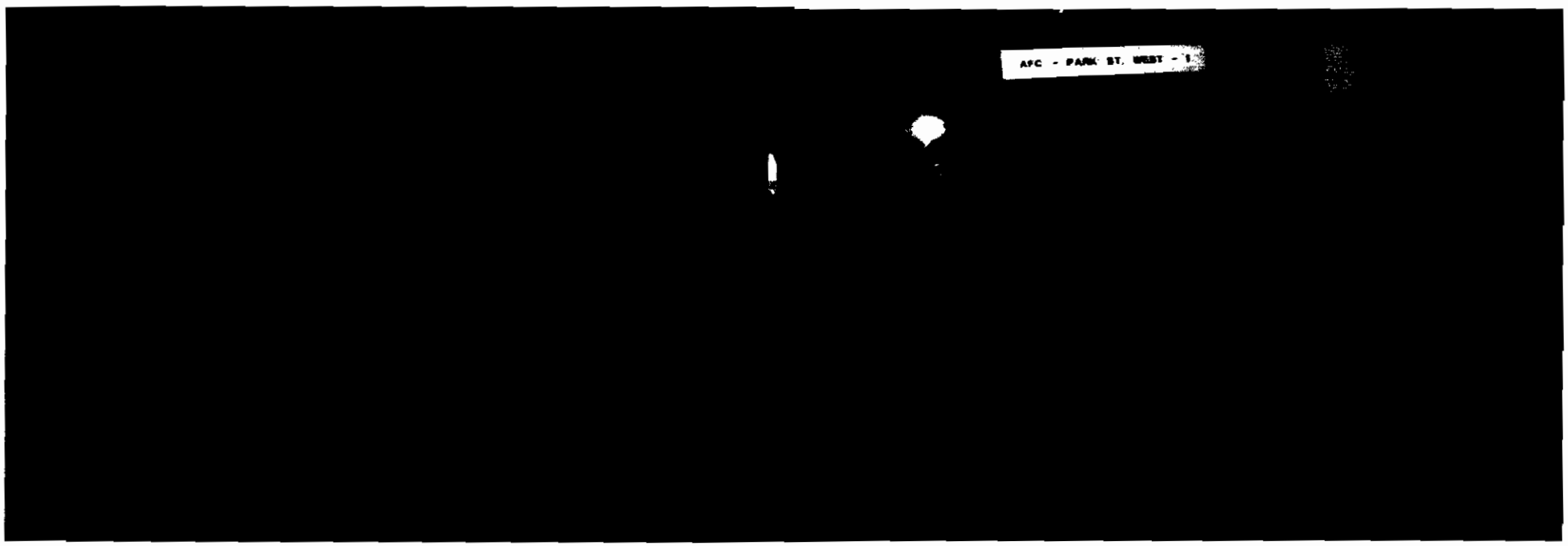


21

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 73 of 97

fiber switches in unlocked room

connect fare vending machines to the internal network



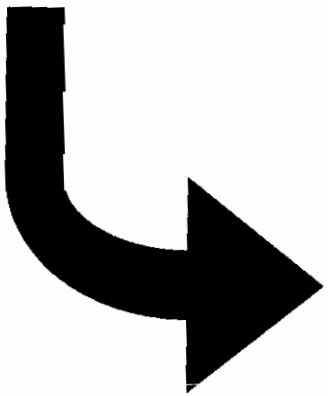


72

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 74 of 97

Social Engineering

Executed the "PHANTOM MEETING" attack



Gained access to internal network drops and computers

Nobody suspected a thing as we walked into offices and conference rooms…

So we took it up a notch.

73

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 75 of 97

first there was **wardialing**

c.**1983** - 2000 – 2001 – 2002 – 2006 – 2007 - 2008

74

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 76 of 97

then there was **wardriving**

c.1983 - **2000** – 2001 – 2002 – 2006 – 2007 - 2008

75

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 77 of 97

then there was **warwalking**

c.1983 - 2000 – **2001** – 2002 – 2006 – 2007 - 2008

26

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 78 of 97

then there was **warflying** and **warboating**

c.1983 - 2000 – 2001 – **2002** – 2006 – 2007 - 2008

77

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 79 of 97

then there was **war-rocketing**

c.1983 - 2000 – 2001 – 2002 – **2006** – 2007 - 2008

78

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 80 of 97

then there was **warballooning**

c.1983 - 2000 – 2001 – 2002 – 2006 – **2007** - 2008

79

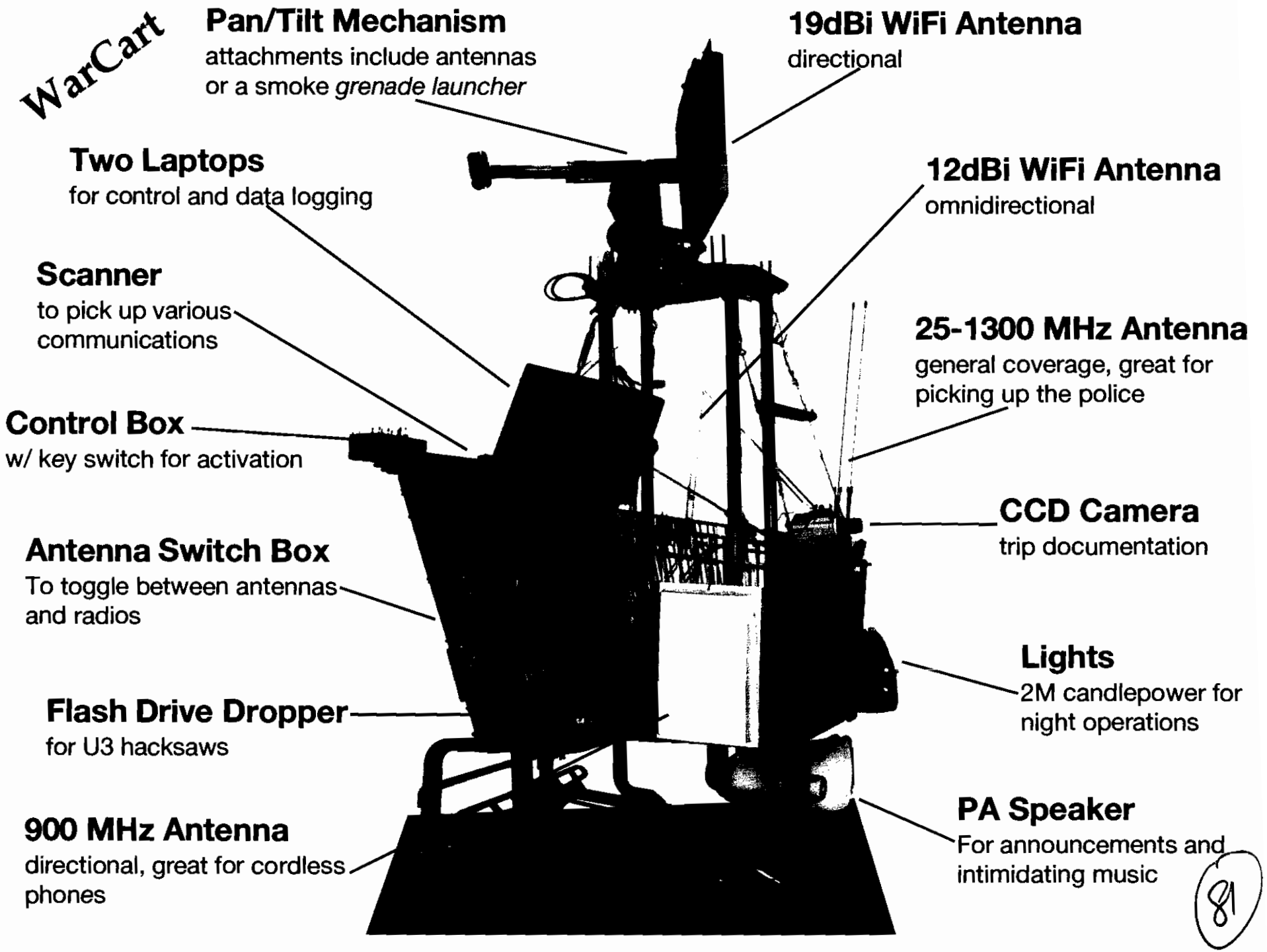
Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 81 of 97

and now… **warcarting**

c.1983 - 2000 – 2001 – 2002 – 2006 – 2007 - **2008**

80

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 82 of 97



Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 83 of 97

(28)

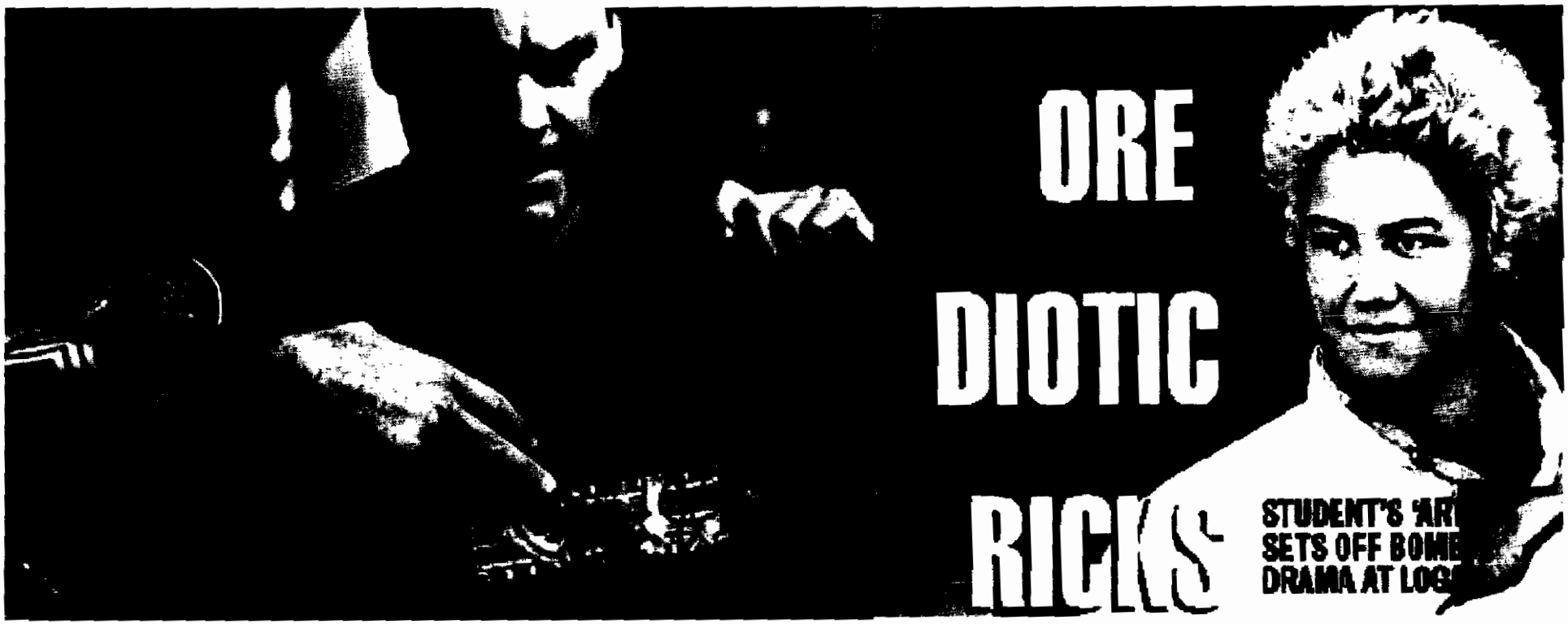
And then we ran into some problems with the police



That's one of the WarCart's smoke grenades, by the way

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 85 of 97

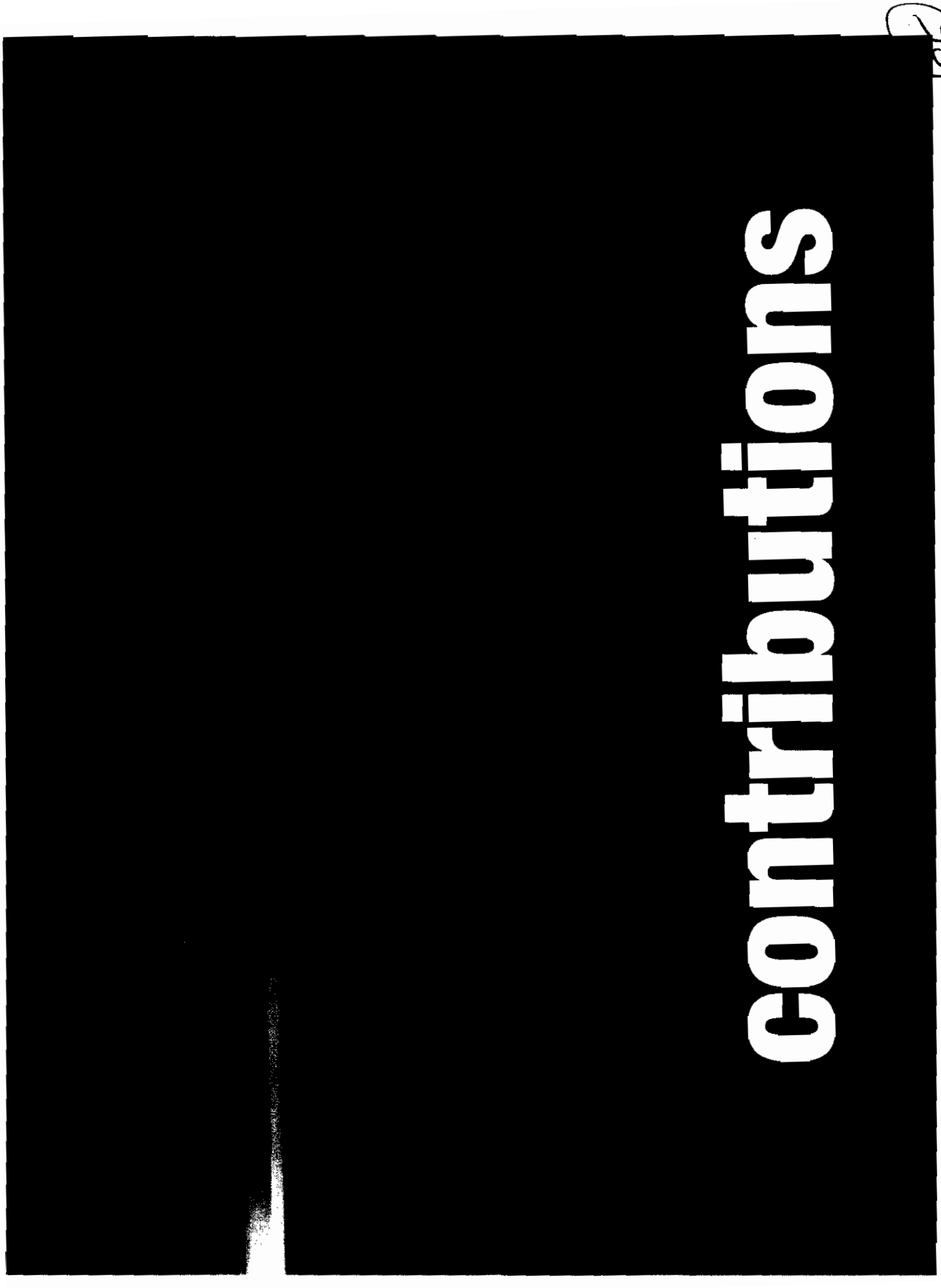
So to avoid ending up like this



We turned back

64

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 86 of 97


contributions

contributions

1) **Exploited** physical security holes

2) **Reverse engineered** the CharlieTicket

3) Wrote code to analyze & **generate** magcards

4) Wrote a **toolchain** for analyzing 13.56MHz RFID transactions using the USRP+GNUradio

5) **Attacked** problems with the MIFARE Classic cards

6) Wrote **brute forcer**-generator to crack keys on an FPGA

7) Developed software to **reduce MQ to SAT**, allowing key recovery

8) Wrote code to **read and clone** MIFARE cards (given the key)

Case 1:08-cv-11364-GAO Document 9-8 Filed 08/09/2008 Page 88 of 97

Exhibit 8

Mahony, Ieuan (BOS - X75835)

From: Marcia Hofmann [marcia@eff.org]
Sent: Saturday, August 09, 2008 4:38 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu
Subject: Re: MBTA v Anderson et al

Attachments: defcon-16-anderson-ryan-cheisa.pdf



defcon-16-ander
son-ryan-cheisa..

Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

--
Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tel: (415) 436-9333 x. 116 | fax: (415) 436-9993 marcia@eff.org | http://www.eff.org

Join EFF today! http://www.eff.org/support

ieuan.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
>
> I note that we still do not have your clients' presentation materials.
> I am inclined to object to any discussion of a postponement, as the
> decision to continue to withhold these materials makes me concerned.
> As I stated during our 9:00, and 11:30 calls this evening, I see no
> basis for continuing to withhold this information.
>
> With that said, we remain interested in discussing an amicable
> resolution. Once I have finished the Supplemental Declaration I
> discussed, I will begin work on a proposed Consent Judgment and format
> for your review.
>
> Ieuan

>
>
> *Holland + Knight*
>
> *Ieuan G. Mahony*
> Partner
> Holland & Knight LLP
> 10 St. James Avenue
> Boston, MA 02118
> Main 617 523 2700
> Direct 617 573 5835
>
> Cell 781-789-4230
> Fax 617 523 6850
> Email ieuan.mahony@hklaw.com
>
> www.hklaw.com
>
> *NOTICE: * This e-mail is from a law firm, Holland & Knight LLP
> ("H&K"), and is intended solely for the use of the individual(s) to
> whom it is addressed. If you believe you received this e-mail in
> error, please notify the sender immediately, delete the e-mail from
> your computer and do not copy or disclose it to anyone else. If you
> are not an existing client of H&K, do not construe anything in this
> e-mail to make you a client unless it contains a specific statement to
> that effect and do not disclose anything to H&K in reply that you
> expect it to hold in confidence. If you properly received this e-mail
> as a client, co-counsel or retained expert of H&K, you should maintain
> its contents in confidence in order to preserve the attorney-client or
> work product privilege that may be available to protect confidentiality.
>
>

Exhibit 9

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:15 AM
To: 'Marcia Hofmann'
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu; 'Swope, Jeffrey'; William Mitchell; Scott Darling; Mahony, Ieuan (BOS - X75835)
Subject: RE: MBTA v Anderson et al

Marcia:
I am circulating this now. Given the time, and Scott's flight, I am not sure how close a review of the substance we will have by the hearing.

I have the following two requests, and would appreciate a response as far in advance of the hearing as you are able:

(1) Please let me know the time at which the slide deck was first distributed to DEFCON attendees.

(2) Please let me know the relationship, if any, between (a) the point in time the MIT Undergrads understood the MBTA wanted an opportunity to view these materials; and (b) the point in time when the materials were distributed at DEFCON.

I will wait for your call, and would appreciate a response to the above two questions.

Ieuan

-----Original Message-----
From: Marcia Hofmann [mailto:marcia@eff.org]
Sent: Saturday, August 09, 2008 4:38 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu
Subject: Re: MBTA v Anderson et al

Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

--
Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tel: (415) 436-9333 x. 116 | fax: (415) 436-9993 marcia@eff.org | http://www.eff.org

Join EFF today! http://www.eff.org/support

ieuan.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
>
> I note that we still do not have your clients' presentation materials.
> I am inclined to object to any discussion of a postponement, as the
> decision to continue to withhold these materials makes me concerned.
> As I stated during our 9:00, and 11:30 calls this evening, I see no
> basis for continuing to withhold this information.
>
> With that said, we remain interested in discussing an amicable
> resolution. Once I have finished the Supplemental Declaration I
> discussed, I will begin work on a proposed Consent Judgment and format
> for your review.
>
> Ieuan
>
>
> *Holland + Knight*
>
> *Ieuan G. Mahony*
> Partner
> Holland & Knight LLP
> 10 St. James Avenue
> Boston, MA 02118
> Main 617 523 2700
> Direct 617 573 5835
>
> Cell 781-789-4230
> Fax 617 523 6850
> Email ieuan.mahony@hklaw.com
>
> www.hklaw.com
>
> *NOTICE: * This e-mail is from a law firm, Holland & Knight LLP
> ("H&K"), and is intended solely for the use of the individual(s) to
> whom it is addressed. If you believe you received this e-mail in
> error, please notify the sender immediately, delete the e-mail from
> your computer and do not copy or disclose it to anyone else. If you
> are not an existing client of H&K, do not construe anything in this
> e-mail to make you a client unless it contains a specific statement to
> that effect and do not disclose anything to H&K in reply that you
> expect it to hold in confidence. If you properly received this e-mail
> as a client, co-counsel or retained expert of H&K, you should maintain
> its contents in confidence in order to preserve the attorney-client or
> work product privilege that may be available to protect confidentiality.
>
>

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:26 AM
To: 'Swope, Jeffrey'
Cc: 'Marcia Hofmann'; kurt@eff.org; jennifer@eff.org; jaren@mit.edu; William Mitchell; Scott Darling; Mahony, Ieuan (BOS - X75835)
Subject: RE: MBTA v Anderson et al

Jeffrey:
I make the following request of you, again, as far in advance of the hearing as you are able:

(1) Please state when MIT first become aware of this slide deck?

(2) Please state whether MIT at any point had access to a copy of this slide deck? If so, when?

Thank you

Ieuan
-----Original Message-----
From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:15 AM
To: 'Marcia Hofmann'
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu; 'Swope, Jeffrey'; William Mitchell; Scott Darling; Mahony, Ieuan (BOS - X75835)
Subject: RE: MBTA v Anderson et al

Marcia:
I am circulating this now. Given the time, and Scott's flight, I am not sure how close a review of the substance we will have by the hearing.

I have the following two requests, and would appreciate a response as far in advance of the hearing as you are able:

(1) Please let me know the time at which the slide deck was first distributed to DEFCON attendees.

(2) Please let me know the relationship, if any, between (a) the point in time the MIT Undergrads understood the MBTA wanted an opportunity to view these materials; and (b) the point in time when the materials were distributed at DEFCON.

I will wait for your call, and would appreciate a response to the above two questions.

Ieuan

-----Original Message-----
From: Marcia Hofmann [mailto:marcia@eff.org]
Sent: Saturday, August 09, 2008 4:38 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu
Subject: Re: MBTA v Anderson et al

Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these

slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

--
Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tel: (415) 436-9333 x. 116 | fax: (415) 436-9993 marcia@eff.org | http://www.eff.org

Join EFF today! http://www.eff.org/support

ieuan.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
>
> I note that we still do not have your clients' presentation materials.
> I am inclined to object to any discussion of a postponement, as the
> decision to continue to withhold these materials makes me concerned.
> As I stated during our 9:00, and 11:30 calls this evening, I see no
> basis for continuing to withhold this information.
>
> With that said, we remain interested in discussing an amicable
> resolution. Once I have finished the Supplemental Declaration I
> discussed, I will begin work on a proposed Consent Judgment and format
> for your review.
>
> Ieuan
>
>
> *Holland + Knight*
>
> *Ieuan G. Mahony*
> Partner
> Holland & Knight LLP
> 10 St. James Avenue
> Boston, MA 02118
> Main 617 523 2700
> Direct 617 573 5835
>
> Cell 781-789-4230
> Fax 617 523 6850
> Email ieuan.mahony@hklaw.com
>
> www.hklaw.com
>
> *NOTICE: * This e-mail is from a law firm, Holland & Knight LLP
> ("H&K"), and is intended solely for the use of the individual(s) to
> whom it is addressed. If you believe you received this e-mail in
> error, please notify the sender immediately, delete the e-mail from
> your computer and do not copy or disclose it to anyone else. If you
> are not an existing client of H&K, do not construe anything in this
> e-mail to make you a client unless it contains a specific statement to
> that effect and do not disclose anything to H&K in reply that you
> expect it to hold in confidence. If you properly received this e-mail
> as a client, co-counsel or retained expert of H&K, you should maintain

> its contents in confidence in order to preserve the attorney-client or
> work product privilege that may be available to protect confidentiality.
>
>

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. No. 08- 11364-GAO

DECLARATION OF SCOTT HENDERSON

1. I am the Systems Project Manager for the Automated Fare Collection System for the plaintiff, Massachusetts Bay Transportation Authority ("MBTA").

2. My duties include (a) responsibility for the computer systems resident in all of the devices within the Automated Fare Collection ("AFC") System, and (b) responsibility for all software application systems within the AFC System. I have included further information concerning my qualifications, relevant to this Declaration, in paragraphs 28 through 37.

3. I make this declaration based on my personal knowledge and a review of MBTA business records concerning the matters set out below.

Requests To The MIT Undergrads For Their DEFCON Presentation Materials

4. I have reviewed the documents referred to in the Complaint as the " Initial Announcement" and the "Revised Announcement". I use the term "MIT Undergrads" to refer to the defendants, Zack Anderson, RJ Ryan, and Alessandro Chiesa.

FILED
In Open Court
USDC, Mass.
Date 8/9/08
By JANETTE LOVETT
Deputy Clerk

5. I have communicated with the defendant, Zack Anderson, requesting that he send to the MBTA the materials the MIT Undergrads plan to present at the DEFCON Conference.

6. I spoke with Mr. Anderson at some length on Friday, August 8, 2008, to further explain the MBTA's concerns. I discussed concerns over information the MIT Undergrads might disclose, and again requested Mr. Anderson's cooperation. I asked for presentation materials he was planning to disclose and discuss at the DEFCON Conference.

7. By email dated Friday, August 8, 2008 at 4:27 PM, Mr. Anderson provided a document to William Mitchell, General Counsel for the MBTA. This document consists of a title page, and four pages of text. It is entitled "Fare Collection Vulnerability Assessment Report: Analysis and Recommendations," is dated as of Friday, August 8, 2008, and states that it was "Prepared for the Massachusetts Bay Transit Authority" (the "August 8 Undergrad-to-MBTA Report"). I have attached to this Declaration as Exhibit 1 a true and accurate copy of this August 8 Undergrad-to-MBTA Report.

8. In his email, Mr. Anderson provided brief covering text for the August 8 Undergrad-to-MBTA Report, and this text reads, in relevant part:

> We have attached a confidential disclosure report to this email. It details what we found and ways to fix some of the issues. Note that we absolutely are not disclosing everything we found in this report. We have no intention to allow anyone in any way to defraud the MBTA. This is a very important note that we made clear to Richard Sullivan when we met with him. Please call me after looking over this report.

9. I have attached a true and accurate copy of this email as Exhibit 2 to this Declaration

10. After reviewing the August 8 Undergrad-to-MBTA Report, I concluded (as described in further detail beginning at paragraph 18, below) that the Report likely did not constitute the materials the MIT Undergrads planned to present at the DEFCON Conference.

11. Moreover, I was concerned with the statement: "[n]ote that we absolutely are not disclosing everything we found in this report."

12. It is unclear, among other interpretations, whether Mr. Anderson meant (a) that the August 8 Undergrad-to-MBTA Report disclosed all of the MIT Undergrads' information concerning claimed security flaws in the Fare Media System, and the Undergrads did not plan to present all information in this Report at the DEFCON Conference; or (b) that the MIT Undergrads had additional information concerning claimed security flaws, and this additional information was not included in the August 8 Undergrad-to-MBTA Report.

13. I requested all of the MIT Undergrads' presentation materials. When I did not receive presentation materials, I emailed Mr. Anderson on Friday, August 8, 2008 at 6:08 to again request these materials, and to ensure that he had my correct email address. I have attached a true and accurate copy of this email, as Exhibit 3 to this Declaration.

14. I received a voice mail from Mr. Anderson on Aug 8 2008 at 6:25 PM stating that he was looking for an internet connection to send me the "presentation files" for the DEFCON Conference. He stated that he should have these materials sent to me in an hour.

15. I received a second voice mail from Mr. Anderson at 6:49 PM stating that his lawyers advised him not to send me the presentation materials, because of the MBTA's Complaint.

16. The only security-related materials I have received from the MIT Undergrads is the August 8 Undergrad-to-MBTA Report. No one at the MBTA has received anything substantive from the MIT Undergrads beyond the August 8 Undergrad-to-MBTA Report.

17. Mr. Anderson's 6:49PM voice-mail indicates that presentation materials exist, which have not been provided to the MBTA for review.

Review Of The MIT Undergrads' Four Page Document

18. I have reviewed the August 8 Undergrad-to-MBTA Report in detail. This Report appears incomplete, and appears not to comprise the information the MIT Undergrads have developed concerning security attacks on the MBTA's Fare Media System. In addition, the Report does not appear to constitute the specific materials the MIT Undergrads intend to present at the DEFCON Conference.

19. First, the Report states that it is "prepared for" the MBTA. It is unlikely that such a Report would be presented at the DEFCON hacking convention.

20. Second, the Report presents little to no original information concerning smartcards or the MBTA's CharlieCard. In the Initial and Revised Announcements, the MIT Undergrads stated that they had developed "several attacks to completely break the CharlieCard." The only substantive attack the August 8 Undergrad-to-MBTA Report references (on the third page, under the heading "CharlieCard") is an attack keyed to the underlying MIFARE Classic card.

21. This is not original work or an original attack. The security risk of the MIFARE Classic card standing alone has been documented by Karsten Nohl, et al, as referenced by the MIT Undergrads in the August 8 Undergrad-to-MBTA Report. Moreover, as noted in Gary Foster's Declaration, paragraphs 6 and 7, the potential security risk of the MIFARE Classic card is not even relevant, given the substantial added MBTA proprietary security systems and technology that protect the CharlieCard.

22. I understand that MIT Professor Ron Rivest awarded the MIT Undergrads an "A" for the paper that was the genesis for the Undergrads' desire to present at the DEFCON Conference. It would seem unlikely that Professor Rivest would award an A for unoriginal, duplicative work, such as that outlined in the August 8 Undergrad-to-MBTA Report.

23. Finally, Mr. Anderson's August 8, 4:27 PM email suggests that more materials and information exist, beyond the August 8 Undergrad-to-MBTA Report, and Mr. Anderson, in his 6:49PM voice-mail, stated that presentation materials exist.

24. In sum, in my evaluation the August 8 Undergrad-to-MBTA Report is incomplete. Moreover, the MIT Undergrads, apparently on the advice of counsel, continue to decline to provide their DEFCON presentation materials, or other materials that would allow an individual reasonably skilled in the art to evaluate whether the MIT Undergrads in fact have compromised, or are able to compromise, the MBTA's Fare Media System.

25. Therefore, in my opinion, despite the MBTA's continued requests for information, it remains not possible to determine, to a reasonable degree of certainty, (i) what the MIT Undergrads have done (if anything) with respect to attacking the security and integrity of the MBTA's Fare Media System; (ii) what they plan to disclose at the DEFCON Conference; or (iii) what level of threat, if any, the information they possess poses to the MBTA's CharlieCard and CharlieTicket structures.

26. In these circumstances, without solid assurance that the MIT Undergrads' activities do not pose an immediate threat to the Fare Media System's integrity and security, the required course in my opinion is to conclude that the activities do pose an immediate threat, and to act, as the MBTA is, to mitigate that threat through direct Court intervention.

Further Information On Qualifications

27. I possess the following additional qualifications, relevant to the subject matter of this Declaration:

28. Information Technology. I was hired by the MBTA on June 1, 1992, in the Information Technology Department. In this role, I implemented the MBTA's Wide Area Network. In addition, I planed and implemented the MBTA's internal electronic mail system.

29. Revenue Department. In December, 1994, I transferred into the MBTA Revenue Department. There, I held the position of Systems Integration Engineer for the Token Vending machine project. This system was in operation until the installation of the Automated Fare Collection System in 2005. I co-managed the GFI farebox replacement contract in 1994. I co-authored the first technical specification of the Automated Fare Collection System in 1995. I was responsible for the automation of the Revenue counting facility, which facility included new coin and bill high speed counting and sorting equipment. I was also charged with the integration of this counting equipment into the Vault control system. I was responsible for the procurement and the installation of the Vault control system. This system remains in place at the MBTA, and has been upgraded to support the latest technology.

30. Y2K Project Manager. I was Project Manager for the Y2K projects through out the various systems in place in the Revenue department. My responsibilities included operation system patches, firmware upgrades and hardware modifications along with total application replacements.

31. IT End User Computing. I was later promoted to the Information Technology Department Head of End User Computing. In this position, I was responsible for the installation and maintenance of entire MBTA's Desktops and servers. I instituted a PC life-cycle system which replaced each system every three years. I was responsible for the MBTA's digital infrastructure which included all hardware, operating system software and applications. I managed a staff of 20 full-time employees in this role.

32. Automated Fare Collection System IT Specialist. In October of 2002 I was selected to work with the Automated Fare Collection System (the "AFC") as the IT Specialist with respect to the review of the technical specifications for this System. I spent approximately

the next 9 months on review of the technical design documents for this System. These duties included a review of all computer hardware and operating systems along with the design of the application software for our existing fare tariff.

33. CharlieTicket and CharlieCard; AFC Project Manager. In this role, I involved in the review and design of the MBTA's media layout and function of fare media, which included the CharlieTicket and CharlieCard and the existing monthly fare media. I was promoted to the role of AFC Systems Project Manager, responsible for the computer systems in all of the devices and the application systems. I am also responsible for the encryption Key generation. The encryption Key generation has a series of steps designed to ensure that no one person had knowledge of all keys involved. These keys are for the CharlieCard pass and associated smart card readers along with the encryption of all personnel information that is transported and stored throughout the AFC network. I spent a number of weeks working in Germany with the developers of the systems as well with the designers of the smart card systems that the MBTA employs. The MBTA has developed additional security in all of its systems in case the keys were compromised by illegal activity.

34. Smart Card Alliance. I am a current and active member of the Smart Card Alliance. The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests in education on the appropriate uses of technology for identification, payment and other applications, and advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the

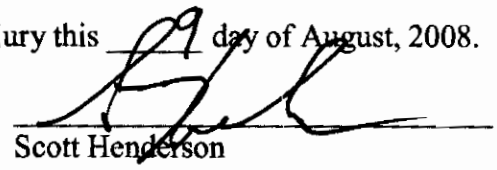
single industry voice for smart card technology, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

35. Relevant Publications. I co-published a paper for the Smart Card Alliance that was released August of 2008. The topic of the paper is "*Transit Payment System Security.*" The paper can be found at http://www.smartcardalliance.org/pages/publications-transit-payment-system-security. I have also worked on a number of sub-committees in the Alliance that have published white papers. These papers are: "*Serving Unbanked Consumers in the Transit Industry with Prepaid Cards*"; "*Co-Branded Multi-Application Contactless Cards*"; and "*Proximity Mobile Payments*".

36. Industry Work. I have been working on new contactless payment options such as Near Field Communications (NFC) with the following companies: Visa, MasterCard Worldwide, AMEX, Nokia, and Discover. My work with industry includes a limited pilot with NFC technology, which pilot consisted of a joint venture with Nokia, MasterCard, the MIT Slone School of Business, and the MBTA. This pilot involved an NFC enabled phone which was encoded with a CharlieCard embedded into it. Nokia provided the NFC enabled phones; the MBTA encoded the Phones with the CharlieCard; and MIT developed additional applications for the phones and provided the final report of the findings of this limited pilot.

37. Credit and Debit Fraud. I designed and implemented, and maintain a velocity checking program which identifies fraudulent credit card purchase patterns. This program has kept the incidence of credit card fraud on the MBTA systems approximately ten times lower than the industry transportation average. In addition, I work with law enforcement agencies on a local and national level in fraud investigations.

Signed under the penalties of perjury this 9 day of August, 2008.



Scott Henderson

Table of Exhibits

Ex. No.	Description
1.	Fare Collection Vulnerability Assessment Report: Analysis and Recommendations, dated August 8, 2008, prepared for the Massachusetts Bay Transit Authority (the "August 8 Undergrad-to-MBTA Report")
2.	Email dated Friday, August 8, 2008 at 4:27 PM from Z. Anderson to W. Mitchell
3.	Email dated Friday, August 8, 2008 at 6:08 from S. Henderson to Z. Anderson

5533211_v2

Exhibit 1

Prepared for the Massachusetts Bay Transit Authority

Fare Collection Vulnerability Assessment Report

ANALYSIS AND RECOMMENDATIONS

August 8, 2008

CONFIDENTIAL

By:
Zack Anderson
Russell Ryan
Alessandro Chiesa

Report Overview

We conducted a comprehensive security analysis of the fare collection systems used at various subways around the country. We focused most of our research on the Boston T system. This report details the vulnerabilities that we found, and ideas for improvement. In particular, we demonstrate how criminals can breach security mechanisms in the CharlieTicket and CharlieCard.

Vulnerability Assessment

CharlieTicket

The CharlieTicket is vulnerable to both *cloning* and *forgery* attacks. The key problems are:

a) Value is stored on the card, NOT in a central MBTA database.
b) Anyone that has a card can read and write it, given the correct equipment.
c) A cryptographic signature algorithm is NOT used on the data to ensure integrity.
d) MBTA networks do not leverage any type of centralized card verification.

Here is a possible *forgery* attack scenario:

> *A sophisticated criminal purchases a $150 magnetic card reader/writer from the internet. He goes to a fare vending machine (FVM) and purchases several 5-cent tickets. He then re-encodes these cards using the magnetic card reader/writer and custom software that puts $655.36 (the maximum possible) onto each card and then sells them. He ensures each card has a unique ID, making it harder for the MBTA to detect and ban fraudulent cards.*

And here is a possible *cloning* attack scenario:

> *Using the same magnetic card reader/writer and included software, an unsophisticated criminal can purchase a single card of, say, $50 value, and make several copies of it onto 5-cent cards. Each of these will be worth $50. The attacker does not need to have any understanding of the data on the card to execute this attack.*

While these fraudulent cards will work as valid fare, if an official were to inspect one of these cards she would see the actual initial value printed on the card (here, 5-cents) and there would be no record of the card (under a *forgery* attack) in MBTA databases. An attacker can get around these limitations as follows:

> *The attacker takes the forged or cloned ticket to an FVM. Suppose he inserts a forged $99 ticket. He then selects "add value" and inserts one dollar cash. The machine prints out a legitimate ticket with $100 value, even though the cost to the attacker was only $1.05 (one dollar plus the cost of the initial forged CharlieTicket).*

Since this will register as a legitimate ticket paid with cash, the audit trail will not necessarily demonstrate criminal activity. This is a serious vulnerability. We show in the Recommendations section how such problems can be mitigated.

Our research shows that one can write software that will generate cards of any value up to $655.36. CharlieTickets are stored-value cards. The value is stored as unencrypted data on track 3 of the magnetic stripe card. Anyone in possession of one of these cards can read, copy, reverse-engineer, and/or rewrite the data.

The CharlieTicket has a non-trivial checksum on track 3 of the magnetic card data. Unless an attacker knows how to calculate this checksum from the forged data, the card will not work. This is a security feature on the CharlieTicket. Unfortunately, the checksum formula is not a secure cryptographic algorithm. In addition, it is only six-bits long which allows an attacker to execute a brute-force attack (trying all 64 possible cards) until one works. We have purposely omitted details of this checksum in any public disclosures we have made. That said, this "security feature" has weaknesses that should be improved. We detail how this can be done in the Recommendations section. Note that the checksum is only a problem if one is trying to *forge* a card. When a card is *cloned*, the checksum is known.

CharlieCard

The CharlieCard is based on a MIFARE Classic RFID card produced by NXP. The card secures its data and transactions using a proprietary encryption algorithm called Crypto-1. Karsten Nohl, et al. of the University of Virginia reverse-engineered this algorithm and found serious vulnerabilities. These vulnerabilities allow one to recover the key from a card in less than 30 seconds. Armed with a key, an attacker can copy someone's card remotely. Although we have not absolutely verified this, we have strong reason to believe all CharlieCards use a common key. The following assumes this fact, but the system is still vulnerable even if this is not the case.

Here is a possible attack scenario:

> *An attacker uses RFID equipment purchased online to sniff communications between a legitimate CharlieCard and a turnstile. He takes the data back home and executes one of several attacks that exploit the weak Crypto-1 cipher to recover a key. Armed with this key, a high-gain antenna, and RFID equipment, he walks down a crowded street in Boston remotely copying the CharlieCards in people's pockets. He can then encode any MIFARE Classic Cards (such as CharlieCards) with this data and use them as fare.*

The details of key recovery are not relevant to the scope of this document. If interested, refer to Nohl's paper.

We have not used the CharlieCard key to read CharlieCards, so we cannot comment for certain about the data on the card. We have evidence to show that the card has a stored value, which makes it vulnerable to the same *forgery* attacks detailed in the CharlieTicket section. Likewise, it is vulnerable to *cloning* attacks too, meaning the above scenario would not steal money from the people in the street, but rather, it would duplicate the value on those cards.

Physical Security

Physical security issues are bound to happen in any case where a large system (such as a transit system) has to be secured. In our research, we discovered many blatant security issues. Doors were left unlocked allowing free entry in many subways. The turnstile control boxes were unlocked at most stations. Most shocking, however, were the FVM control rooms that were occasionally left open. The FVMs and turnstiles are networked. These fiber network cables run into the FVM control closets, where the fiber lines go to network switches. Since confidential

data (i.e. credit cards) are transmitted across these lines, it is highly important that they be physically secured. A strong firewall is useless if an attacker is allowed to tap an internal network switch.

Recommendations

Summary

In this section we detail possible fixes to vulnerabilities in the MBTA fare collection system. With cost in mind, we recommend the MBTA use the following tactics:

1) A central auditing system
2) A cryptographically-secure digital signature on CharlieCards and CharlieTickets
3) Educate staff about securing high-value rooms such as FVM closets

Fare Collection Network Infrastructure Improvements

The MBTA should deploy a centralized database to detect clones and forgeries. There are two possible configurations of such a database.

1. An **auditing system** to detect forgeries after they occur and disable the illegitimate cards

An auditing system cannot prevent the creation of clones and forgeries, but it can aid in their detection and disabling of fraudulent cards. For example, cards used at different locations in short time spans, cards whose value grows without a corresponding record of purchase, or cards with fare value larger than the possible purchase value (e.g. $100) can be flagged as illegitimate. This auditing system is compatible with stored-value cards such as the CharlieTicket and CharlieCard.

2. A **central repository** to store the current value of the cards in the system.

A central repository would require significant changes to the system software, but it will eliminate the risk of card forgery and cloning. This is the most secure way of fixing problems in the system, but it presents potential cost and availability issues. Clones will not result in a loss of MBTA revenue because they subtract fare from the same account in the database.

One downside of this configuration is that if a user has their card cloned by an attacker, then their account will be deducted every time the attacker uses their card. This is analogous to cloning somebody's credit card: both the real card and the clone refer to the same account in the credit card company's files.

CharlieTicket Improvements

The Charlie Ticket's main vulnerability is a weak checksum. The MBTA should use a cryptographically secure digital signature or message digest. A secret key will then protect the card from forgery. A good example of this is the HMAC with AES. Even with a secure signature, the card will still be vulnerable to cloning. To counter cloning follow the improvements outlined in the previous section.

The current checksum is only 6 bits long. This means that even if an attacker does not know the checksum algorithm, he only has to generate and try 64 different cards to find a working forgery. A simple fix to this is to incorporate more bits into the current checksum algorithm to make brute forcing infeasible. Sixteen bits are enough for this purpose, as the attacker would have to try 65,536 cards before finding the correct one.

Another approach to avoid forgery is to encrypt the data on the card with a cryptographically secure cipher, such as AES. An attacker will be unable to understand the contents of the card, preventing forgeries. The CharlieTicket stores some personal information, such as the last station where the card was used, as well as the last time it was used. Encrypting the card data has the additional benefit of protecting the owner's privacy.

CharlieCard Vulnerability Mitigations

If cost were not an issue, the best way to fix problems with the CharlieCard is to merge to a secure RFID card such as the MIFARE DESfire. This will prevent key recovery, meaning the above exploits cannot be executed. This fix may pose a significant cost, but is clearly the most secure solution.

Since cost is an issue, we have devised various ways the MBTA can mitigate the above detailed vulnerabilities without hardware revamping. Several of these fixes are similar to the recommendations we made for the CharlieTicket.

The CharlieCard is vulnerable to two types of attacks: *forgery* and *cloning* attacks. We propose different fixes to mitigate risk on each of these.

To prevent *forgery* attacks, a secure cryptographic signature or a secondary layer of encryption on the data should be used. This is a purely software fix, and will prevent an attacker from forging cards. In order to implement this fix, the system integrator will have to upgrade the firmware running on the FVM and turnstile devices.

To prevent *cloning* attacks, central auditing should be performed. Even for a stored value card, the network infrastructure already in place can be leveraged to detect suspicious activity. Examples of this are (repeated here from the auditing section):

1) The same card is used in a short time-span at two different stations.
2) A card ID with a known value suddenly increases in value.

Physical Security Recommendations

We recommend that the MBTA stress during employee training the importance of keeping certain areas secured at all times. High-value locations such as the FVM closets need to remain secure due to the network switches they contain.

Exhibit 2

>>> Zack Anderson <zacka@MIT.EDU> 8/8/2008 4:27 PM >>>
Hi Mr. Mitchell,

We have attached a confidential disclosure report to this email. It details what we found and ways to fix some of the issues. Note that we absolutely are not disclosing everything we found in this report. We have no intention to allow anyone in any way to defraud the MBTA. This is a very important note that we made clear to Richard Sullivan when we met with him. Please call me after looking over this report.

My number is 310-270-3995.

Best regards,
Zack Anderson

Exhibit 3

Mahony, Ieuan (BOS - X75835)

From: Scott Henderson [shenderson@mbta.com]
Sent: Friday, August 08, 2008 6:08 PM
To: zacka@MIT.EDU
Subject: Presentation

Zack, I have not received the defcon 16 presentation that you were going to send. I am dropping you an email to be sure that you have my correct email address.

Thanks in advance

Scott

Scott A. Henderson
Systems Project Manager
Automated Fare Collection
617-222-6954

Mahony, Ieuan (BOS - X75835)

From: zacka@mit.edu
Sent: Friday, August 08, 2008 6:47 PM
To: Scott Henderson
Subject: Re: Presentation

Hi,

Please give me a call. I left a message on your voicemail.

Zack
------Original Message------
From: Scott Henderson
Sender:
To: zacka@mit.edu
Subject: Re: Presentation
Sent: Aug 8, 2008 6:42 PM

Thanks

Scott A. Henderson
Systems Project Manager
Automated Fare Collection
617-222-6954

This email/electronic message, including any attached files, is being sent by the MBTA. It is solely intended for the recipient(s) and may contain information that is proprietary, confidential, legally privileged, and/or exempt from disclosure pursuant to state and federal law. If you have received this message in error or are not the intended recipient(s), please notify the sender immediately by reply, and delete all copies of this email/electronic message and any attached files from your computer. If you are the intended recipient(s), you may use the information contained in this email/electronic message and any attached files only as authorized by the MBTA. Any unauthorized use, dissemination, or disclosure of this email/electronic message and/or its attached files is strictly prohibited.

Sent from my Verizon Wireless BlackBerry

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

CERTIFICATE OF SERVICE FOR SUPPLEMENTAL FILINGS IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER

1. The term "Defense Counsel" for purposes of this Certificate of Service means the following:

Party	Counsel
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Marcia Hofman, Esq. Electronic Frontier Foundation 1875 Connecticut Ave., Suite 650 Washington, DC 20009 202-797-9009 Fax: 202-797-9066 Email: marcia@eff.org Kurt Opsahl Electronic Frontier Foundation 454 Shotwell St. San Francisco, CA 94110 415-436-9333 Fax: 415-436-9993 Email: kurt@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue

FILED
In Open Court
USDC, Mass.
Date 8/9/08
By JANET LOVETT
Deputy Clerk

Boston, Massachusetts 02199 USA
617-239-0100
Fax: 617-227-4420
Email: JSwope@eapdlaw.com

2. I verified the above email addresses for Defense Counsel, either by using the email address by which counsel contacted me via email, or by confirming over the phone that counsel received email I had sent to that email address.

3. With respect to the revised Order, I certify (a) that I provided a copy of the document to Defense Counsel by email on Friday, and served Counsel for MIT by hand before the Saturday, August 09, 2008 hearing.

4. With respect to the second revised Order, I certify (a) that I provided a copy of the document to Defense Counsel by email on Saturday morning, and served Counsel for MIT by hand before the Saturday, August 09, 2008 hearing.

5. With respect to the Declaration of Scott Henderson (and attached Exhibits), I certify (a) that I provided a copy of the document to Defense Counsel by email on Saturday morning, and served Counsel for MIT by hand before the Saturday, August 09, 2008 hearing.

6. With respect to the Supplemental Declaration of Ieuan G. Mahony (and attached Exhibit), I certify (a) that I provided a copy of the document to Defense Counsel by email Saturday morning, and served Counsel for MIT by hand before the Saturday, August 09, 2008 hearing.

Ieuan G. Mahony

5533213_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

TEMPORARY RESTRAINING ORDER

After hearing this day and upon consideration of the written and oral submissions of the parties regarding the Plaintiff's Motion for Temporary Restraining Order, for the reasons stated orally from the bench at the conclusion of the hearing, it is hereby ORDERED as follows:

A. That the following terms herein shall have the following definitions:

(1) Fare Media System. The term "Fare Media System" means the plaintiff's system that meets the following two criteria: the system (i) is employed by the MBTA to manage, track, charge for, and collect fares; and (ii) relies on CharlieTicket passes and/or CharlieCard passes.

(2) MIT Undergrads. The term "MIT Undergrads" means the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa and all persons in active concert or participation with any of them.

B. That the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ P. 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System

DONE AND ORDERED in Boston, Massachusetts at 1:30 pm this 9th day of August 2008.

_____

DOUGLAS P. WOODLOCK
UNITED STATES DISTRICT JUDGE

5533219_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

TEMPORARY RESTRAINING ORDER

After hearing this day and upon consideration of the written and oral submissions of the parties regarding the Plaintiff's Motion for Temporary Restraining Order, for the reasons stated orally from the bench at the conclusion of the hearing, it is hereby ORDERED as follows:

A. That the following terms herein shall have the following definitions:

(1) Fare Media System. The term "Fare Media System" means the plaintiff's system that meets the following two criteria: the system (i) is employed by the MBTA to manage, track, charge for, and collect fares; and (ii) relies on CharlieTicket passes and/or CharlieCard passes.

(2) MIT Undergrads. The term "MIT Undergrads" means the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa and all persons in active concert or participation with any of them.

B. That the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ P. 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System

DONE AND ORDERED in Boston, Massachusetts at 1:30 pm this 9th day of August 2008.

/s/ Douglas P. Woodlock

DOUGLAS P. WOODLOCK
UNITED STATES DISTRICT JUDGE

5533219_v1

AO 458 (Rev. 10/95) Appearance

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACHUSETTS

Massachusetts Bay Transportation Authority

v.

Jack Hanbon, et al

APPEARANCE

Case Number: 08-CV-11364-GAO

To the Clerk of this court and all parties of record:

Enter my appearance as counsel in this case for

Massachusetts Institute of Technology

I certify that I am admitted to practice in this court.

8/9/2008
Date

Signature

Jeffrey Swope 4/90760
Print Name Bar Number

Gunster, Yoakley & Stewart PA
Address

111 Huntington Ave
City Boston State MA Zip Code 02199

Phone Number 617 2390181 Fax Number 617 227 4420

FILED
In Open Court
USDC Mass.
Date 8/9/08
By JAZRES LOVETT
Deputy Clerk

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08- 11364-GAO

Declaration of Eric Johanson

I, Eric S. Johanson, hereby declare:

1. I am a security consultant specializing in penetration testing and application assessments. I have worked for the last seven years on application code assessments, wireless penetration tests, and architecture reviews. My involvement with the security industry builds on five years in software development.

2. I have worked for years as an independent consultant, and I have been a member of IOActive, Levianthan Security Group, and Security Innovation. My clients have included federal and state government agencies and Fortune 500 companies.

3. I am a frequent speaker at national and international computer security conferences, including ShmooCon, H.O.P.E., and DEFCON. I am a member of the Shmoo Group, a professional non-profit computer security organization that gives me an active research role in emerging security issues. My security research work has resulted in wide coverage in the press, including academic forums and national newspapers.

FILED
In Open Court
USDC, Mass.
Date 8/9/08
By JARRETT LOVELL
Deputy Clerk

4. I hold the opinions expressed herein to a reasonable degree of professional certainty. If called as a witness I could and would testify competently to the following.

5. I have reviewed the slides submitted by Defendants Zack Anderson, RJ Ryan and Alessandro Chiesa to DEFCON 16, in connection with their presentation, "The Anatomy of a Subway Hack" (hereafter the "Slides"), which is currently scheduled for Sunday, August 10, 2008.

6. DEFCON is one of the premier computer security conventions and is held every year in Las Vegas, Nevada. Attendees at DEFCON include numerous computer security professionals, along with journalists, lawyers, and federal government employees.

7. As part of my professional career, I am familiar with the literature and continually survey the publicly available research on security issues in payment systems, including magnetic stripe and Radio Frequency Identifier (RFID) based technologies.

8. For example, I have reviewed a presentation that security researchers Karsten Nohl and Henryk Plötz gave in December 2007, entitled "Mifare—Little Security, Despite Obscurity," at the 24th Chaos Communication Congress (24C3) in Berlin. This presentation documented critical flaws in the security integrity of the Mifare RFID transit payment system and generated substantial comment in the security research community. I am informed and believe that the Charlie Card uses the Mifare technology.

9. I reviewed the Slides to determine the extent to which the information presented in the Slides was already publicly known, based on my knowledge of the literature and publicly available research. I also considered whether the Slides presented sufficient information to compromise the security of the Charlie Ticket and the Charlie Card.

10. As discussed in detail below, in my expert opinion, the information presented in the Slides regarding the Charlie Ticket and the Charlie Card is already publicly known.

11. Further, in my expert opinion, key information needed to compromise both the Charlie Ticket and the Charlie Card is not present in the Slides.

The Practice of Security Research

12. Security in any particular application often depends on the soundness of many different components, as well as how these components interact with one another. Vulnerabilities can, and frequently do, arise from weaknesses in cryptographic algorithms and protocols, incorrect assumptions about the nature of attack threats, poor overall design, and human factor and user interface problems, to name but a few.

13. A significant focus of ongoing research, therefore, must be concerned with evaluating real-world security systems in an effort to discover whether they are, in fact, secure. Case studies of proposed and existing systems and standards form the essential basis for this research.

14. It is only by a thorough understanding of how real systems fail in practice that we are able to develop design principles for more secure systems in the future. Because there are no systematic techniques for ensuring the correctness of most aspects of secure systems architecture, research toward discovering vulnerabilities in systems as they are actually designed and implemented is essential for the advancement of the field. Scientific progress in this discipline necessarily depends upon the exploration of computer system weaknesses and the publication of the knowledge learned.

15. Security researchers, like all scientific and engineering researchers, necessarily rely on open publication of the knowledge learned as the means for communicating with one another and for measuring progress in the field.

16. Although presentations on security vulnerabilities often discuss how weaknesses might be exploited, prohibition of open discussion and publication of security vulnerabilities greatly harms the ability of researchers to function, and has a chilling effect not only on publication, but on whether some important research is done in the first place, greatly stifling scientific advancement.

17. Publication restrictions also encourage vulnerability research to go underground. Discouraging aboveboard, open research in legitimate institutions leads to a situation where the people who enjoy the most complete knowledge of the subject are those working unlawfully in the underground. Criminal organizations already have obvious incentives to learn how to defeat security measures. The question is whether the open scientific community and the public will be permitted to study and fix the same vulnerabilities that are visible to criminals.

18. Security researchers are drawn from many different disciplines, come from a wide range of backgrounds, and enjoy a variety of employment situations. It is not uncommon for students and non-academics to make significant contributions to the field. The set of individuals with a legitimate need to test systems for vulnerabilities and publish their results is not at all limited to those holding academic credentials or advanced educational or professional status.

Analysis of the Slides

19. The Slides describe using commercial, off-the-shelf hardware to read the data encoded on the magnetic stripe portion of the Charlie Ticket. This technique is widely known.

20. The Slides describe having written software to interact with the commercial, off-the-shelf hardware. This technique is also widely known.

21. The Slides describe applying standard, commonly used research techniques to the magnetic stripe data to categorize the data.

22. The Slides describe using the commercial, off-the-shelf hardware to write updates to the data on the Charlie Ticket magnetic stripe. This technique is widely known.

23. The Slides depict a field called "checksum," and show that it changes when the ticket value changes, but do not describe how to compute the checksum.

24. The Slides describe implementing the public standard known as ISO14443A, using commercial, off-the-shelf hardware. ISO refers to the International Standards Organization.

25. The Slides summarize and describe implementing techniques disclosed in "Reverse-Engineering a Cryptographic RFID Tag," an academic paper published on pages 185-193 of the Proceedings of the 17th USENIX Security Symposium.

26. The Slides do not describe any new techniques for breaking the cryptography used by the Charlie Card.

27. Slides 60-62 appear to be merely aspirational, and do not document successful, new vulnerabilities.

I declare under penalty of perjury that the foregoing is true and correct and was executed at Las Vegas, Nevada on this 9th day of August 2008.

_____/s/_____
Eric S. Johanson

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CLERK'S NOTICE

This document can not be scanned due to its size, or the way in which it was bound.

The original is available for viewing in the Clerk's Office.

Massachusetts Bay Transportation Authority v. Anderson et al Doc. 16

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08-11364-GAO

PLAINTIFF'S MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER

Introduction

The plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), hereby moves to modify the terms, but not the duration, of the Temporary Restraining Order issued by this Court on Saturday, August 9, 2008. As grounds, the MBTA states as follows:

1. On Saturday, August 9, 2008, after a hearing, this Court entered a Temporary Restraining Order in this matter (the "TRO"). A copy of the TRO is included in the Exhibits in Support of Plaintiff's Motion To Modify Terms But Not Duration Of Temporary Restraining Order (the "8/11 Exhibits").

2. In connection with issuing the TRO, the Court issued Findings and Rulings orally from the bench. These Findings and Rulings have not yet been transcribed, and the transcript of the hearing itself has not yet been transcribed. Plaintiff's counsel requested an expedited transcript of these items early this morning.

Dockets.Justia.com

3. In the context of the Court's Findings and Rulings, the TRO language is clear and unequivocal, and fairly balances the parties' interests.

4. To date, attorneys from the Electronic Frontier Foundation (the "EFF") have been acting as counsel to the individual defendants in this matter, Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads").

5. In statements to the press, the MIT Undergrads' EFF attorneys have claimed that the TRO is improper, unclear, and illegally restrains the MIT Undergrads' rights under the First Amendment, among other claims.

6. The MBTA has emphasized that it seeks relief to uphold industry standard concepts of "responsible disclosure," and does not seek to impose impermissible restraints on the MIT Undergrads. *See, e.g.,* Complaint ¶ 57; Declaration of Joseph Kelley ¶28; Memorandum in Support of Motion for Temporary Restraining Order at iv-vi.

7. To further demonstrate its desire to act in accordance with "responsible disclosure," the MBTA has offered in writing to immediately mediate this dispute, in order to seek a method for balancing all parties' interests in a tailored manner. *See* Declaration Of Ieuan G. Mahony In Support Of Plaintiff's Motion To Modify Terms But Not Duration Of Temporary Restraining Order ("Mahony 8/11 Decl.") at ¶¶5, 7-8; 8/11 Exhibits 3, 5.

8. The EFF has declined to respond to the MBTA's request, and instead demands that the TRO be lifted in full. Mahony 8/11 Decl. at ¶6; 8/11 Exhibit 4.

9. To correct any public or intra-party misperception concerning the TRO and the MBTA's goals in this matter, the MBTA requests this Court to modify the TRO as follows:

10. The current TRO reads as follows, in operative part:

> [I]t is hereby ORDERED as follows: … [t]hat the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ. P.

> 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attach the security of the Fare Media System.

11. The MBTA requests that this language be modified by the inclusion of the term "non-public" as indicated by the bolded-underlined language that follows:

> [I]t is hereby ORDERED as follows: … [t]hat the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ. P. 65(b)(2), from providing **non-public** program, information, software code, or command that would assist another in any material way to circumvent or otherwise attach the security of the Fare Media System.

12. The MBTA believes that this language is warranted, indeed required by the text of the Courts Findings and Rulings. Moreover, the MBTA has no desire to prevent the MIT Undergrads from discussing materials, code, information, or ideas that are in the public domain.

13. Instead, as the MBTA has made clear both in its court filings and in communications with Defendants' counsel, the MBTA seeks as soon as it practicable to understand what sensitive information – if any – the MIT Undergrads may (or may not) have learned through their conduct as evidenced in part (a) by the Presentation attached as Exhibit 7 to the Supplemental Declaration of Ieuan G. Mahony; (b) by the Report attached as Exhibit 1 to the Declaration of Scott Henderson; and (c) by the Initial and Revised Announcements.

14. The MBTA believes that the most efficient, and balanced method for sharing this information is via non-binding, confidential mediation. The MBTA, accordingly, has committed to mediate this matter in writing.

15. In arguing "first amendment rights" and "prior restraint," the MIT Undergrads' EFF counsel ignores the MBTA's attempts to uncover whether this is in fact a "prank", or whether the MIT Undergrads are in fact able to compromise the Fare Media System in the manner they publicly claim.

16. Therefore, to demonstrate that the MBTA is in fact only concerned with the core issue of immediate concern in this case – the security and integrity of its Fare Media System — the MBTA affirmatively moves to limit to further eliminate claimed First Amendment concerns, and in the hope of obtaining some level of constructive discourse with the EFF's clients without Court involvement.

Conclusion

THEREFORE, the plaintiff respectfully requests that this Court modify the Temporary Restraining Order as stated above.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

CERTIFICATE PURSUANT TO LOCAL RULE 7.1

The undersigned counsel for the Massachusetts Bay Transportation Authority hereby certifies that he has sought to confer with defendants' counsel in a good faith effort to resolve or narrow any issues related to this motion. MBTA Counsel has conferred in detail with counsel for MIT on the present motion. Given press statements by EFF counsel for the MIT Undergrads, the position of EFF counsel's refusal to respond concerning the MBTA's proposals to discuss the TRO and other relevant matters via mediation, I perceived there to be little time available to conduct such conferences, and little likelihood of reasonable results at this point from EFF counsel. Further details concerning these points are provided in the Declaration of Ieuan G. Mahony in Support of Plaintiff's Motion To Modify Terms But Not Duration Of Temporary Restraining Order.

/s/ Ieuan G. Mahony

Dated: August 11, 2008
Boston, Massachusetts

5530567_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

DECLARATION OF IEUAN G. MAHONY IN SUPPORT OF PLAINTIFF'S MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER

1. I am a partner at Holland & Knight, LLP, representing the Massachusetts Bay Transportation Authority ("MBTA") in this matter. The following supplements my earlier Declarations in this matter.

The TRO

2. A true and accurate copy of the Temporary Restraining Order that entered in this case on Saturday (the "TRO") is included as Exhibit 1 in the Exhibits in Support of Plaintiff's Motion To Modify Terms But Not Duration Of Temporary Restraining Order (the "8/11 Exhibits").

Relevant Position of EEF Counsel for the MIT Undergrads'

3. By telephone conversation and shortly thereafter by email dated Saturday, August 9 at 5:14 PM EFF counsel for the MIT Undergrads ("EFF Counsel") informed me that she believed the MBTA should "take emergency measures" before this Court based on Court filings in this matter. *See* 8/11 Exhibit 2.

4. By email dated Sunday, August 10 at 9:27 AM I informed EFF Counsel that the MBTA and one of its vendors had completed review of the matters addressed in her earlier email (Ex. 2), and would be responding with conclusions later on Sunday. *See* Exhibit 3.

The MBTA Proposes Mediation

5. By email dated Sunday, August 10 at 3:18 PM, I responded with the MBTA's conclusions, informed EFF counsel that the MBTA and counsel did not see a basis for taking the "emergency measures" suggested, and proposed that the parties engage in expedited mediation to seek a negotiated resolution. *See* Exhibit 3.

6. By email dated Monday August 11 at 12:27 AM, EFF counsel declined to respond to the MBTA's mediation proposal, and instead requested that the TRO be dissolved in full. *See* Exhibit 4.

EFF Counsel Ignores This Proposal;
The MBTA Again Requests Expedited Mediation

7. By email dated Monday, August 11 at 3:36 PM, I responded with reasons why dissolving the TRO in full was not acceptable, noted perceived misinformation in the news media concerning the matter, re-emphasized the MBTA's desire to avoid all but necessary restraint on the MIT Undergrads, and again proposed mediation, on an expedited basis.

8. In this email, the MBTA again explained its interest in understanding what sensitive information, if any, the MIT Undergrads had obtained, as the first priority.

9. At approximately 3:45 PM on Monday, August 11, I called Defense Counsel and explained the MBTA's intent to file the current Motion.

Signed under the penalties of perjury this 11th day of August, 2008.

/s/ Ieuan G. Mahony
Ieuan G. Mahony

5533212_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

EXHIBITS IN SUPPORT OF
PLAINTIFF'S MOTION TO MODIFY TERMS BUT NOT DURATION OF
TEMPORARY RESTRAINING ORDER

Exhibit	**Description**
1.	Temporary Restraining Order.
2.	Email dated Saturday, August 9 at 5:14 PM.
3.	Email dated Sunday, August 10 at 9:27 AM *and* email dated Sunday, August 10 at 3:18 PM.
4.	Email dated Monday, August 11 at 12:27 AM.
5.	Email dated Monday, August 11 at 11:37 AM *and* email dated Monday, August 11 at 3:36 PM.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III_____
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

5533212_v1

Exhibit 1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

TEMPORARY RESTRAINING ORDER

After hearing this day and upon consideration of the written and oral submissions of the parties regarding the Plaintiff's Motion for Temporary Restraining Order, for the reasons stated orally from the bench at the conclusion of the hearing, it is hereby ORDERED as follows:

A. That the following terms herein shall have the following definitions:

(1) Fare Media System. The term "Fare Media System" means the plaintiff's system that meets the following two criteria: the system (i) is employed by the MBTA to manage, track, charge for, and collect fares; and (ii) relies on CharlieTicket passes and/or CharlieCard passes.

(2) MIT Undergrads. The term "MIT Undergrads" means the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa and all persons in active concert or participation with any of them.

B. That the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ P. 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System

DONE AND ORDERED in Boston, Massachusetts at 1:30 pm this 9th day of August 2008.

/s/ Douglas P. Woodlock

DOUGLAS P. WOODLOCK
UNITED STATES DISTRICT JUDGE

5533219_v1

Exhibit 2

From: Jennifer Granick [mailto:jennifer@eff.org]
Sent: Saturday, August 09, 2008 5:14 PM
To: Mahony, Ieuan (BOS - X75835)
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann
Subject: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Mr. Mahony:

This email is to follow up on my phone call to you of just a few minutes ago. As you know, Mr. Anderson, Mr. Ryan and Mr. Chiesa provided your client MBTA with a confidential three page summary of their research and recommendations for securing the fare collection system. It has just come to our attention through third parties at the Defcon conference that plaintiffs have made this report publicly available on the court's pacer website by filing the document as an exhibit. This confidential document contains the checksum information without which an attacker can not create a forged card. This information is highly sensitive, which is why my clients planned to withhold it from their presentation. We strongly urge you to take emergency measures to have it removed expeditiously.

Best wishes,

Jennifer Granick

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

Exhibit 3

From: Mahony, Ieuan (BOS - X75835)
Sent: Sunday, August 10, 2008 3:18 PM
To: 'Jennifer Granick'
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann; William Mitchell; 'Scott Darling'; Mahony, Ieuan (BOS - X75835)
Subject: RE: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Jennifer:
Let me address your email and phone call from yesterday, and also return to earlier discussions over a "moving-forward" relationship between the parties.

(A) Your Email

First, we want to thank you for your concern. Second, as I indicated earlier today, the MBTA, along with a system vendor, has completed its review of your email, and re-reviewed the three page summary report attached as Exhibit 1 to Scott Henderson's Declaration (the "Report"). This review does not alter the original assessment of the Report, provided by Mr. Henderson in his declaration. Yet it is the case that (a) the quantity and quality of information provided by the three page Report, standing alone, is less than (b) the quantity and quality of the information provided by the Report read in combination with the Students' 87 page presentation entitled "Anatomy of a Subway Hack" (the "Presentation"). If the MBTA had been given the Presentation when first requested (or even at the time when the Presentation , we understand, was made available to DEFCON attendees), the "(b)" circumstance might have been avoided. In any event, the MBTA's evaluators do not assess the risk of this information at the level you set in your email.

The MBTA, with vendor support, has begun work on internal responses to the potential security risks at issue. It is our view that an internal, technical and personnel response is the best long-term solution. Accordingly, we do not share your view that legal "emergency measures" are required. We do not think that seeking court relief on this issue and at this point is appropriate. Again, thank you for your concern.

(B) Moving-Forward Relationships

We can see from your clients' statements in the press, and the EFF's public statements, that the lawsuit generally, and Temporary Restraining Order in particular, do not from your perspectives represent a fair or balanced situation. From my first conversations with Marcia and Kurt, and then later with you, Jennifer, I stated my view that parties, acting reasonably, will invariably develop and implement a resolution of a dispute that is substantially better tailored to their interests than a resolution imposed on them by an external authority.

We think we should continue discussions, to see if we can find a solution that is better tailored to all parties' interests. In my view, Judge Woodlock, in his findings and rulings, directed the parties to work toward a solution perhaps more "creative" and "outside the box" than the standard "keep fighting in court over abstract issues while life goes by". The goal would be to shift from an adversarial mode to a cooperative, discussion mode, if possible. We respect your clients' continued statements that their goal remains to provide solutions to security risks.

We propose formal mediation as the process for seeking a more optimal going-forward solution. We think we should reserve a full day, or perhaps two. We suggest that the mediation take place in Boston. Other issues, such as mediator costs, whether formal "written submissions" are exchanged, and the like we can discuss.

Let us know your thoughts.

Thanks

Ieuan

From: Mahony, Ieuan (BOS - X75835)
Sent: Sunday, August 10, 2008 9:27 AM
To: 'Jennifer Granick'
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann; Mahony, Ieuan (BOS - X75835)
Subject: RE: CRITICAL INFORMATION: MBTA v Anderson et al

Jennifer:
The MBTA and one of its vendors have completed review per your email, below. I'll have results to you later today.

I'll continue to keep you informed.
Thanks

Ieuan

From: Jennifer Granick [mailto:jennifer@eff.org]
Sent: Saturday, August 09, 2008 5:14 PM
To: Mahony, Ieuan (BOS - X75835)
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann
Subject: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Mr. Mahony:

This email is to follow up on my phone call to you of just a few minutes ago. As you know, Mr. Anderson, Mr. Ryan and Mr. Chiesa provided your client MBTA with a confidential three page summary of their research and recommendations for securing the fare collection system. It has just come to our attention through third parties at the Defcon conference that plaintiffs have made this report publicly available on the court's pacer website by filing the document as an exhibit. This confidential document contains the checksum information without which an attacker can not create a forged card. This information is highly sensitive, which is why my clients planned to withhold it from their presentation. We strongly urge you to take emergency measures to have it removed expeditiously.

Best wishes,

Jennifer Granick

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

Exhibit 4

From: Jennifer Granick [mailto:jennifer@eff.org]
Sent: Monday, August 11, 2008 12:27 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: cindy@eff.org; kurt@eff.org; marcia@eff.org; WMitchell@mbta.com; SDarling@mbta.com
Subject: Re: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Ieuan:

Thank you for your thoughts. I'm surprised your client feels that the Report does not pose a risk, given that it contains information my clients intended to keep confidential. It appears my clients are more cautious about disclosing vulnerability information than yours are. Moving forward, both the slides from our client's intended presentation and the confidential Report are now publicly available. This constitutes more information than the students would have presented at their Defcon talk. Furthermore, your client reportedly does not feel that the security risk posed by the availability of this information warrants emergency measures. Finally, Defcon is over and the students did not give their talk. Under these circumstances, would your client be willing to stipulate to lifting the TRO at this time? While the protection it provides is now moot as to your client's concerns, it continues to hang over our clients' heads, making them uncertain what if anything they can say about their research and this case. Please let me know right away.

Thank you,

Jennifer

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

On Aug 10, 2008, at 12:18 PM, <ieuan.mahony@hklaw.com> <ieuan.mahony@hklaw.com> wrote:

> Dear Jennifer:
> Let me address your email and phone call from yesterday, and also return to earlier discussions over a "moving-forward" relationship between the parties.
> **(A) Your Email**
> First, we want to thank you for your concern. Second, as I indicated earlier today, the MBTA, along with a system vendor, has completed its review of your email, and re-reviewed the three page

summary report attached as Exhibit 1 to Scott Henderson's Declaration (the "Report"). This review does not alter the original assessment of the Report, provided by Mr. Henderson in his declaration. Yet it is the case that (a) the quantity and quality of information provided by the three page Report, standing alone, is less than (b) the quantity and quality of the information provided by the Report read in combination with the Students' 87 page presentation entitled "Anatomy of a Subway Hack" (the "Presentation"). If the MBTA had been given the Presentation when first requested (or even at the time when the Presentation , we understand, was made available to DEFCON attendees), the "(b)" circumstance might have been avoided. In any event, the MBTA's evaluators do not assess the risk of this information at the level you set in your email.

The MBTA, with vendor support, has begun work on internal responses to the potential security risks at issue. It is our view that an internal, technical and personnel response is the best long-term solution. Accordingly, we do not share your view that legal "emergency measures" are required. We do not think that seeking court relief on this issue and at this point is appropriate. Again, thank you for your concern.

(B) Moving-Forward Relationships

We can see from your clients' statements in the press, and the EFF's public statements, that the lawsuit generally, and Temporary Restraining Order in particular, do not from your perspectives represent a fair or balanced situation. From my first conversations with Marcia and Kurt, and then later with you, Jennifer, I stated my view that parties, acting reasonably, will invariably develop and implement a resolution of a dispute that is substantially better tailored to their interests than a resolution imposed on them by an external authority.

We think we should continue discussions, to see if we can find a solution that is better tailored to all parties' interests. In my view, Judge Woodlock, in his findings and rulings, directed the parties to work toward a solution perhaps more "creative" and "outside the box" than the standard "keep fighting in court over abstract issues while life goes by". The goal would be to shift from an adversarial mode to a cooperative, discussion mode, if possible. We respect your clients' continued statements that their goal remains to provide solutions to security risks.

We propose formal mediation as the process for seeking a more optimal going-forward solution. We think we should reserve a full day, or perhaps two. We suggest that the mediation take place in Boston. Other issues, such as mediator costs, whether formal "written submissions" are exchanged, and the like we can discuss.

Let us know your thoughts.

Thanks

Ieuan

From: Mahony, Ieuan (BOS - X75835)
Sent: Sunday, August 10, 2008 9:27 AM
To: 'Jennifer Granick'
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann; Mahony, Ieuan (BOS - X75835)
Subject: RE: CRITICAL INFORMATION: MBTA v Anderson et al

Jennifer:

The MBTA and one of its vendors have completed review per your email, below. I'll have results to you later today.

I'll continue to keep you informed.

Thanks

Ieuan

From: Jennifer Granick [mailto:jennifer@eff.org]
Sent: Saturday, August 09, 2008 5:14 PM
To: Mahony, Ieuan (BOS - X75835)
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann
Subject: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Mr. Mahony:

This email is to follow up on my phone call to you of just a few minutes ago. As you know, Mr. Anderson, Mr. Ryan and Mr. Chiesa provided your client MBTA with a

confidential three page summary of their research and recommendations for securing the fare collection system. It has just come to our attention through third parties at the Defcon conference that plaintiffs have made this report publicly available on the court's pacer website by filing the document as an exhibit. This confidential document contains the checksum information without which an attacker can not create a forged card. This information is highly sensitive, which is why my clients planned to withhold it from their presentation. We strongly urge you to take emergency measures to have it removed expeditiously.

Best wishes,

Jennifer Granick

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

Exhibit 5

From: Mahony, Ieuan (BOS - X75835)
Sent: Monday, August 11, 2008 3:36 PM
To: 'jennifer@eff.org'
Cc: 'cindy@eff.org'; 'kurt@eff.org'; 'marcia@eff.org'; JSwope@eadplaw.com; 'WMitchell@mbta.com'; 'SDarling@mbta.com'
Subject: RE: CRITICAL INFORMATION: MBTA v Anderson et al

Jennifer:
We are unwilling to lift the TRO in the binary "on/off" manner you state, and respond more fully to your email as follows:

(A) Removing the TRO Is Not a Tailored Solution

We are willing to discuss tailored solutions to the underlying problem, and have proposed a formal mediation process for these discussions. You have given no response to our proposal for mediation. You recall that I asked for a negotiated solution before the Saturday hearing. I confirmed these inquiries to you in email, and these emails are public record and freely available on the web. See http://www-tech.mit.edu/V128/N30/subway.html. You did not respond meaningfully to those requests, either.

(B) Misinformation Threatens To Cloud the Issues

In following the DEFCON-related press, it is clear that a large amount of misinformation has been circulated concerning the meaning of the TRO, and related points. For example, you know, because Judge Woodlock asked you these questions in open court, that the primary concern was with the content the students might or might not supply to go with the literal expression embodied in the Presentation, as well as the Report. Press reports suggest that the TRO banned circulation of the paper materials themselves. You know this is incorrect.

Yet your email relies on this theme. We made it clear in our papers: based on the information we have (a large part of which you intentionally withheld from us until 4:38 AM Saturday morning) we do not know what your clients have done or are capable of doing. Their broad statements concerning "free subway rides for life" suggest they are capable of a lot. This is the concern. We would like to create an environment, immediately, where all parties can share the information they feel is warranted, in order to quantify and assess this risk. We would like to "re-do" the August 5 (or 4) meeting, but with more sensitivity, hopefully all around, as to the mutual stakes.

We think a mediated solution presents mutual benefits. The structure of non-binding mediation assures mutual benefits -- or at a minimum a clear assessment of the alternatives to a negotiated solution. In a mediation process, for example, we would hope to discuss and obtain an understanding of the information, if any, the MIT Undgrads hold that might threaten Fare Media System security. We do not set preconditions on a mediation, however, as we stongly believe --

again -- that discussions between reasonable parties toward a resolution are preferable to an externally imposed resolution, where it is possible to avoid such an external resolution.

(C) We Are Very Sensitive To Your Clients' Concerns Over The Restraint

Finally, we believe we understand the point in your email that the TRO "continues to hang over our clients' heads, making them uncertain what if anything they can say about their research and this case." One goal with a mediated solution, working together, would be to reduce or eliminate uncertainty (to the extent uncertainty from a legal or practical perspective exists). Another goal of a mediated solution would be to determine other parameters of responsible disclosure under these circumstances. Yet another goal with a mediated solution might be to "make amends" on all sides, whatever that might mean here. There are countless examples from large to small of relationships that are polarized and entrenched-hostile because of bad choices by both sides shortly after the rift began. We would like to avoid this here, if possible. We think talking in a non-binding, professionally mediated environment is the best way to avoid further misunderstanding, and potential "bad choices."

(D) Conclusion: Renewed Request for Mediation

You request, in an "on/off" manner, that we now "shut off" the TRO. This is traditional advocacy, where the goal is to "win all" and avoid "lose all." With our mediation proposal, we look for, and are willing to accept, gradations between these poles. We believe -- whether in light or not in light of recent history -- that reasonable "win-win" solutions are available, if the parties meet and work through options. We ask that you confer carefully with your clients, and respond to our mediation proposal. We believe that mediation should commence as soon as possible. We have made this proposal to MIT counsel as well.

Let me know

Ieuan

From: Mahony, Ieuan (BOS - X75835)
Sent: Monday, August 11, 2008 11:37 AM
To: 'jennifer@eff.org'
Cc: 'cindy@eff.org'; 'kurt@eff.org'; 'marcia@eff.org'; 'WMitchell@mbta.com'; 'SDarling@mbta.com'
Subject: Re: CRITICAL INFORMATION: MBTA v Anderson et al

Jennifer:
We are considering your proposal. We are having a meeting of senior management on this and related issues this afternoon at 1:30 eastern. I will report our response as soon as it is complete.

I will continue to keep you posted.

Ieuan

Sent from my BlackBerry Wireless Handheld (www.BlackBerry.net)

From: Jennifer Granick
To: Mahony, Ieuan (BOS - X75835)
Cc: cindy@eff.org ; kurt@eff.org ; marcia@eff.org ; WMitchell@mbta.com ; SDarling@mbta.com
Sent: Mon Aug 11 00:26:42 2008
Subject: Re: CRITICAL INFORMATION: MBTA v Anderson et al
Dear Ieuan:

Thank you for your thoughts. I'm surprised your client feels that the Report does not pose a risk, given that it contains information my clients intended to keep confidential. It appears my clients are more cautious about disclosing vulnerability information than yours are. Moving forward, both the slides from our client's intended presentation and the confidential Report are now publicly available. This constitutes more information than the students would have presented at their Defcon talk. Furthermore, your client reportedly does not feel that the security risk posed by the availability of this information warrants emergency measures. Finally, Defcon is over and the students did not give their talk. Under these circumstances, would your client

be willing to stipulate to lifting the TRO at this time? While the protection it provides is now moot as to your client's concerns, it continues to hang over our clients' heads, making them uncertain what if anything they can say about their research and this case. Please let me know right away.

Thank you,

Jennifer

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

On Aug 10, 2008, at 12:18 PM, <ieuan.mahony@hklaw.com> <ieuan.mahony@hklaw.com> wrote:

> Dear Jennifer:
> Let me address your email and phone call from yesterday, and also return to earlier discussions over a "moving-forward" relationship between the parties.
>
> **(A) Your Email**
>
> First, we want to thank you for your concern. Second, as I indicated earlier today, the MBTA, along with a system vendor, has completed its review of your email, and re-reviewed the three page summary report attached as Exhibit 1 to Scott Henderson's Declaration (the "Report"). This review does not alter the original assessment of the Report, provided by Mr. Henderson in his declaration. Yet it is the case that (a) the quantity and quality of information provided by the three page Report, standing alone, is less than (b) the quantity and quality of the information provided by the Report read in combination with the Students' 87 page presentation entitled "Anatomy of a Subway Hack" (the "Presentation"). If the MBTA had been given the Presentation when first requested (or even at the time when the Presentation , we understand, was made available to DEFCON attendees), the "(b)" circumstance might have been avoided. In any event, the MBTA's evaluators do not assess the risk of this information at the level you set in your email.
>
> The MBTA, with vendor support, has begun work on internal responses to the potential security risks at issue. It is our view that an internal, technical and personnel response is the best long-term solution. Accordingly, we do not share your view that legal "emergency measures" are required. We do not think that seeking court relief on this issue and at this point is appropriate. Again, thank you for your concern.
>
> **(B) Moving-Forward Relationships**
>
> We can see from your clients' statements in the press, and the EFF's public statements, that the lawsuit generally, and Temporary Restraining Order in particular, do not from your perspectives represent a fair or balanced situation. From my first conversations with Marcia and Kurt, and then later with you, Jennifer, I stated my view that parties, acting reasonably, will invariably develop and implement a resolution of a dispute that is substantially better tailored to their interests than a resolution imposed on them by an external authority.
>
> We think we should continue discussions, to see if we can find a solution that is better tailored to all parties' interests. In my view, Judge Woodlock, in his findings and rulings, directed the parties to work toward a solution perhaps more "creative" and "outside the box" than the standard "keep fighting in court

over abstract issues while life goes by". The goal would be to shift from an adversarial mode to a cooperative, discussion mode, if possible. We respect your clients' continued statements that their goal remains to provide solutions to security risks.

We propose formal mediation as the process for seeking a more optimal going-forward solution. We think we should reserve a full day, or perhaps two. We suggest that the mediation take place in Boston. Other issues, such as mediator costs, whether formal "written submissions" are exchanged, and the like we can discuss.

Let us know your thoughts.

Thanks

Ieuan

From: Mahony, Ieuan (BOS - X75835)
Sent: Sunday, August 10, 2008 9:27 AM
To: 'Jennifer Granick'
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann; Mahony, Ieuan (BOS - X75835)
Subject: RE: CRITICAL INFORMATION: MBTA v Anderson et al

Jennifer:
The MBTA and one of its vendors have completed review per your email, below. I'll have results to you later today.

I'll continue to keep you informed.
Thanks

Ieuan

From: Jennifer Granick [mailto:jennifer@eff.org]
Sent: Saturday, August 09, 2008 5:14 PM
To: Mahony, Ieuan (BOS - X75835)
Cc: Cindy Cohn; Kurt Opsahl; Marcia Hofmann
Subject: CRITICAL INFORMATION: MBTA v Anderson et al

Dear Mr. Mahony:

This email is to follow up on my phone call to you of just a few minutes ago. As you know, Mr. Anderson, Mr. Ryan and Mr. Chiesa provided your client MBTA with a confidential three page summary of their research and recommendations for securing the fare collection system. It has just come to our attention through third parties at the Defcon conference that plaintiffs have made this report publicly available on the court's pacer website by filing the document as an exhibit. This confidential document contains the checksum information without which an attacker can not create a forged card. This information is highly sensitive, which is why my clients planned to withhold it from their presentation. We strongly urge you to take emergency measures to have it removed expeditiously.

Best wishes,

Jennifer Granick

Civil Liberties Director
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134
fax 415.436.9993
jennifer@eff.org

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

CERTIFICATE OF SERVICE

1. The term "Defense Counsel" for purposes of this Certificate of Service means the following:

Party	Counsel
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Marcia Hofman, Esq. Electronic Frontier Foundation 1875 Connecticut Ave., Suite 650 Washington, DC 20009 202-797-9009 Fax: 202-797-9066 Email: marcia@eff.org Kurt Opsahl Electronic Frontier Foundation 454 Shotwell St. San Francisco, CA 94110 415-436-9333 Fax: 415-436-9993 Email: kurt@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue Boston, Massachusetts 02199 USA

617-239-0100
Fax: 617-227-4420
Email: JSwope@eapdlaw.com

2. I verified the above email addresses for Defense Counsel, either by using the email address by which counsel contacted me via email, or by confirming over the phone that counsel received email I had sent to that email address.

3. I hereby certify that I provided copies of the following documents to Defense Counsel by overnight delivery and email, and to Counsel for MIT by hand delivery, on Monday, August 11, 2008:

(a) Plaintiff's Motion to Modify Terms But Not Duration of Temporary Restraining Order;

(b) Declaration of Ieuan G. Mahony in Support of Plaintiff's Motion to Modify Terms But Not Duration of Temporary Restraining Order; and

(c) Exhibits in Support of Plaintiff's Motion to Modify Terms But Not Duration of Temporary Restraining Order.

/s/ Ieuan G. Mahony
Ieuan G. Mahony

5534398_v1

EXHIBIT 1

From: Manuel Albers [manuel.albers@nxp.com]
Sent: Wednesday, July 30, 2008 5:53 PM
To: shenderson@mbta.com
Cc: Fluegge.Wolfgang@Scheidt-Bachmann.de; bhoene@scheidt-bachmann-usa.com
Subject: Boston Charlie Card Hack Demo subject at speach at upcoming Defcon conference in August

Scott,

FYI: Today we learned about a conference (Defcon) at which a team of MIT students intends to demo a Charlie Card Hack. Of special concern is the announced intent to release open source tools required to perform the attacks:

http://defcon.org/html/defcon-16/dc-16-speakers.html#Anderson

The Anatomy of a Subway Hack:

Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson
Student, MIT
RJ Ryan
Student, MIT
Alessandro Chiesa
Student, MIT

Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of

hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

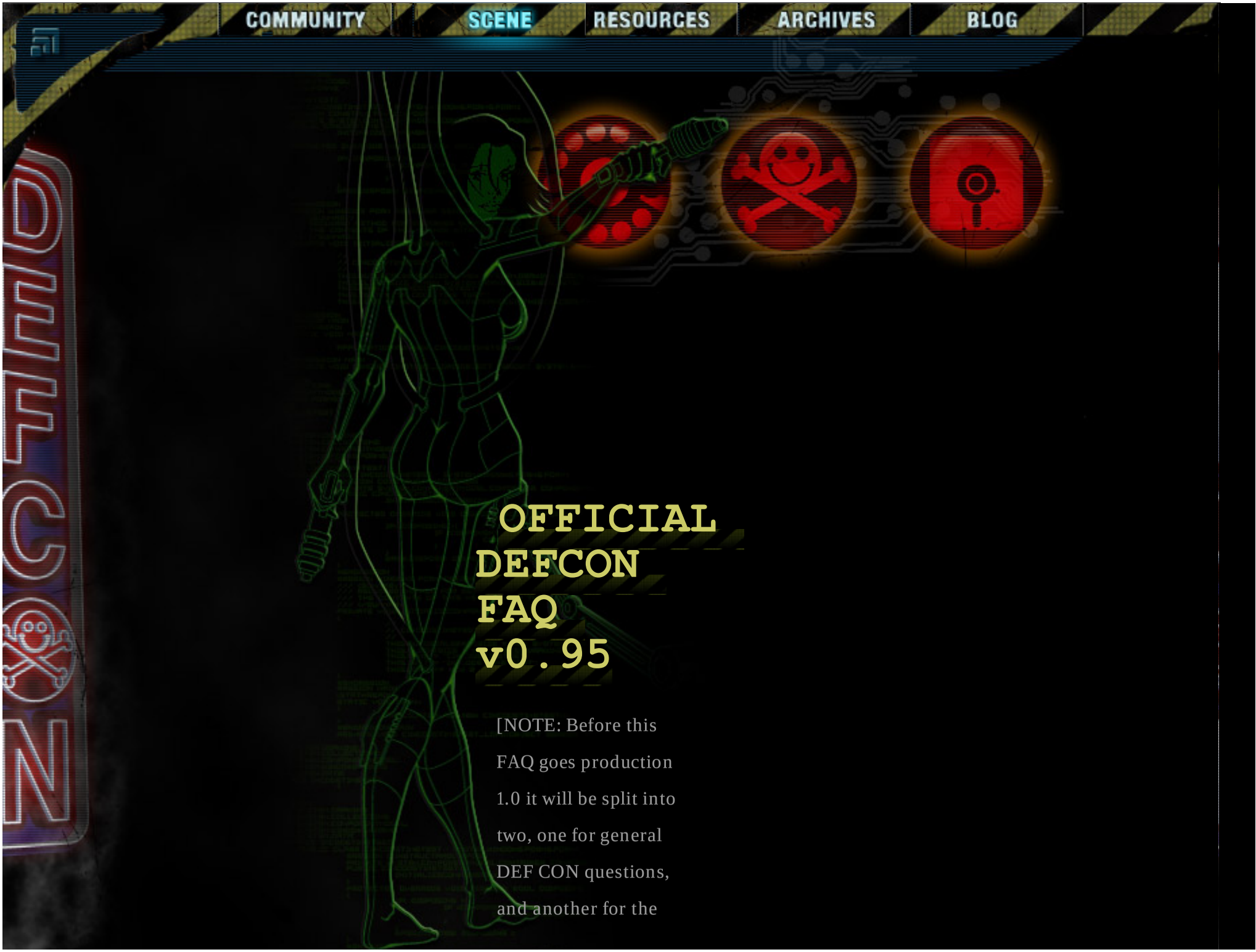
Please let me know if we can support you in any way.

Best regards,
-Manuel Albers

Director, Regional Marketing Americas & BU A&I - Sales & Marketing - Identification & NXP Semiconductors
(P) +1.802.497.0888 & (C) +1.401.359.4999 & (F) +1 866.333.2976 & http://www.NXP.com &
(founded by Philips)

The information contained in this message is confidential and may be legally privileged. The message is intended solely for the addressee(s). If you are not the intended recipient, you are hereby notified that any use, dissemination, or reproduction is strictly prohibited and may be unlawful. If you are not the intended recipient, please contact the sender by return e-mail and destroy all copies of the original message.

EXHIBIT 2


COMMUNITY
SCENE
RESOURCES
ARCHIVES
BLOG
DEFCON
OFFICIAL
DEFCON
FAQ
v0.95
[NOTE: Before this
FAQ goes production
1.0 it will be split into
two, one for general
DEF CON questions,
and another for the

current years con]

What is DEFCON?

DEFCON is one of the oldest continuous running hacker conventions around, and also one of the largest.

How did DEFCON start?

Originally started in 1993, it was a meant to be a party for member of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U. S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the

member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and

remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places. There as a SummerCon in the summer, a HoHoCon in the winter, a PumpCon during Halloween, etc. I didn't want any association with a time of year. If you are a Phreak, or just use your phone a lot you'll notes "DEF" is #3 on the phone. If you are into military lingo DEFCON is short for "Defense Condition."

Now being a fan of the movie War Games I took note that the main character, David Ligntman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEFCON is all about.

DEFCON Press: through the prism of the media

DEFCON Pics: visual evidence, thousands of pictures, some NSFW

DEFCON Groups:

Local groups that meet

DEFCON Media archives: Speeches from DC 1 to the present, captured

Google: always a good research starting point

Just remember, DEFCON is what you make of it.

When and where is DEFCON?

DEFCON is generally in the last week of July or first week of August in Las Vegas. DEFCON 16 will be held August 8-10 at the Riviera Hotel & Casino in Las Vegas. Many people arrive a day early, and many stay a day later.

Isn't there a DEFCON FAQ already?

Yes, an unofficial one. It's quite humorous, somewhat outdated, sometimes informative, and DEFCON takes no responsibility for its content. It can be found at http://defcon.stotan.org/faq/

What are the rules of DEFCON?

Physical violence is prohibited. We don't support illegal drug use. Minors should be accompanied by their parent(s) or guardian

doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEFCON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEFCON. Talking about how you are

going to bomb the RNC convention in front of an FBI agent is a Career Limiting Move!

Is DEFCON canceled?

No.

What is there to do at DEFCON?

DEFCON is a unique experience for each con-goer. If you google around you'll find dozens of write-ups that will give you an idea of what people have experienced at DEFCON. Trust write-ups more than media

articles about the con. Some people play capture the flag 24x7, while many people never touch a computer at DEFCON. Some people see every speech they can, while others miss all speeches. Other activities include coffee wars, WI-FI shoot outs, robot contests, TCP/IP contests, movie marathons, scavenger hunts, sleep deprivation, lock picking, warez trading, drunken parties, spot the fed contest, charity dunk tanks, the Black and White Ball. Because DEFCON is what the attendees make of it, there are

more events than even we are aware of. Half the fun is learning what happened at DEFCON after the fact!

I'm not a hacker, should I go to DEFCON?

Many people have different definitions of what is a 'hacker'. I would recommend looking at previous years speeches, and write-ups from past attendees - this should give you a good idea if DEFCON is for you. This hacker FAQ might give you some insight into the matter as well. If you do not have any technical

interests, DEFCON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEFCON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Ssshhh. Don't tell anyone.

What are Goons?

They are the staff at DEFCON. They have many roles including security, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address. Security Goons generally wear red shirt, Speaker and Content Control wear Blue.

How can I help out

or become a Goon?

The staff at DEFCON has grown organically. All positions have some degree of trust associated with them, so typically new goons are 'inducted' by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work. Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they

actually do (hint: you may want to enjoy being at DEFCON, not working full-time at it). Last year the network group got a new Goon when a networking engineer was need, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEFCON is not a spectator sport! Before

the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirt and posters. You can build a bot for Robot Wars, practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEFCON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually

every official event at DEFCON started out as an unofficial event.

After DEFCON you can help support the conference by posting links to your DEFCON photographs at defconpics.org, writing a review of your experiences and posting it online (Don't forget to mailing us (press [at] DEFCON døt org) a copy) or just sending us feedback so we can improve in the future. If you ran a contest write it up and we'll link to it. If you have the results of a contest or a new event we'd love to hear about it.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEFCON were conceived by the attendees. The DEFCON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEFCON (space, namely) you generally don't have to ask anyone’s permission. Most events are unofficial until they've been going on for a couple of years. Please

let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEFCON døt org] to keep us in the loop.

How can I speak at DEFCON?

You can submit a response to our CFP (call for papers). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers opens March 1, 2008.

I'm press, how do I sign up, why can't I

get in for free (I'm just doing my job)?

Please email press[at] defcon[døt]org if you wish press credentials. Lots of people come to DEFCON and are doing their job; security professionals, federal agents, and the press. It wouldn't be fair to DEFCON attendees if we exempted one group from paying. If you are a major network and plan on doing a two minute piece showing all the people with blue hair, you probably shouldn't bother applying for a press pass - you won't get one. If you are a security writer or from

a real publication please submit, and someone will respond with an answer.

I want to sell stuff, how do I do this?

If you want a space in our vendor area, you need to apply. Because of limited space and our attempt to have a diversity of vendors, you may not be able to get a booth. It is wise to think of staffing issues - if you are one person do you want to spend your entire time behind a vendors booth?

What are the

different price rates?

Everyone pays the same: The government, the media, the 'well known hackers', the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

How much is admission DEFCON, and do you take credit cards?

DEFCON costs $120 USD cash. Do we take credit cards? Are you JOKING? No, we only

accept cash - no checks, no money orders, no travelers checks. We don't want to be a target of any State or Federal fishing expeditions.

Can I pre-register for DEFCON?

No. We used to do this a long time ago, but found that managing the registration list, and preventing one 'Dr. Evil' from impersonating another 'Dr. Ev1l' too much of a hassle. Seeing how we would only take case in the first place, and things becomes time consuming and easy to abuse. Cash at

the door works every time.

DEFCON is too expensive, how can I afford it?

DEFCON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. Many people have made an art and science out of coming to DEFCON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)
Lodging: Share rooms - some people have up

to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)

Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)

Booze: You don't need to drink. Brew your own and bring it. (It's been done.)

Entrance: $120 can be saved, mow some

lawns. Try to go to another 3 day event for cheaper than this that offers so much. We have increased the fees slowly over the years, but also the amount and quality of events have increased. With a new hotel for DC-14 some costs have increased, and we have to pass those along.

Inevitably people will try to do some math and pretend that DT gets rich each DEFCON - they seem to lack the ability to subtract.

How many people typically attend DEFCON?

There have been roughly 3,000-5,000 attendees in the last few years of DEFCON.

Is there a network at DEFCON?

Yes. It would be fair to describe the network as 'hostile'. It has been described as 'the worlds most hostile network', but such descriptions are just attempts at flattery. It is recommended that if you want to connect to the DEFCON network pretend that you are sharing out your entire hard drive to 5,000 hackers. You may want to bring a 'clean' computer that you

don't mind being infected/hacked/etc. It is considered very poor form to attempt to DoS the network; while the DEFCON staff may not do anything about such attempts it is reasonable to assume that 'peer justice' may be meted out. If you're unhappy about the possible risks associated with connecting to DEFCON networks there are a couple of options: refrain from computer use for a few days or connect using another network elsewhere in Vegas (another hotel or something).

At DEFCON 13 we rolled out a new WiFi network using Aruba gear. If you were inside the coverage area of the DEFCON access points the new network switch would do thinks like detect rogue APs and attack them, reset or FIN network connections it didn't like, and prevent one user from being able to scan another user. Nothing is foolproof, but it brought a new level of sanity and stability to the network. We plan to do this again for DC-14. Look in the printed program for the correct MAC and IP address of the gateway router.

What is the age limit?

People have brought children to DEFCON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an 'adult' atmosphere (language, booze, et cetera). If you've never been to DEFCON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have consistently cooperated with parents and/or private investigators who are

looking for children that 'ran away from home' to go to DEFCON. You will have to be 18 to reserve a room.

That said I think NullTone ties with the youngest person to attend DEFCON at 13 year old. Years later he is in college and set up the DEFCON Forums. See, DEFCON won't destroy you completely.

What is a DEFCON "Black Badge"?

The Black Badge is the highest award DEFCON gives to contest winners of

winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEFCON for life— potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of

mail continually. Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

What about having a DEFCON in XYZ city/country?

We've been in the city of sin since DC 1. We are not looking to franchise. It's always fun to see people organize conventions in their local areas, and if you do, we'll include you in our calendar, but not with the name "DEFCON".

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEFCON. This is discussed in quite some depth on the unofficial DC FAQ, as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the Black and White Ball, an annual Saturday night event where everyone shows off nifty attire.

Will the Riviera allow free parking?

Yes. You will be able to park for free

regardless if you have a room at the Riviera.

I looked at a map of the convention space and noticed there are sky boxes. Can I reserve one?

No. If you have any great ideas for what a sky box should be used for, feel free to send us suggestions, but individual attendees will not be able to reserve sky boxes.

How much do rooms at the Riviera cost, and how do I reserve a room?

The Riviera has reservations online or over the phone (800) 634-6753. Room Rates are "flat-fee" based on quantity of occupants. $98 + tax with 1 or 2 people, $118 + tax with 3 or 4 people. Priority for room assignment when you say you're with DEFCON is "Deluxe" when making reservations on the phone.

How much is internet access in the rooms of the Riviera?

$9.00 for 24 hours. Free (and more dangerous) internet access is available for

free in the convention area.

Will the Riviera broadcast the speeches on their cable system?

No. There will be two DEFCON channels that will provide 'extra' content (short clips, hacker related videos, etc.). It is our intention that everyone who wishes to attend a speech will be able to - this was a primary motivation for moving hotels.

Will we have DEFCON branded poker chips?

You will have to attend DEFCON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. The hotel is very cooperative in attempting to centralize the DEFCON attendees, for their convenience and ours, but there will be non-DEFCON attendees in hotel rooms next to us.

This FAQ didn't answer my

unclear, how can I get further information?

There is a forum discussion thread in which you can ask follow up questions.



Get involved with DEFCON Groups in your area!



Discuss hacker related issues at the DEFCON Forums



Upload all your photos and videos from DEFCON at pics.defcon.org

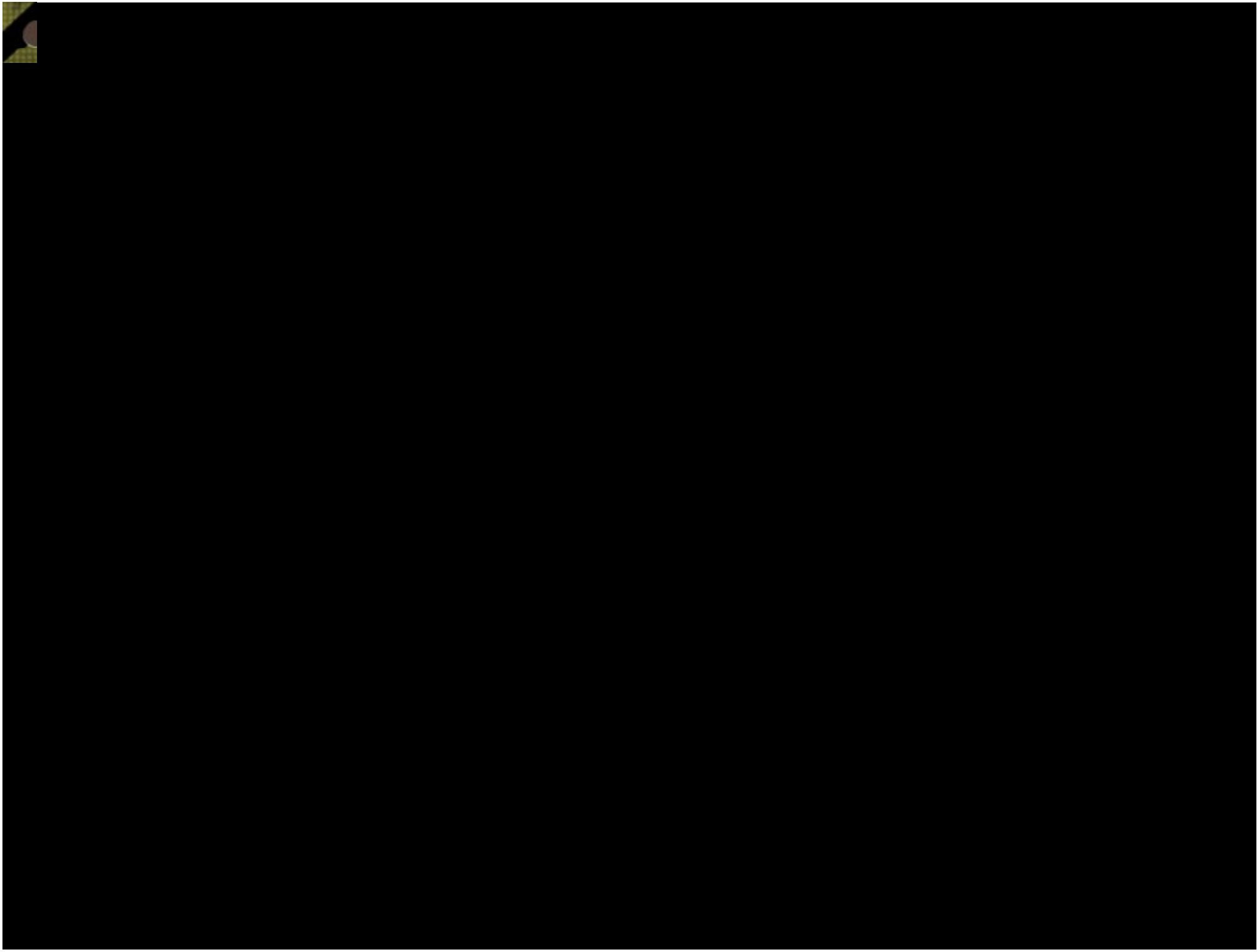


EXHIBIT 3



Schedule
Speakers
Venue
Events/Contests
Be Prepared
FAQ
Contact

Schedule

Skyboxes

Place skybox requests with grifter[at]defcon[dot]org

© 1992-2008 DEF CON Communications, Inc. Main DEFCON Site | RSS

Friday	"Spiders are Fun" party	Hacker pimps		Hardware Hacking Village	Wireless Village	Lockpick Village
Saturday	303 (Skytalks)	Ninja Networks	i-hacked			
Sunday	HAM Radio Testing	Available	Available			

Pre-Con: Thursday, August 7

12:00 - 22:00	Registration - $120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store Vendor Area Setup: 11:00 - 18:00
18:00 - ???	**The Unofficial Defcon 16 Toxic BBQ** will be held for its fourth consecutive year. Details of the TBBQ's location can be found at http://www.toxicbbq.com. Sign on to the Defcon Forums and help plan this year's event.
21:00 - ???	**theSummit** fundraiser for EFF/THF at the Top of the Riv

Day One: Friday, August 8

08:00 - 22:00	Registration - $120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the same area as the Registration desk until 22:00 - Get your official DEFCON swag at the DEFCON Store. Vendor Area Hours: 10:00 - 19:00

	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Chillout 101/102
10:00 - 10:50	**Welcome by DT & Making the DEFCON 16 Badge with Joe "Kingpin" Grand**	**Weasel** Compliance: The Enterprise Vulnerablity Roadmap.	**Chema Alonso & Jose Parada** Time-Based Blind SQL Injections Using Heavy Queries: A Practical Approach to MS SQL Server, MS Acess, Oracle, MySQL Databases and Marathon Tool. 	**Brenno J.S.A de Winter** Hacking Data Retention: Small Sister your Digital Privacy Self Defense. 	**Ben Feinstein** The Wide World of WAFs. 	**oCTF** till 22:00 **Coffee Wars** till 12:00 **Race to Zero** till 18:00 **Buzzword Survivor** till 22:00 Sat **DEFCONBots** practice during Contest Area hours **GH3** Signup till 12:00 **Badge Hacking Contest** till 14:00 Sunday **Mystery Challenge** till 14:00 Sunday		
11:00	**Schuyler**	**Michael**	**Ian Angell**	**Joe Cicero**	**Panel:**	**GH3** Free	**Warballooning**	

11:20	How to make friends & influence Lock Manufacturers. 	Deciphering Captcha 	Security: A Risky Business	E.S.P.	**the Name of Science.**	**The Phreaking Callenge** till 17:00 **Mystery Challenge** Wildcard Slot Competition	Outdoor Area till 14:00	
11:30-11:50		**Kolisar** Whitespace: A Different Approach to JavaScript Obfuscation. 		**Clinton Wong** Web Privacy & Flash Local Shared Objects.				
12:00 - 12:50		**Mike Spindel** Captchas: Are they really Hopeless? (Yes!) 	**Mark Bristow** ModScan: A SCADA MODBUS Network Scanner 	**Roger Dingledine** Security and anonymity vulnerabilities in Tor: past, present, and future		**Scavenger Hunt** till 17:00 **GH3** Med. Heat 1 **Beverage Cooling Contraption Contest**		Chillout Area, DJs **QueerCon Mixer** @ 16:00
13:00 - 13:20	**Marc Weber Tobias** Open in 30 Seconds:	**Tom "Strace" Stracener & Robert**	**Robert Ricks** New Tool for SQL Injection with DNS	**Jim O'Leary** Every Breath you Take.	**Greg Conti** Could Googling Take Down	**GH3** Med. Heat 2 **Mystery**		

	Cracking One of the Most Secure Locks in America. DEMO TOOL EXPLOIT	**"RSnake" Hansen** Xploiting Google Gadgets: Gmalware & Beyond TOOL	Exfiltration. DEMO TOOL	DEMO TOOL	a President, Prime Minister, or an Average Citizen? DEMO	**Challenge** begins at 1:05:70 till 14:00 Sunday	
13:30 - 13:50			**Morgan Marquis-Boire** Fear, Uncertainty and the Digital Armageddon.				
14:00 - 14:50		**Nathan Hamiel & Shawn Moyer** Satan is on my friends list: Attacking Social Networks. DEMO	**Kurt Grutzmacher** Nail the Coffin Shut,NTLM is Dead. DEMO TOOL	**Magnus Bråding** Generic, Decentralized, Unstoppable Anonymity: The Phantom Protocol. TOOL	**Jan Newger** Anti-RE Techniques in DRM Code DEMO	**GH3** Med. Heat 3	**Mobile Hacker Spaces Demo** in outdoor area till 16:00
15:00 - 15:50	**Eric Schmiedl** Advanced Physical Attacks: Going Beyond Social Engineering and Dumpster Diving Or, Techniques of Industrial	**Wendel Guglielmetti Henrique** Playing with Web Application Firewalls. DEMO	**Kevin Figueroa, Marco Figueroa, & Anthony L. Williams** VLANs Layer 2 Attacks: Their Relevance		**Alex Stamos, David Thiel & Justine Osborne** Living in the RIA. DEMO		

	Espionage		and their Kryptonite. DEMO					
16:00 - 16:50	**David Maynor & Robert Graham** Bringing Sexy Back: Breaking in with Style. DEMO TOOL EXPLOIT	**Fyodor** NMAP- Scanning the Internet. DEMO TOOL	**James Shewmaker** StegoFS DEMO TOOL	**Blake Self & Durandal** Free Anonymous Internet Using Modified Cable Modems. DEMO	**Travis Goodspeed** Journey to the center of the HP28.			
17:00 - 17:50	**Matt Yoder** Death Envelope: Medieval Solution to a 21st Century Problem.	**Ben Feinstein** Snort Plug-in Development: Teaching an Old Pig New Tricks. DEMO TOOL	**D.J. Capelis** Building a Real Session Layer. DEMO TOOL	**Vic Vandal** Keeping Secret Secrets Secret & Sharing Secret Secrets Secretly. DEMO	**Panel: Meet the Feds**			
18:00 - 18:50	**Fabian "Fabs" Yamaguchi & FX** New Ideas for	**Guy Martin** Sniffing Cable Modems. DEMO	**John Fitzpatrick** Virtually Hacking. DEMO	**Eric Smith & Dr. Shana Dardan.** Medical Identity Theft.				Closed for Ball Setup

	Port Scanning Improved. DEMO TOOL	TOOL	TOOL	DEMO				
19:00 - 19:20				**Nathan Evans** De-TOR-iorate Anonymity				
19:30 - 19:50								
20:00 - 20:50				**TCP/IP Drinking Game**			**Forum Meet** @ 20:30 in Q&A 5 (room 103) till 22:30	**Black Ball** till 3:00 Sat.
21:00 - 21:50	Movie Night With DT: Premiere of "**Hackers Are People Too**"			**Hacker Jeopardy**				
22:00 - 22:50	Movie Night With DT: **Appleseed: Ex Machina**						**Club QueerCon** in Skybox 211 till ???	
23:00 -								

Day Two: Saturday, August 9

08:00 - 22:00	Registration - $120 USD CASH ONLY - Avoid the lines and get your badge early. Official DEFCON Store in the Vendor Area at the J!nx Hackwear Booth Vendor Area Hours: 10:00 - 19:00							
	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Chillout 101/102
10:00 - 10:50	**David Weston & Tiller Beauchamp** RE:Trace: The Reverse Engineer's Unexpected Swiss Army Knife. 	**Nelson Murilo & Luiz "effffn" Eduardo** Beholder: New WiFi Monitor Tool. 	**Don Blumenthal** Working With Law Enforcement.	**Joe "kingpin" Grand & Zoz** BSODomizer. 	**G.Mark Hardy** A Hacker Looks at 50.	**oCTF** till 22:00 **Øwn the Box** in oCTF Area during oCTF Hours	**Skytalks** in Skybox 206 till 18:00	
11:00 - 11:50	**Matt Weir & Suhir Aggarwal** Password Cracking on a Budget. 	**Thomas d'Otreppe de Bouvette** **"Mister X" & Rick Farina "Zero_Chaos"** Shifting the Focus of WiFi Security: Beyond Cracking your neighbor's	**Scott Moulton** Forensics is ONLY for Private Investigators.	**Cameron Hotchkies** Under the iHood.	**Ferdinand Schober** Gaming- The Next Overlooked Security Hole.	**GH3** Free Play **Gringo Warrior** till 18:00	**Warballooning Demo** in Outdoor Area till 14:00	

		WEP key. 						
12:00 - 12:50	**FX** Developments in Cisco IOS Forensics. 	**Matt "DCFLuX" Krick** Flux on:EAS (Emergency Alert System) 	**John "Jur1st" Benson**. When Lawyers Attack! Dealing with the New Rules of Electronic Discovery.	**Jay Beale** Owning the Users with Agent in the Middle. 	**"Ne0nRa1n" & Joe "Kingpin" Grand** Brain Games: Make your own Biofeedback Video Game. 	**Scavenger Hunt** till 18:00 **GH3** Hard Heat 1		Chillout Area, DJs
13:00 - 13:50	**Adam Bregenzer** Buying Time- What is your Data Worth? (A Generalized Solution to Distributed Brute Force Attacks.) 	**Alexander Lash** Taking Back your Cellphone. 		**Luciano Bello & Maximiliano Bertacchini** Predictable RNG in the Vulnerable Debian OpenSSL Package, the What and the How. 	**Ian Clarke** Hacking Desire. 	**DEFCONBots** **GH3** Hard Heat 2 **The Phreaking Callenge** till 17:00 **EEE PC Mod Workshop** meetup till 15:00		

14:00 - 14:50	**Panel: All your Sploits (and Servers) are belong to us.** 	**Major Malfunction** Feed my SAT Monkey. 	**Panel: Ask the EFF:** The Year in Digital Civil Liberties Panel	**SensePost** Pushing the Camel through the eye of a needle. 	Lyn Tuning Your Brain. 	**GH3** Expert Heat	Mobile **Hacker Spaces Demo** in outdoor area till 16:00
15:00 - 15:50		**Zac Franken** Is that a unique credential in your pocket or are you just pleased to see me?		**Mati Aharoni** BackTrack Foo- From bug to 0day. 	**Phreakmonkey & mutantMandias** Urban Exploration- A Hacker's View.	**GH3** Finals Med. **GH3** Finals Hard @ 15:30	
16:00 - 16:20	**Michael Brooks** CSRF Bouncing. 	**Mike Perry** 365-Day:Active https cookie hijacking. 	**Panel: Commission on Cyber Security for the 44th Presidency**	**atlas** VulnCatcher: Fun with Vtrace & Programmatic Debugging. 	**Lee Kushner & Mike Murray** Career Mythbusters: Separating Fact from Fiction in your Information Security Career.	**GH3** Finals Expert	
16:30 - 16:50		**MD Sohail Ahmad, JVR Murthy & Amit Vartak**					

		Disorder in Wireless LANs. 						
17:00 - 17:20	**Felix "FX" Lindner** Toying With Barcodes	**NYCMIKE** The World of Pager Sniffing/ Interception: More Activity than one may suspect.	**Don Blumenthal** What to do when your Data winds up where it shouldn't.	**David Byrne** Grendel-Scan: A New Web Application Scanning Tool. 	**Christopher Tarnovsky** Introducing Momentary Faults Within Secure Smartcards/ Microcontrollers. 			
17:20 - 17:50		**Fouad Kiamilev & Ryan Hoover** Demonstration of Hardware Trojans. 						
18:00 - 18:50	**Paul F. Renda** The True Story of the Radioactive Boyscout: The first Nuclear Hacker & how his work relates to Homeland	**Scott Moulton** Solid State Drives Destroy Forensic & Data Recovery Jobs: Animated! 	**TBA**	**Renderman** How can I pwn thee? Let me count the ways.				Closed for Ball Setup

	Security's model of the dirty bomb. 							
19:00 - 19:50	Movie Night With DT: 25th Anniversary Showing of **Wargames** Followed by a fireside chat with David Scott Lewis, IT & green tech entrepreneur, model for David Lightman							
20:00 - 20:50				**LeetSkills Talent Competition**				
21:00 - 21:50				**Hacker Jeopardy**				**White Ball** till 3:00 Sunday
22:00 - 22:50	Movie Night With DT: **Three Days of the Condor**							
23:00 - ????								

Day Three: Sunday, August 10

08:00 - 12:00	Official DEFCON Store in the Vendor Area at the J!nx Hackwear Booth Vendor Area Hours: 10:00 - 15:00							
	Track 1	Track 2	Track 3	Track 4	Track 5	Contest Area	Events	Room
10:00 - 10:20	**Bruce Potter** Malware Detection through Network Flow Analysis. 	**Brian K. Edwards** Markets for Malware: A Structural Economic Approach	**Tony Howlett** The death of Cash: The Loss of anonymity & other danger of the cash free society.	**Christer Oberg, Claes Nyberg, & James Tusini** Hacking Open VMS. 	**Stefan Frei, Thomas Duebendorfer, Gunter Ollman & Martin May** Exploiting A Hundred-Million Hosts Before Brunch			
10:30 - 10:50		**Ryan Trost** Evade IDS/IPS Systems using Geospatial Threat Detection. 	**Peter Berghammer** The Emergence (and use) of Open Source Warfare.		**JonM** Ham for Hackers-Take back the Airwaves. 			
11:00 - 11:50	**Rick Hill** War Ballooning-Kismet Wireless "Eye in the Sky" 	**Dan Kaminsky** TBA	**Sandy Clark "Mouse"** Climbing Everest: An Insider's Look at one state's Voting Systems.	**N.N.P.** VoIPER:Smashing the VoIP Stack while you sleep. 	**Nick Harbour** Advanced Software Armoring and Polymorphic Kung Fu 			

				EXPLOIT	TOOL			
12:00 - 12:20	**Simon Howard** Race-2-Zero Unpacked. DEMO	**Teo Sze Siong & Hirosh Joseph** Let's Sink the Phishermen's Boat! DEMO	**Doug Farre** Identification Card Security: Past, Present, Future. DEMO	**Jay Beale** They're Hacking Our Clients! Introducing Free Client-side Intrustion Prevention. DEMO TOOL EXPLOIT	**Valsmith & Colin Ames** MetaPost-Exploitation DEMO TOOL			
12:30 - 12:50		**Renderman** 10 Things that are Pissing me off.						
13:00 - 13:50	**Thomas Wilhelm** Mobile Hacker Space. DEMO	**Anthony Martinez & Thomas Bowen** Toasterkit, a Modular NetBSD Rootkit. DEMO TOOL	**Zack Anderson, RJ Ryan & Alessandro Chiesa** The Anatomy of a Subway Hack: Breaking Crypto RFID's & Magstripes of Ticketing Systems. DEMO TOOL	**Paul Craig** Compromising Windows Based Internet Kiosks. DEMO TOOL	**Jonathan Brossard** Bypassing pre-boot authentication passwords	**The Phreaking Callenge** till 14:30		

14:00 - 14:50	**Panel: Internet Wars**	**Michael Ligh & Greg Sinclair** Malware RCE: Debuggers and Decryptor Development. DEMO TOOL	**Mike Renlund** The Big Picture: Digital Cinema Technology & Security.	**Panel: Black vs. White: The complete life cycle of a real world breach.** DEMO TOOL	**DAVIX Visualization Workshop**		**Mobile Hacker Spaces Demo** in outdoor area till 16:00	
15:00 - 15:50	**Jason Scott** Making a Text Adventure Documentary. DEMO TOOL	**Igor Muttik** Good Viruses. Evaluating the Risks. DEMO	**Taylor Banks & Carric.** Pen-Testing is Dead, Long live the Pen Test.					
16:00 - 16:50		**Chris Eagle & Tim Vidas** Next Generation Collaborative Reversing with IdaPro &CollabReate. DEMO TOOL	**Tottenkoph, Rev & Philosopher** Hijacking the Outdoor Digital Billboard Network. EXPLOIT	**Iclee_vx** Comparison of File Infection on Windows & Linux. DEMO				
17:00 - 17:50	**Awards Ceremonies hosted by Dark Tangent**							

EXHIBIT 4

The Anatomy of a Subway Hack:
Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson *Student, MIT*
RJ Ryan *Student, MIT*
Alessandro Chiesa *Student, MIT*

In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

José Parada is an IT Pro Evangelist in Microsoft. He is a very famous speaker in Spanish conferences about IT Infrastructures, Microsoft Technologies and Security. He has been working in the Microsoft Technet Program from 2005 delivering conferences, webcasts and technical information.

Top of page

The Anatomy of a Subway Hack:
Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack Anderson*Student, MIT*
RJ Ryan*Student, MIT*
Alessandro Chiesa*Student, MIT*

In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

Top of page

Digital Security: a Risky Business
Ian O. Angell*Professor of Information Systems. London School of Economics*

In this talk Professor Angell will take the devil’s advocate position, warning that computer technology is part of the problem as well as of the solution. The belief system at the core of computerization is positivist and/or statistical, and that itself leads to risk. The mixture of

EXHIBIT 5

Schematic Illustrating the MBTA's Fare Media System

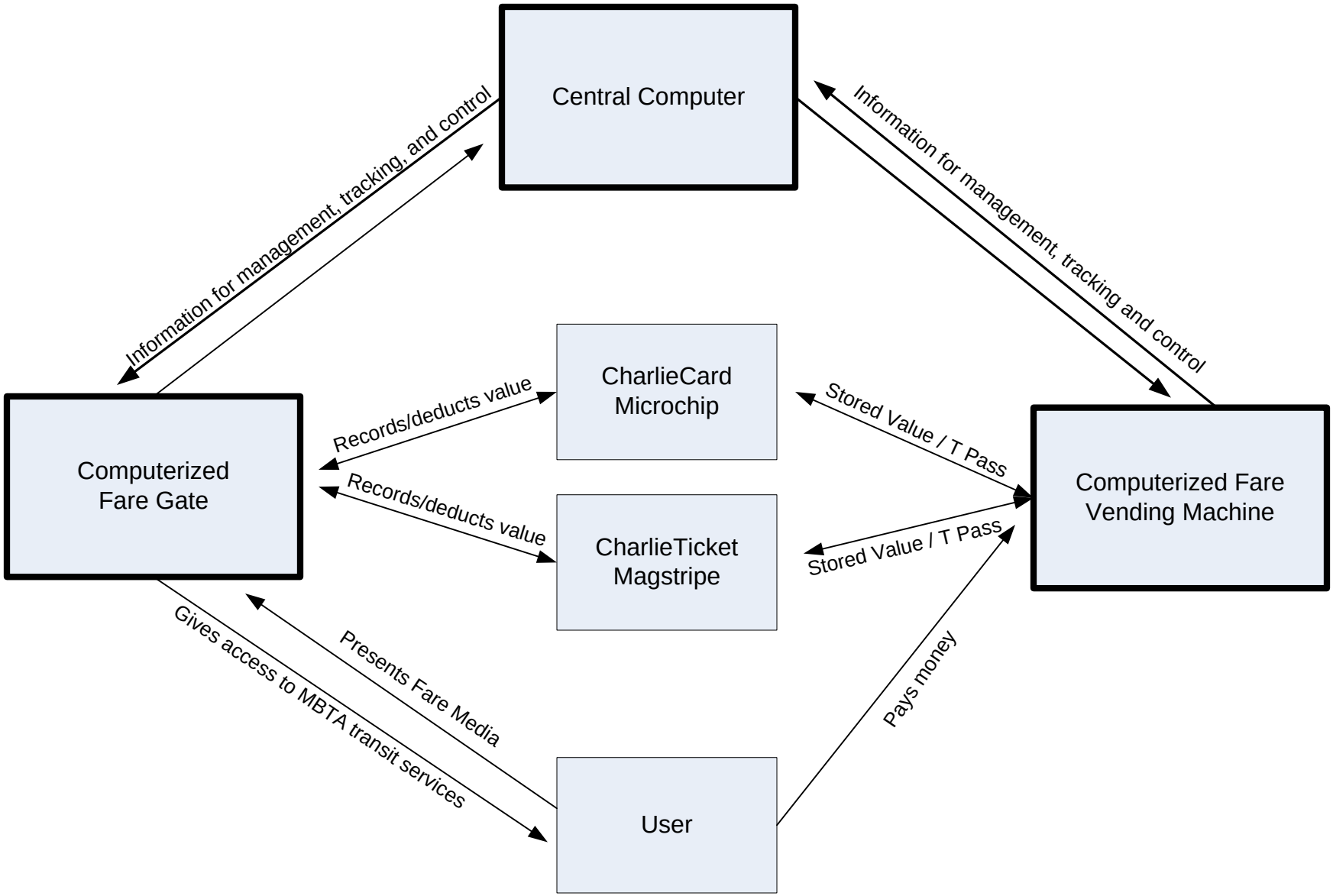


EXHIBIT 6

~~Original~~Current Version
The Anatomy of a Subway Hack:
Breaking Crypto RFID's and Magstripes of Ticketing Systems

Zack ~~AndersonStudent~~AndersonStudent, MIT
RJ ~~RyanStudent~~RyanStudent, MIT
Alessandro ~~ChiesaStudent~~ChiesaStudent, MIT

~~Want free subway rides for life?~~ In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We ~~go over social engineering attacks we executed on employees~~survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote ~~to perform~~in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Zack Anderson is studying electrical engineering and computer science at MIT. He is an avid hardware and software hacker, and has built several systems such as an autonomous vehicle for the DARPA Grand Challenge. Zack is especially interested in the security of embedded systems and wireless communications. He has experience building and breaking CDMA cellular systems and RFID. Zack has worked for a security/intelligence firm, and has multiple patents pending. He enjoys building systems as much as he enjoys breaking them.

RJ Ryan is researcher at MIT. His longtime passion for security has resulted in a number of hacks and projects, including a steganographic cryptography protocol. RJ works on a number of technical projects ranging from computer security to operating systems, distributed computation, compilers, and computer graphics. He enjoys learning how things work, and how to make things work for him.

Alessandro Chiesa is a Junior at MIT double majoring in Theoretical Mathematics and in Electrical Engineering and Computer Science. Born and raised in Varese,Italy, he came to MIT with interests in computational algebraic geometry, machine learning, cryptography, and systems security. He has authored papers such as "Generalizing Regev's Cryptosystem", which proposes a new cryptosystem based on shortest vector problems in cyclotomic fields. He is currently working with Oracle's Database Security group.

~~# 5526763_v1~~# 5526763_v2

Document comparison done by Workshare DeltaView on Thursday, August 07, 2008 5:11:58 AM

Input:	
Document 1	interwovenSite://BOSDMS/Active/5526763/1
Document 2	interwovenSite://BOSDMS/Active/5526763/2
Rendering set	standard

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Style change	
Format change	
~~Moved deletion~~	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	7
Deletions	11
Moved from	0
Moved to	0
Style change	0
Format changed	0
Total changes	18

EXHIBIT 7

July 14, 2008 9:12 AM PDT

Column: The man who changed Internet security

Posted by Robert Vamosi 14 comments

Programming note: *As of Friday, July 11, 2008, Defense in Depth will now only carry my weekly column plus additional commentary on the state of computer security. My security news blogs will instead appear under the CNET News Security banner going forward. And my CNET News Security Bites podcasts can be found at here. All of these can be subscribed to via RSS.*

While security researcher Dan Kaminsky still won't comment on the specific nature of a flaw within the Domain Name System--for fear that criminal hackers might exploit it before the worldwide network of name servers worldwide and client systems that contact them can be updated--he nonetheless went public on July 8 with some details, backed by simultaneous patch releases from Microsoft, Cisco, and others.

There have been other multiparty patch releases, but never has there been one on such a massive scale. It took someone with the gravitas and reputation of Kaminsky to pull together the affected parties.

What he and others he took into his confidence did over the last
few months was not only responsible but extraordinary. The flaw that Kaminsky discovered could allow criminal hackers to guess the transaction ID of any request to a DNS server for a particular domain, such as one used for a bank or an e-commerce site, and then redirect that request to another site, a phishing site. It would do so silently, evading most anti-phishing technology because

Ad Feedback



About Defense in Depth

Covering computer viruses and computer crime, Robert Vamosi goes beyond the hype to provide you with expert interviews of the top security researchers, as well as offeri the hands-on, nontechnical advice you'll need to stay safe online.

Subscribe via RSS
Click this link to view as XML.

the change would be made not at the desktop level but at the DNS server itself. Certainly this is big, and certainly one would want to get the news out as soon as possible--but Kaminsky took the time to inform the proper vendors and authorities and, only after they were ready with patches, did he disclose some of what he'd discovered.



Dan Kaminsky at DefCon in 2006.

(Credit: Declan McCullagh/CNET News)

That isn't to say what Kaminsky did was perfect; he himself admits there are lessons to be learned and improved upon the next time this happens. Whether you agree with the severity of the flaw Kaminsky disclosed last Tuesday, I do think all future vulnerability disclosures could benefit from his example.

Kaminsky, director of penetration testing at IOActive, is no stranger to vulnerabilities. Over the years he's found a fair share and says that in the case of the DNS flaw he wasn't looking for it. In this week's Security Bites podcast, Kaminsky told me that after three days of testing he knew he had something important. At that point, early in 2008, he had a few options.

One was to tell the vendor (or, in this case, vendors) directly. Ari Takanen of Codenomicon told me he prefers that security researchers keep vulnerabilities between them and the vendor. Vendors, Takanen said, have their own development cycles, and for a researcher to burst into a room or go public and demand that everyone work on his or her vulnerability is unrealistic. While Kaminsky was willing to work with the vendors, he wasn't willing to give them forever.

Another option was to sell the vulnerability to a third party like TippingPoint's Zero Day Initiative. ZDI acts as the middleman, talking with the vendor and communicating with the researcher. The advantage here is that a researcher with no connections to the affected vendor can communicate the problem clearly.

Add this feed to your online news reader

Defense in Depth topics

Antivirus
Audio and video
Bots and botnets
Browsers and extensions
Chat and e-mail
Criminal Hackers
Mobile
Networking
Phishing
Rootkits
Security
Spyware
Storage
Uncategorized

Most popular stories

Kaminsky provides the why of attacking DNS
IKEA to sell solar panels?
Photos: Muse spins from the Oshkosh air show
Images: Scientists develop eye camera
Black Hat a sure bet to be big, bold in Vegas

Latest tech news headlines

ZDI has been credited with several vulnerabilities, such as those announced by Apple and Microsoft. Kaminsky has no qualms with those who opt for this method, although he said he didn't understand why a company would pay for this information. (I know the answer: TippingPoint uses the vulnerability data it purchases to protect its customers first, thereby giving it a competitive advantage in the vulnerability assessment space).

Another option for Kaminsky was to go public, to announce the vulnerability and publish details, including an exploit, on, say, Bugtraq. A few researchers have gone this route, but often as a last resort after getting a cold shoulder from the vendor. A few researchers have published flaw details first without contacting anyone, taking both the public and the vendor by surprise. But such moves are unwise since they give the bad guys all the information they need while everyone is vulnerable.

Finally, as Kaminsky reminded me, there's the option of selling your vulnerability to the criminal underside of the Internet.

With the DNS flaw, Kaminsky was in a very weird position. What he found wrong with DNS, the servers that translate a Web site's common name to its IP address, wasn't just within one vendor's product, it cut across various products, from various vendors. He said he consulted with DNS expert Paul Vixie, and together they decided they had to convene a meeting, and do so within a few weeks of the discovery.



Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure.

That meeting occurred at Microsoft's Redmond, Wash., headquarters on March 31, 2008. There, representatives from 16 vendors sat down and listened to Kaminsky's pitch. After deciding this was a real and exploitable problem, the vendors decided they would have little choice but to agree to release simultaneously their respective patches.

At some point, July 8, 2008, was agreed upon as the date,

EA, Paramount announce 'Godfather II' video ga
Posted in Geek Gestalt by Daniel Terdiman

perhaps because it coincided with Microsoft's monthly Patch Tuesday. The date was significant in other ways: for example, it fell roughly 30 days before Kaminsky was scheduled to speak at Black Hat in Las Vegas.

Between March and July, there was considerable back and forth among Kaminsky and the vendors, and then, as the date neared, he decided to share the details with a few others.

In retrospect, Kaminsky confessed that he really should have told more people. He had gone through great pains to inform the DNS community, the specific vendors, and few researchers. He did so to keep word from getting out.

But within hours of making his announcement, Kaminsky faced a chorus of public ridicule by other security researchers, most hearing about the flaw for the very first time. The complaints, at times, trivialized the announcement, with fellow researchers citing that similar claims had been made against DNS 3 to 10 years before or even longer. Some suggested Kaminsky was simply trying to advertise his talk at Black Hat next month.

Most vocal was Matasano Security researcher Thomas Ptacek, who blogged his doubts. But Kaminsky called Ptacek and he retracted his comments. He now says, "Dan has the goods. Patch now, ask questions later."

Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure. He could have, as Ptacek notes, made thousands of dollars off this DNS thing. Instead, Kaminsky has set a high mark for future disclosures. He has changed Internet security, and done so for the better of us all.

TOPICS: **Security**
TAGS: **security**, **column**, **Security Watch**, **Dan Kaminsky**, **DNS patch**
BOOKMARK: Digg Del.icio.us Reddit Yahoo! Buzz

August 8, 2008 5:35 AM PDT



Between a rock and YouTube, video execs see promise
Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT



Targeted for hacking by reporters at my table
Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT

All News.com headlines »

Featured blogs

Beyond Binary by Ina Fried
Coop's Corner by Charles Cooper
Defense in Depth by Robert Vamosi
Geek Gestalt by Daniel Terdiman
Green Tech
One More Thing by Tom Krazit
Outside the Lines by Dan Farber
The Iconoclast by Declan McCullagh
The Social by Caroline McCarthy
Underexposed by Stephen Shankland

Recent posts from Defense in Depth

Black Hat 2008: Notes from the field

Column: Finally, ID fraud protection that works

Column: Will you be ditching your antivirus app anytime soon?

A real simple answer to password protection

Despite patch, today's systems still vulnerable to 2002 flaw

ADD A COMMENT **(Log in or register)**

14 comments (Page 1 of 2)

by inachu July 14, 2008 7:55 AM PDT

I miss the days where most govt agencies had their own BBS.
Using telnet and going into various areas just exploring.
I went from my local library to MIT then onto NIST then onto some tokyo university BBS retracing mysteps it went all the way around the world through nasa then loggen back into my library.
Sad to see we can't do that anymore. No more wild jungle.

Reply to this comment

by tekwiz4u July 14, 2008 11:17 AM PDT

It's commendable what he did. He wasn't in it for bragging rights, like most of the hackers out

Resource center from News.com sponsors

Same great protection. Reengineered for speed.

Norton Internet Security™2008



Norton still delivers award-winning protection and now uses 83% less memory and scans 48% faster than the competitor average.
Get a FREE trial today!

Norton from symantec

Norton Beats the Competition
See how Norton Internet Security™2008 uses less memory, while scanning and booting faster than the competitor average.

Norton Protection Blog
Read the latest from our security experts as they help protect people from evolving online threats.

Protect Your Bluetooth Connection
Don't let fraudsters sink their teeth into your Bluetooth connection.

Vishing - What you

there. The exploit would have been bad for all of us. But he took it upon himself to be responsible to benefit the greater whole. Good job.

Reply to this comment

by n3td3v July 14, 2008 11:28 AM PDT

Media hype and clever marketing for Blackhat security conference.

Let's find out who is making the money, this vulnerability is over hyped.

Reply to this comment

by The_Decider July 14, 2008 12:10 PM PDT

Responsible? Only because the parties involved took it seriously.

If they had not and Kaminsky hadn't disclosed it would have been irresponsible. The black hats would have found it eventually leaving everyone at the mercy of them.

Full disclosure is always better than those idiots who think there is any merit to security through obscurity.

Reply to this comment

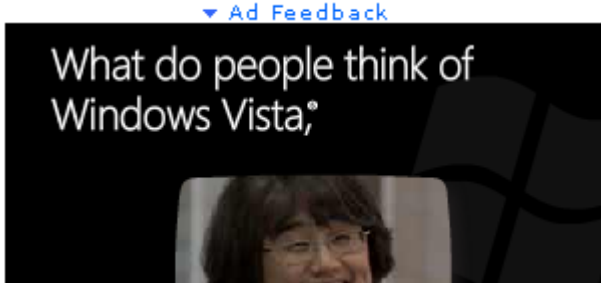
by RobertinOhio July 14, 2008 12:44 PM PDT

As a security professional whom is certified I still do not see the value of this "admiral approach" to

need to know
Meet the latest ID theft scam: Voice Phishing.

Take Norton for a Test Drive Today!
Act now to get your FREE trial of Norton Internet Security 2008.

Ad Feedback





releasing of security incidents and vulnerabilities. Yeah Dan Kaminsky has made a name for himself in the security community. If he was just some other schmo...then he would have never seen the inside of any vendor's office. My name does not mean jack so I know I am not going to pick up the phone and get a meeting at Cisco or Microsoft in a couple of days to discuss the issue with them. I am going to put my discovery on Bugtraq and if the internet gets shut down in North America as a result...oh well.

BUT...if I do sit on it and a hacker finds the exploit and then I come out afterward, I get nailed for not sharing it. D-amned if I do and d-amned if I don't. The good guys always loose.

Another thing I have learned is usually the hacker will almost always win. All you can do is contain, eradicate, and learn from attacks and exploits to make it harder for them to break in. Not sharing your discoveries from the general public and only with vendors is most certainly NOT the way to resolve these issues however. I do not commend Dan Kaminsky for his actions, he is setting a BAD precedent. One that unfortunately Infragard, another organization with a history of one way traffic with information, follows.

Reply to this comment

by DanKaminsky July 14, 2008 2:13 PM PDT

Robert--

The vendors have become pretty good at responding to stuff -- and, of course, if you do find something of technical value, please feel free to contact me and I will be happy to help. I'm trying to find a balancing point between not releasing (which leads to no patches, and/or no deployment of patches) and releasing in a problematic manner (i.e. even those places that are responsible, and do maintain their security, are still hit). Maybe this isn't perfect, but please give me the benefit of the doubt until you know just what I've found.

Reply to this comment | View all 2 replies

by DanKaminsky July 14, 2008 2:17 PM PDT

Decider--

I agree. It's only because the vendors were so amazingly responsive that this path could be taken at all. If they'd been lame, we'd be screaming at them for being so. So, they weren't lame, in all fairness they deserve some appreciation for that.

Reply to this comment

by n3td3v July 14, 2008 3:47 PM PDT

Dan Kaminsky is making money out of this there is no doubt.

If he hadn't circled his disclosure around a profiteering security conference I wouldn't bash this **** so much.

Because he has circled his disclosure around a big security conference, I know his motivation is money.

I don't know who he has been shaking hands with and what money has been exchanged, but this is something for the government to wire tap on.

Reply to this comment

by mehap July 14, 2008 11:12 PM PDT

So what if he is making/indulging in making money?

Your whole system is geared on making money.

How do you survive mate?

Reply to this comment

by DanKaminsky July 15, 2008 3:45 PM PDT

n3td3v--

Dude, did you miss the fact that Defcon is like three days later? Black Hat is just practice for Defcon  Seriously, the last big talk was Seattle Toorcon. Rickrolling the Internet isn't exactly profit source number one.

Reply to this comment

1 | 2 | Next 10 Comments >>

Register to submit a comment

Already have an account? Log in now

Join the CNET community To continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's Terms of Use

CONTINUE

Need help? »

Powered by Jive Software

On TechRepublic: 19 words you don't want in your resume

Log in | Sign up W

c|net NEWS.com

Search: News Go Advan search

Today on CNET Reviews **News** Downloads Tips & Tricks CNET TV Compare Prices Blogs

ad Click to Save up to $300/yr

Business Tech Cutting Edge Green Tech Wireless Security Media Markets Personal Tech Video My News

Sponsored Links

Lock Down Windows XP
Secure your confidential data. Free security guide download.
www.newboundary.com

Norton Internet Security
Newest 2008 version available now! Includes AntiVirus™ and Firewall.
www.norton.com

SAP Security & Controls
Affordable, remote security admin for SAP by The Security Experts
www.sym-corp.com

Site map Help center Corrections Newsletters Send tips News.com mobile Content licensing RSS feeds

Search: News

Popular topics: CES Drivers Games IE7 iPhone iPod iPod Nano iPod Touch iTunes Leopard Macworld Nintendo Wii PS3 Spyware TVs Vista Xbox 360

About CNET Today on CNET Reviews News Compare prices Tips & Tricks Downloads CNET TV

Popular on CBS sites: Fantasy Football Miley Cyrus MLB Wii GPS Recipes Mock Draft

About CNET Networks Jobs Advertise

Visit other CBS Interactive sites Select Site

Copyright ©2008 CNET Networks, Inc., a CBS Company. All rights reserved. Privacy policy Terms of use

August 7, 2008 9:07 AM PDT

Kaminsky provides the why of attacking DNS

Posted by Robert Vamosi 6 comments

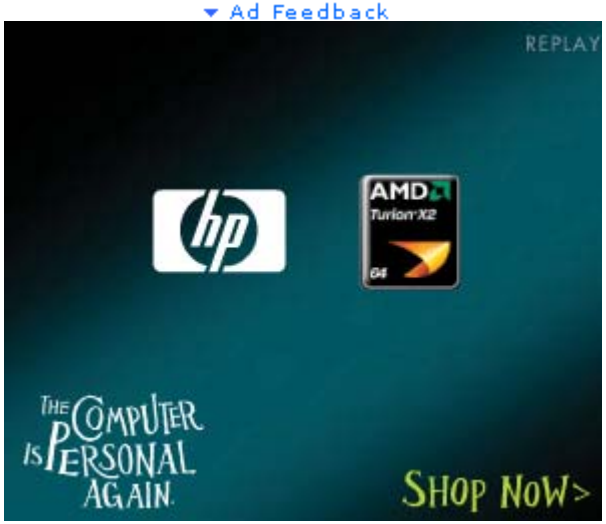
LAS VEGAS--Speaking before a packed audience, researcher Dan Kaminsky explained the urgency in having everyone patch their systems: virtually everything we do on the Internet involves a Domain Name System request and therefore is vulnerable.

Expectations were running high before Wednesday morning as Kaminsky, director of penetration testing for IOActive, had revealed little about his DNS vulnerability up till then. That didn't stop others from trying to figure it out. But that actually helped Kaminsky in the end; it meant during his speech, he was able to skip the what and go directly to the why.

Security researchers always thought it was hard to poison DNS records, but Kaminsky said to think of the process as a race, with a good guy and bad guy each trying to get a secret number transaction ID. "You can get there first," he said, "but you can't cross finish line unless you have the secret number."

The question is why would someone bother? Well, Kaminsky talked about how deeply embedded DNS is in our lives. Kaminsky said there are three ages in computer hacking. The first was attacking servers (for example FTP and Telnet). The second was attacking the browsers (for example Javascript and ActiveX). We're now about to enter the third age, where attacking Everything Else is possible.

Ad Feedback



About News - Security

Online security is threatened by more than hacking and phishing attempts. Check here for the latest updates on software vulnerabilities, data leaks, and rapidly spreading viruses--and learn how to protect your systems.

Subscribe via RSS
Click this link to view as XML.

Add this feed to your online news reader

We know that if we type a name.com into a browser, the DNS resolves it to its numerical address. But what we don't realize is that same process occurs when we send e-mail or when we log onto a Web site. These also require DNS lookup.

Kaminsky then detailed how various security methods on the Web can be defeated if one owns the DNS. For example, if a site wants to establish a Trust Authority Certificate with the Certificate Authorities, they use e-mail to confirm the identity of the requester. He also said that it's possible to poison Google Analytics and even Google AdSense, which also rely on DNS lookup.

Prior to the patch, the bad guy had a 1 in 65,000 chance of getting it because the transaction ID is based, in part, on the port number used. With the patch, the chances decrease to 1 in 2,147,483,648. Kaminsky said it's not perfect, but it's a good enough start.

Click here for full coverage of Black Hat 2008.

TOPICS: **Vulnerabilities & attacks**, **News**
TAGS: **Security**, **Black Hat 2008**, **Dan Kaminsky**, **DNS**
BOOKMARK: Digg Del.icio.us Reddit Yahoo! Buzz

Recent posts from News - Security

Targeted for hacking by reporters at my table

Black Hat expels reporters in network snooping

Microsoft to seek credit for finding vulnerabilities

Wall of Sheep comes to Black Hat

Is Check Point's security profile the broadest?

News - Security topics

Corporate & legal
Privacy & data protection
News
Vulnerabilities & attacks

Most popular stories

Kaminsky provides the why of attacking DNS

IKEA to sell solar panels?

Photos: More spins from the Oshkosh air show

Images: Scientists develop eye camera

Black Hat a sure bet to be big, bold in Vegas

Latest tech news headlines



Between a rock and YouTube, video execs see promise
Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT



Targeted for hacking by reporters at my table
Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT



Google sours on $1 billion AOL investment
Posted in News - Digital Media by Steven Musil
August 7, 2008 9:20 PM PDT

ADD A COMMENT (**Log in or register**)

6 comments (Page 1 of 1)

by One Mark Bliss August 7, 2008 10:04 AM PDT

Actually, the chances decrease, since the one is divided by the increased number. Consider that the concept of chance being used in the article represents the random likelihood that someone will guess the secret code in one attempt.
It seems that a similar confusion exists in another concept nothing to do with chance, namely turning the air conditioning up, or down. Which makes the room colder? In that case it depends on whether the concept being referred to is the amount of the flow of cold air, in which case it would be up, or the numerical representation of temperature, in which case it would be down.
The only way a similar confusion can arise with chance is whether it is couched as the chance of guessing something randomly, or the chance of not guessing it. So, in the article, the chance would only increase if it were the chance of a hacker randomly NOT getting the secret code.

Reply to this comment | View reply

by conobs August 7, 2008 11:20 AM PDT

instead of giging them on symantecs
WHERE IS THE MEAT?
how dos it work?

this would qualify more as a story about a story, not an actual news story
take it up a notch
thx
bob

All News.com headlines »

Featured blogs

Beyond Binary by Ina Fried
Coop's Corner by Charles Cooper
Defense in Depth by Robert Vamosi
Geek Gestalt by Daniel Terdiman
Green Tech
One More Thing by Tom Krazit
Outside the Lines by Dan Farber
The Iconoclast by Declan McCullagh
The Social by Caroline McCarthy
Underexposed by Stephen Shankland

Resource center from News.com sponsors

Same great protection.

Reply to this comment

by conobs August 7, 2008 11:25 AM PDT

i dont know maybe i am wrong and overly harsh

Reply to this comment

by frazmann August 7, 2008 12:55 PM PDT

@conobs - the crux of the hack are that you send a DNS request to a server, knowing that the server will send a request to it's DNS master server to obtain the translation, and then bombard the server with fake responses, hoping to guess the transaction id that it used when making the request. If you get it right before the master server's response arrives then you have planted a fake DNS entry in your server, and the real response is thrown away. If you do this from your comcast account then you can re-direct all your neighbors to a fake google.com that sits on your PC. Seems so simple I'm surprised no-one tried it before....

Reply to this comment

by benjaminstraight August 8, 2008 3:14 AM PDT

Good article.

Reply to this comment

Reengineered for speed.

Norton Internet Security™2008



Norton still delivers award-winning protection and now uses 83% less memory and scans 48% faster than the competitor average.
Get a FREE trial today!

Norton from symantec

Norton Beats the Competition
See how Norton Internet Security™2008 uses less memory, while scanning and booting faster than the competitor average.

Norton Protection Blog
Read the latest from our security experts as they help protect people from evolving online threats.

Protect Your Bluetooth Connection
Don't let fraudsters sink their teeth into your Bluetooth connection.

Vishing - What you need to know
Meet the latest ID theft scam: Voice Phishing.

Take Norton for a Test Drive Today!
Act now to get your FREE trial of Norton Internet Security 2008.

On The Insider: Paris Says the Video Speaks for Itself Log in | Sign up W

c|net NEWS.com

Search: News Go Advan search

Today on CNET Reviews News Downloads Tips & Tricks CNET TV Compare Prices Blogs ad Click to Save up to $300/yr

Business Tech Cutting Edge Green Tech Wireless Security Media Markets Personal Tech Video My News

Register to submit a comment

Already have an account? Log in now

Join the CNET community To continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's Terms of Use

CONTINUE

Need help? »

Ad Feedback



Powered by Jive Software

Site map Help center Corrections Newsletters Send tips News.com mobile Content licensing RSS feeds

Search: News

Popular topics: CES Drivers Games IE7 iPhone iPod iPod Nano iPod Touch iTunes Leopard Macworld Nintendo Wii PS3 Spyware TVs Vista Xbox 360

On The Insider: Paris Says the Video Speaks for Itself Log in | Sign up W

c|net NEWS.com

Search: News Go Advan search

Today on CNET Reviews **News** Downloads Tips & Tricks CNET TV Compare Prices Blogs ad Click to Save up to $300/yr

Business Tech Cutting Edge Green Tech Wireless Security Media Markets Personal Tech Video My News

About CNET Today on CNET Reviews News Compare prices Tips & Tricks Downloads CNET TV

Popular on CBS sites: Fantasy Football Miley Cyrus MLB Wii GPS Recipes Mock Draft

About CNET Networks Jobs Advertise

Visit other CBS Interactive sites Select Site

Copyright ©2008 CNET Networks, Inc., a CBS Company. All rights reserved. Privacy policy Terms of use

EXHIBIT 8

Athena Rules of Use (including MITnet)

MITnet, MIT's campus-wide computer network, connects thousands of computers on and off campus, including the Athena workstations, printers, and servers, many student machines in the dorms, and the campus dialup servers. Network connectivity has many advantages which you will discover as you explore Athena, MITnet, and the Internet beyond. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

Similarly, the **Athena-specific end-user facilities** (clusters, workstations, printers, etc.) are provided as an Institute resource, and certain guidelines are necessary to help maintain this resource.

This section summarizes:

- the rules that apply to all users of MITnet (this includes all Athena users)
- the rules regarding the appropriate use of Athena-specific facilities

We expect you to follow these rules, and we hope you will help others follow them as well. If you need assistance in dealing with someone willfully violating the rules, send email to stopit@mit.edu.

We appreciate your cooperation.

Summary

The listing below provides only summaries of the rules. For the full text of each rule, please see the following pages.

MITnet Rules of Use

Comply with Intended Use of the System

1. Don't violate the intended use of MITnet.

Assure Ethical Use of the System

2. Don't let anyone know your password(s).

3. Don't violate the privacy of other users.

4. Don't copy or misuse copyrighted material (including software).

5. Don't use MITnet to harass anyone in any way.

Assure Proper Use of System Resources

6. Don't overload the communication servers; in particular, don't abuse your electronic mail (email) or Zephyr privileges.

Additional Rules for Athena Facilities

Comply with Intended Use of the System

A1. Don't violate the intended use of the Athena system.

Protect Athena Equipment

A2. Don't eat, drink, or bring food or liquids into the Athena clusters.

A3. Don't turn the power off on Athena equipment.

A4. Don't reconfigure the cluster, either hardware or software.

Assure Fair Access to Workstations in Athena Clusters

A5. Don't violate the official priorities for the use of workstations; in particular, don't play games or engage in other non-academic activity if the cluster is busy, and don't log on to more than one workstation at a time.

A6. Don't leave your workstation unattended for more than 20 minutes.

A7. Don't make a lot of noise in the Athena clusters.

Assure Fair Access to Athena Printers

A8. Don't violate the official priorities for the use of printers; in particular, don't be a printer hog or use the Athena printers as copy machines.

MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsibile, legal, and respectful of privacy. If you have questions or wish further information about any of the MITnet policies outlined below, send e-mail to itpolicy AT mit.edu.

All network users are expected to follow these rules. ***Violations of the rules can subject the offender to Institute disciplinary proceedings and, in some cases, to state or federal prosecution.***

PLEASE NOTE: Laws that apply in "the real world" also apply in the "virtual" networked computer world (including MITnet). Laws about libel, harassment, privacy, copyright, stealing, threats, etc. are *not* suspended for computer users, but apply to all members of society whatever medium they happen to be using: face-to-face, phone, *or* computer. Furthermore, law-enforcement officials are more computer-savvy than ever, and violations of the law in "Cyberspace" are vigorously prosecuted.

Similarly, Institute policies (as described in MIT's *Policies and Procedures*, for example) also apply to MITnet users. Other rules may also apply to users of particular facilities connected to MITnet: users of MIT's

academic computing resources are subject to the **Additional Rules for Athena Facilities**; providers of information to MIT's Campus-Wide Information System (via TechInfo, the World Wide Web, etc.) have specific guidelines (see http://web.mit.edu/cwis/www/faq/guidelines.html); other facilities may have their own constraints (check with your local system manager); and external networks to which MITnet provides access may have their own rules to which MITnet users may be subject.

Complying with the Intended Use of the System

It is important that you understand the purpose of MITnet so that your use of the system is in compliance with that purpose.

1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:

- *Don't try to interfere with or alter the integrity of the system at large*, by doing any of the following:
  - permitting another individual to use your account
  - impersonating other individuals in communication (particularly via forged email or Zephyrgrams)
  - attempting to capture or crack passwords or encryption
  - destroying or altering data or programs belonging to other users
- *Don't try to restrict or deny access to the system by legitimate users.*
- *Don't use MITnet for private financial gain.* For example, users are *not* permitted to run a private business on MITnet. (Commercial activity *is* permitted, but *only* for business done on behalf of MIT or its organizations. Cf. Section 13.2.3 of MIT's *Policies and Procedures*: "MIT's computing and telecommunications facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization.")
- *Don't transmit threatening or harassing materials.* (Cf. Rule 5.)

Assuring Ethical Use of the System

Along with the many opportunities that Athena provides for members of the MIT community to share information comes the responsibility to use the system in accordance with MIT standards of honesty and personal conduct. Those standards, outlined in Section 13.2 of MIT's *Policies and Procedures*, call for all members of the community to act in a responsible, professional way.

Appropriate use of MITnet resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

2. Don't let anyone know your password(s).

While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should *never* let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., IS&T staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one. And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, how to change passwords, and how to share information on Athena without giving away your password, see the document *Managing Your Athena Account*.

3. Don't violate the privacy of other users.

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet, and the operating systems used by Athena and other MITnet systems, encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections 11.2, 11.3, and 13.2 of MIT's *Policies and Procedures*). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section 11.1 of MIT's *Policies and Procedures* notes, "Invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- *Don't try to access the files or directories of another user without clear authorization from that user.* Typically, this authorization is signaled by the other user's setting file-access permissions to allow public or group reading of the files. If you are in doubt, ask the user.
- *Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.* These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.
- Unless you understand how to protect private information on a computer system, *don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves* (e.g., grades, address information, etc.)
- *Don't make any personal information about individuals publicly available without their permission.* This includes both text and number data about the person (biographical information, phone numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.) For instance, it is *not* appropriate to include a picture of someone on a World Wide Web page without that person's permission. (Depending on the source of the information or image, there may also be copyright issues involved; cf. Rule 4).
- *Don't create any shared programs that secretly collect information about their users.* Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)
- *Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.*

4. Don't copy or misuse copyrighted material (including software).

Many computer programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. You must abide by these legal and contractual restrictions, because to do otherwise may subject you to civil or criminal prosecution.

Copyright-related restrictions may include (but are not necessarily limited to) prohibitions against:

- copying programs or data
- reselling programs or data
- redistributing or providing facilities for redistributing programs or data
- using programs or data for non-educational purposes
- using programs or data for financial gain
- using programs or data without being among the individuals or groups licensed to do so
- publicly disclosing information about programs (e.g., source code) without the owner's authorization

For more information about the legal issues surrounding duplication of software, see the pamphlet "Is it okay to copy my colleague's software?" (To request a copy, send e-mail to sendpubs@mit.edu or call x3-5150.) Some software on Athena is subject to special licensing restrictions; see the document *Summary of Available Athena Software*. For all other software licensing questions, send email to contracts@mit.edu.

The above prohibitions focus on computer software, but copyright laws apply to *all* material on MITnet. For example, it is inappropriate to copy *any* material owned by others from *any* source (e.g., cartoons, photographs, articles, poems, graphics scanned from a magazine, etc.) without permission of the owner. You should assume that all materials are copyrighted unless a disclaimer or waiver is explicitly provided. (This is particularly true on the World Wide Web; to include information from some other source on a Web page, *link* to it, *don't* copy it. In some cases, even this action may violate copyright or licensing agreements by enabling illegal redistribution of programs or data. If you're unsure, ask the owner.)

5. Don't use MITnet to harass anyone in any way.

"Harassment," according to MIT's *Policies and Procedures* (Section 9.5), is defined as:

> any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual or group's educational or work performance at MIT or that creates an intimidating, hostile or offensive educational, work or living environment.... Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group.

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to stopit@mit.edu. (If you believe you are in danger, call the Campus Police *immediately* at x3-1212.)

Assuring Proper Use of the System

MITnet's resources, as well as the resources MITnet gives you access to (e.g., Athena, postal servers, bulletin boards, etc.), are powerful tools that can be easily misused. Your use of the system should be consistent with the intended uses of these resources. In particular, you should not overload the system or otherwise abuse the

network.

6. Don't overload the communication servers; in particular, don't abuse your electronic mail (email) or Zephyr privileges.

Electronic mail is a fast, convenient form of communication. It is easy to send electronic mail to multiple recipients, and you can even send a message to many recipients simply by specifying a single list name (i.e., by using a mailing list). But this ability to send messages to many people also makes it easy to misuse the system. The general rule is: *use email to communicate with other specific users, not to broadcast announcements to the user community at large.*

For example, while it is appropriate to use email to have an interactive discussion with a set of people (even 20 or more users) or to use email to send a single copy of an announcement to some "bulletin board" facility with a wide readership (e.g., Network News, or a Discuss meeting), it is not appropriate to use email as a way to broadcast information directly to a very large number of people (e.g., an entire MIT class). This is true whether you include the recipient usernames individually or by using a mailing list: under no circumstance should you use the email system to get a general announcement out to some large subset of the MIT community.

These guidelines are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of email messages at once. When a user sends out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a degradation of service for all users.

These considerations apply to the Zephyr service as well. Zephyr is a central service involving thousands of transactions daily. Using Zephyr to transmit messages to a very large group of people degrades the system performance and is inappropriate.

Finally, the proliferation of electronic chain letters is especially abusive of the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing. Creating or forwarding chain letters may subject you to Institute disciplinary proceedings.

Additional Rules for Athena Facilities

These Rules of Use for Athena Facilities are intended to help members of the MIT community protect the Athena equipment to assure all authorized users effective access to it. These rules supplement the **MITnet Rules of Use**, which all Athena users are also expected to follow.

These rules apply to all users of Athena facilities, including students, faculty, authorized guests, and even IS&T/Athena staff. (In certain private Athena clusters, some of these rules may be relaxed, or additional rules may be in effect; check with your cluster's system manager).

If you need assistance in dealing with someone willfully violating the Athena rules, feel free to contact the Athena Hardware Hotline (phone: x3-1410, email: hotline@mit.edu), or send email to stopit@mit.edu. (If you believe you are in danger, call the Campus Police *immediately* at x3-1212.)

Complying with the Intended Use of the System

While MITnet is a general-purpose Institute resource in support of all kinds of computing on campus, Athena is more specifically focused on academic computing -- the use of computers in fulfilling the Institute's

educational goals. This special focus is echoed in a more specific intended use of the system.

A1. Don't violate the intended use of the Athena system.

Athena is an Institute resource for authorized MIT community members to use to fulfill educational goals. You should not take any action that violates that purpose. In particular:

- *Don't use Athena resources for non-educational purposes in any way that interferes with their use for educational purposes.* This is especially true at peak times of the year, when demand for Athena workstations and services exceeds supply and *any* use of Athena for non-educational purposes can potentially take resources away from education-oriented users. (Cf. Rule A5.)
- *Don't use any software available on Athena for any non-educational purpose if the license for that software does not permit such use.* In many cases, software available on Athena is licensed for educational use only. Users who would like to make non-educational use of Athena software (e.g., members of sponsored research projects who might like to use Athena's third-party software) must first check the licensing terms for the specific software they are interested in using (these terms are usually included in the locker for the software). If non-educational use is prohibited by the software license, the users must make their own arrangements to obtain licenses for the software that are compatible with their requirements. (Cf. MITnet Rule 4.)
- *Don't use Athena for private financial gain*, as by sale of the use of Athena resources (especially to anyone outside MIT), or by use of the system in support of any profit-making scheme not explicitly intended to serve Institute purposes. (Cf. MITnet Rule 1.)
- *Access to Athena computing facilities is restricted to authorized members of the MIT community. Trespassing is prohibited and violators will be subject to removal and/or prosecution.* Authorized Athena users typically login to workstations using their Athena usernames. Individuals who login as "root" from the initial xlogin screen or otherwise use workstations without identifying themselves as authorized Athena users may be asked for proof of identification by Athena staff members responsible for the maintenance of Athena computing facilities.

Protecting Athena Equipment

Much of Athena's computer equipment is accessible to a large number of people and is consequently vulnerable to overuse and damage. The following guidelines are designed to help protect this equipment. In the event of any damage to the equipment, regardless of cause, please contact the Athena Hardware Hotline (at x3-1410) immediately.

A2. Don't eat, drink, or bring food or liquids into the Athena clusters.

Food crumbs and spilled drinks are the primary cause of equipment damage in the Athena clusters. This damage is produced not only in obvious ways (a spilled cup of coffee), but also in subtle ways (even the cumulative effect of sticky fingers or crumbs can ruin equipment -- keyboards have been damaged at the rate of one per day from food crumbs alone, and mice are equally vulnerable).

A3. Don't turn the power off on Athena equipment.

Turning the power off on Athena equipment (e.g., workstations, monitors, or printers) can permanently damage the hardware. However, if the equipment smells or looks like it is burning, do turn it off and contact the Athena Hardware Hotline.

A4. Don't reconfigure the cluster, either hardware or software.

Moving equipment will often cause damage, or may cause it to be reported as stolen. Permanent damage may

result from even unplugging a keyboard.

Similarly, altering a workstation's filesystem in any way may render the machine unusable, or threaten its usability in other ways. For example, you should not reconfigure any workstation in an Athena cluster to allow remote connections unless you are actually sitting at that workstation. Even an apparently "harmless" change such as this (i.e., changing the access configuration of a workstation) may create major system security problems, and may actually jeopardize MIT's ability to license software for users in the future.

Also, do not remove Athena equipment -- or furniture! -- from any Athena facility. Doing so constitutes theft and will be dealt with accordingly.

If you believe the configuration of a cluster needs to be changed, you can contact the Athena Hardware Hotline.

Assuring Fair Access to Workstations in Athena Clusters

Athena clusters are facilities provided for members of the MIT community to achieve their academic goals. As such, they are subject to principles of use that support those goals -- the chief considerations being fair access to the facilities for the widest possible set of users, and the maintenance of a comfortable working environment. The rules below reflect these considerations as they affect users of the Athena clusters.

These rules are easily summarized: *please show consideration to other users.*

A5. Don't violate the official priorities for the use of workstations; in particular, don't play games or engage in other non-academic activity if the cluster is busy, and don't log on to more than one workstation at a time.

In conformance with Athena's stated purpose, the priorities for use of the workstations in crowded Athena clusters are as follows (cf. Rule A1):

- **Highest Priority:** course-related work (including theses)
- **Middle Priority:** personal productivity work (including non-course-related text processing, sending mail, exploring the Athena system)
- **Lowest Priority:** recreational computing (including game-playing and general Web-surfing)

Note that games are the lowest priority software on the system -- you should not play games if there are only a few workstations free, or if people are waiting for workstations. If a user needs a workstation for higher priority work while you are playing games, that user can ask you to give up your workstation. (Low priority activities may actually be disallowed entirely during certain times of the year to assure that the use of the clusters is consistent with the academic purpose of Athena. At these times, you are expected to refrain completely from low-priority activities as defined above.)

Similarly, some clusters have workstations which are reserved for specific course use, or which have special features. If you are using such a workstation for other than its special purpose, and someone who needs its unique feature asks you to surrender it, please do so gracefully.

A6. Don't leave your workstation unattended for more than 20 minutes.

If you are using a workstation in one of the Athena clusters and intend to keep using it but must leave it briefly unattended, you *must* limit your absence to *20 minutes or less* and signal your situation to other users by taking one of the following actions:

- leave a note on the workstation indicating the time you left the machine and your intention to return, *or*
- run the screen saver from the **Panel**, *or*
- run another screensaver program which correctly displays the elapsed time.

(If you choose to use a screen-based timer, note that it is a violation of the rules to tamper with the system such that your display never shows that more than 20 minutes have elapsed.)

If you are gone longer than twenty minutes or leave a workstation without a note or a valid countdown screensaver running, another user who needs a workstation is entitled to log you out or reboot the machine to make that machine available.

At certain times of the year, this rule may be adjusted downwards (e.g., the allowable "time away" may be reduced, possibly to 0) to assure that the clusters are being used effectively and that users will not be without a workstation while machines sit idle.

A7. Don't make a lot of noise in the Athena clusters.

Athena clusters are similar to the MIT Libraries in that students who use these facilities have to be able to concentrate to do their work. Please don't play music, shout, or engage in loud conversation in the clusters.

Also, if you use a workstation that has sound capabilities, you are expected to use earphones rather than have the workstation audible to other users in the cluster.

Assuring Fair Access to Athena Printers

Printing is a shared resource; restraint must still be exercised when using Athena printers to ensure fair access for everyone to this important service. This holds especially true when the clusters are busy. Violation of these rules can result in loss of printing privileges.

A8. Don't violate the official priorities for the use of printers; in particular, don't be a printer hog or use the Athena printers as copy machines. The following rules apply to all Athena Cluster printers including those located in the Copytech Centers (Thesis and color printers).

- Don't use printers as copy machines. Print only **one** copy of a document. Use a copy machine to make multiple copies. The only exception is for printing one's completed thesis to the thesis printer. You are allowed to print two copies maximum of your thesis on archival paper. If additional copies are required, consult your departmental secretary.

- Do not overload the printer queue with multiple jobs that will take longer than 20 minutes total to print. Send the jobs in small groups over time and send them when the printer is not busy. Check the default printer queues by typing **lpq** at the `athena%` prompt. For jobs at printers other than the default, the printing commands (**lpr**, **lpq** and **lprm**) accept the **-P***printername* option.

- Break large or huge jobs that take longer than 10 minutes total to print into smaller sections and send them to the printer individually.

- You are responsible for retrieving any jobs you queue to print. If you no longer want a job or will be unable to retrieve it, please remove it from the queue. Type **lprm -** at the `athena%` prompt.

- Do not remove unused paper from the cluster printers. That paper is provided solely for the use of that particular printer. If a cluster runs out of paper, please notify hotline@mit.edu.

- Color printing is a limited resource; use it sparingly. Color copying services are available in the Copytech centers to make additional copies.

- Above all, be courteous in your use of the Athena printers. While these rules do not enumerate every possible violation of appropriate use of the printers, they do address the most common questions and concerns.

Comments and feedback to olh-suggest@mit.edu.
Last modified: 15 January 2004

UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, *v.* ZACK ANDERSON, *ET AL.*, Defendants.	CIVIL ACTION NO. 08-CV-11364-GAO

ASSENTED TO MOTION OF
DEFENDANT MASSACHUSETTS INSTITUTE OF TECHNOLOGY
TO CORRECT DOCKET ENTRY

The Massachusetts Institute of Technology moves to correct Docket Entry No. 14 as follows (deleting struck-through and inserting underlined language):

"DECLARATION OF ERIC JOHNSON re 2 MOTION for Temporary Restraining Order by Massachusetts Bay Transportation Authority filed by ~~Massachusetts Institute of Technology~~ defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa."

and submits as reasons therefor the following:

1. At the hearing on August 9, 2008, on the plaintiff's Motion for Temporary Restraining Order, the Court allowed Jennifer Granick to participate by telephone in argument on behalf of the individual defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa.

2. In the course of her argument, Ms. Granick referred to a Declaration of Eric Johanson that had been prepared to support the opposition of the individual defendants, and began reading from that Declaration.

3. A colleague of Ms. Granick's had emailed the Johanson Declaration to a lawyer in the Office of the General Counsel of MIT in the early morning of August 9, 2008, and asked that it be printed and brought to the Court due to the fact Ms. Granick would be seeking leave of the Court to participate by telephone.

4. With Ms. Granick's permission, MIT provided a copy of the Johanson Declaration to Ieuan Mahony, lead counsel for the plaintiff, when he arrived at the courthouse for the hearing on the plaintiff's motion on August 9, 2008.

5. When Ms. Granick began to read to the Court from the Johanson Declaration, undersigned counsel representing the defendant Massachusetts Institute of Technology (not the individual defendants) brought to the Court's attention that I had a hard copy of the Johanson Declaration and offered to provide it to the Court, but expressly noted that the Declaration had not been prepared for nor was it being offered by MIT.

6. The Court, to the best of my understanding, accepted the copy of the Johanson Declaration based upon my disclosure of its source and of the parties on whose behalf I offered to provide it to the Court.

By its attorneys,

s/ Jeffrey Swope

Jeffrey Swope (BBO #490760)
EDWARDS ANGELL PALMER & DODGE LLP
111 Huntington Avenue
Boston, Massachusetts 02199-7613
(617) 239-0100

Dated: August 12, 2008

Assented to:

s/ Ieuan G. Mahoney
Counsel for the plaintiff
Massachusetts Bay Transportation Authority

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) on August 12, 2008, and further certify that on that day I provided a copy of this document by email to Jennifer Granick at Jennifer@eff.org.

s/ Jeffrey Swope

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

NOTICE OF APPEARANCE

PLEASE TAKE NOTICE of the appearance of Emily Berger as co-counsel for the defendants Zack Ryan, RJ Ryan, and Alessandro Chiesa in the above-captioned action.

DEFENDANTS ANDERSON, RYAN AND CHIESA

By their attorneys,

Dated: August 12, 2008

/s/ Emily A. Berger

Emily A. Berger, BBO No. 650,841
emily@eff.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO Date: August 14, 2008 Time: 11AM

DEFENDANTS ANDERSON, RYAN AND CHIESA'S RESPONSE TO PLAINTIFF'S "MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER" AND CROSS MOTION FOR RECONSIDERATION

INTRODUCTION AND STATEMENT OF FACTS

This motion is about three MIT students' ability to publish academic research applying known theories about security weaknesses to transit fare payment systems used by the MBTA.

On Saturday August 9, 2008, District Judge Douglas P. Woodlock restrained Defendants Anderson, Ryan and Chiesa ("students") from "providing [any] program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of Plaintiff MBTA's fare CharlieTicket and CharlieCard fare collection system." Defendants seek reconsideration of that temporary restraining order on the grounds that (1) the order is an unconstitutional prior restraint on First Amendment protected speech about their academic research, (2) the Computer Fraud and Abuse Act does not prohibit communication of information about computers or computer security, and (3) the MBTA's publication of the defendants' research and presentation slides undermines its claim to injunctive

relief.

Anderson, Ryan and Chiesa study computer security with professor Ronald Rivest at the Massachusetts Institute of Technology. The students applied existing research on stored value cards commonly used for fare payment in transit systems, including the MBTA's CharlieCard and CharlieTicket. This experiment confirmed that an attacker could modify the CharlieCard and CharlieTicket as the existing research predicted, and showed that additional security measures employed by plaintiff Massachusetts Bay Transportation Authority ("MBTA") were inadequate to prevent these modifications. The students wrote a paper for Rivest on their findings and received an "A." They also were accepted to present their research at the DEFCON computer security conference on August 10, 2008 in Las Vegas, Nevada.

The students and the MBTA attempted to contact each other before the DEFCON presentation. The parties set a meeting on August 4, 2008. The MBTA sent Sergeant Detective Richard Sullivan of the MBTA Police, and he brought a special agent from the Federal Bureau of Investigation with him. The students discussed their research with Sullivan and the FBI agent. At the end of the meeting, the understanding was that the students would deliver a short confidential report to the MBTA summarizing their findings and recommendations. The students did in fact deliver that report as planned and believed in good faith that they had satisfied all of the MBTA's requests.

Detective Sullivan submitted a declaration in this case, but his declaration is oddly silent on what the students discussed at that meeting and what the parties' agreement was. Detective Sullivan's declaration does not acknowledge that, as a result of the August 4 meeting, the students were unaware that MBTA had further demands until the afternoon of Friday, August 8 when the MBTA filed this lawsuit.

On the afternoon the suit was filed, and after the students had left Massachusetts for Nevada, MBTA appeared *ex parte* before Judge Woodlock, who was the duty judge. Judge Woodlock then convened a special court session on Saturday morning to hear this matter. The hearing was audio recorded. Counsel for the students, who were not notified about the hearing until after close of business on Friday afternoon, appeared via telephone.

According to counsel's notes, the Court found that 18 U.S.C. § 1030(a)(5)(A) of the Computer Fraud and Abuse Act prohibits the transmission of information to conference attendees or other individuals or groups if that transmission potentially causes damage to a protected computer. The Court also rejected the students' assertion that any restraining order would be an unconstitutional prior restraint on First Amendment protected speech. The court then enjoined and restrained the students "from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System. [sic]" *Order* at p. 2. The temporary restraining order ("TRO") runs for ten days. Federal Rule Civil Procedure 65(b)(2). As a result of the temporary restraining order the students did not give their presentation at DEFCON and have refrained from commenting on the substance of their research. While the students are no longer able to present their talk at the security conference, and have no plans to present the DEFCON talk in other forums, they wish to publish detailed information concerning the security vulnerability uncovered by their research to an interested public.

On August 11, 2008, after the date for the presentation had passed and after defendants had informed them that they were planning to seek reconsideration of the restraining order, Plaintiff MBTA filed a "Motion to Modify Terms but not Duration of TRO". The requested modification attempts to narrow the current TRO by inserting the phrase "non-public" between

"providing" and "program …" so that it would enjoin defendants "from providing program, non-public information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System. [sic]"

STANDARD FOR GRANTING A MOTION FOR RECONSIDERATION

The TRO was granted pursuant to Fed. R. Civ. P. 65. As such, the MBTA was required the demonstrate (and the Court was required to find):

> (1) a substantial likelihood of success on the merits, (2) a significant risk of irreparable harm if the injunction is withheld, (3) a favorable balance of hardships, and (4) a fit (or lack of friction) between the injunction and the public interest.

Nieves-Márquez v. Puerto Rico, 353 F.3d 108, 120 (1st Cir. 2003) (citation omitted). An "[i]njunction is an equitable remedy which should not be lightly indulged in, but used sparingly and only in a clear and plain case." *Plain Dealer Publishing Co. v. Cleveland Type. Union # 53*, 520 F.2d 1220, 1230 (6th Cir. 1975), *cert. den*. 428 U.S. 909 (1977). "The reluctance to exercise this drastic power should be especially great where temporary relief is sought." *Kass v. Arden-Mayfair, Inc*., 431 F. Supp. 1037, 1047 (C.D. Cal. 1977).

A court may grant a motion for reconsideration when the court has misunderstood a party or there is a significant change in the law or facts since the submission of the issues to the court by the parties. *Reyes Canada v. Rey Hernandez*, 224 F.R.D. 46, 48 (D.P.R.2004) (citing *Bank of Waunakee v. Rochester Cheese Sales, Inc.*, 906 F.2d 1185, 1191 (7th Cir.1990)). Under Fed.R.Civ.P. 59(e), a party may direct the district court's attention to newly discovered material evidence or a manifest error of law or fact enabling the court to correct its own errors. *Aybar v. Crispin-Reyes*, 118 F.3d 10, 15 (1st Cir. 1997).

In this motion for reconsideration, the students draw the Court's attention to the following changed facts and manifest errors of law. First, the DEFCON conference at which the students planned to present their research has now passed and the students did not give their talk. They no longer plan to present that talk, but merely want to publicly explain and verify the

security vulnerability uncovered by their research. Second, most, if not all, of the significant facts known to the students about the Fare Media System are now public, either because they are contained in the slides prepared for and distributed at DEFCON before the TRO issued, or because the MBTA filed research information provided to it by the students on the public docket in this case.

Additionally, the court was wrong to give legal weight to MBTA's version of "responsible disclosure". *See* Memo. ISO Plaintiff's Motion for TRO (Dkt. No. 3) at pp. iv-vi. (arguing for a court order enforcing MBTA's view of responsible disclosure). Contrary to the MBTA's arguments, "responsible disclosure" means only that security professionals must carefully consider when and how to disclose vulnerability information. The "responsible disclosure" norm is not to withhold all details until the vendor or insecure party has a chance to fix, but to take reasonable steps to avoid inadvertently teaching others how to exploit the flaw. See Declaration of Marcia Hofmann (hereafter "Hofmann Decl."), Exhibit A, *Letter From Computer Science Professors and Computer Scientists* at 4-5. Withholding key information about the flaws one discovers while publishing other information, as the students here did, is responsible. This is because disclosure can help security as much or more than hurt it, under certain circumstances. See, e.g. Swire, Peter P., *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?* Journal on Telecommunications and High Technology Law, Vol. 2, 2004. Available at SSRN: http://ssrn.com/abstract=531782.

The students also base this motion on two manifest errors of law – the holding that the CFAA prohibits the communication of information about security problems with computers to any person and the holding that the TRO strikes an acceptable balance between MBTA's financial interests and the students' constitutionally protected speech. The "likelihood of success is the touchstone of the preliminary injunction inquiry." *Philip Morris, Inc. v. Harshbarger*, 159 F.3d 670, 674 (1st Cir. 1998). As discussed in detail below, these manifest errors in law show that the MBTA was never likely to succeed on the merits.

The First Circuit does "not find irreparable injury where only money is at stake and where the plaintiff has a satisfactory remedy at law to recover the money at issue." *Foxboro Co. v. Arabian American Oil Co*., 805 F.2d 34, 36 (1st Cir. 1986). Even a claim of irreparable injury based on an assertion that damages is "not readily susceptible of calculation and likely would not be recovered from the defendants;" *Public Service Co. of New Hampshire v. Town of West Newbury*, 835 F.2d 380, 382 (1st Cir. 1987), is to be closely scrutinized, and "[s]peculative injury does not constitute a showing of irreparable harm." *Id*. at 383.

The MBTA's argument on irreparable harm focuses on trade secret law. *See* Memo. ISO Plaintiff's Motion for TRO (Dkt. No. 3) at pp. iv. This is inapposite. As an initial matter, the MBTA has made no trade secret claim. *See generally* Complaint. Second, trade secrecy law does not protect against reverse engineering, which is all that is claimed here. *See e.g.* Complaint at ¶ 37; *see generally Baystate Technologies, Inc. v. Bentley Systems, Inc*., 946 F.Supp. 1079, 1090-1091 (D.Mass. 1996); *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470 (1974) (holding that reverse engineering is a "fair and honest means" to obtain a trade secret).

Instead the potential harm that MBTA fears is only economic – the possibility that someone might learn from the student's research sufficient information to evade fare payment. Moreover, it is very speculative, since the students have repeated told the MBTA that the students never intended to disclose key details in the public presentation. MBTA admits, as it must, that the "MIT Undergrads stated that they did not intend to harm the MBTA." Complaint at ¶ 50. As noted by security professional Eric Johanson, "key information needed to compromise both the Charlie Ticket and the Charlie Card is not present in the Slides." Johanson Decl. (Dkt. No. 14) at ¶ 11. For example, "[t]he Slides depict a field called 'checksum,' and show that it changes when the ticket value changes, but do not describe how to compute the checksum." *Id*. at ¶ 23; *see also* Confidential Vulnerability Report ("CVR") filed as Henderson Decl. Exhibit 1 (Dkt. No. 10-1) at 2 ("We have purposefully omitted details of this checksum in any public disclosures...").

To the extent that the MBTA has increased the risk of harm by filing the CVR in the public docket, it should not be able to place responsibility on the students.

The balance of hardships also favors the students. When a court balances the hardships, it "must be concerned not only with possible injury to a plaintiff but also with possible injury to the defendant." *Everett J. Prescott, Inc. v. Ross*, 383 F. Supp. 2d 180, 191 (D. Me. 2005). "The loss of first amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion of Brennan, J.).

As noted in the Complaint, the "MIT Undergrads [were] scheduled to give their 'The Anatomy of a Subway Hack' presentation at 1:00 on Sunday, August 10, 2008." Complaint at ¶ 47 (Dkt. No. 1). The conference is now over, the students were silenced, and the presentation will never be given. Hofmann Decl. at ¶¶ 3-4. Even though the Defcon conference is over, the students remain enjoined from disclosing the fruits of their security research, or otherwise demonstrating the security flaws in the MBTA's systems. This restriction causes the students great hardship.

On Monday, August 11, the MBTA filed a motion which raised the question of "whether this is in fact a 'prank,' or whether the MIT Undergrads are in fact able to compromise the Fare Media System in the manner they publicly claim." Motion to Modify Terms But Not Duration of Temporary Restraining Order at 3 (Docket No.16). Likewise, on August 12, the MBTA said to the *Boston Globe*:

> "There have been claims in the past that have been made against our card or other cards, and, happily, they've all been able to be dismissed or dealt with," said Daniel A. Grabauskas, general manager of the Massachusetts Bay Transportation Authority. "I'm confident it will be the same thing here."

Christopher Baxter & Hiawatha Bray, *MIT students' report makes security recommendations to T*, *Boston Globe* (August 12, 2008). Thus, the MBTA is publicly questioning whether the reports that the transit agency is not sufficiently secure are true. The students' research has raised valid concerns about the security of the MBTA's stored value cards, and the students reject the

notion that their research was nothing more than a "prank." However, under the terms of the TRO, the students are unable to effectively participate in this public debate.

Likewise, the public interest strongly favors disclosure. "The public interest carries considerable weight in these matters. … The court must weigh any hindrance or furtherance of the public interest likely to result from interim injunctive relief." *Sheck v. Baileyville School Committee*, 530 F. Supp. 679, 693 (D. Me. 1982) (citing *Yakus v. United States*, 321 U.S. 414, 440-41 (1944)). "Protecting rights to free speech is *ipso facto* in the interest of the general public." *Westfield High School L.I.F.E. Club v. City of Westfield*, 249 F. Supp. 2d 98, 128 (D. Mass. 2003) (citing *Machesky v. Bizzell*, 414 F.2d 283, 289 (5th Cir. 1969) ("First Amendment rights are not private rights ... so much as they are rights of the general public.")).

As an initial matter, open discussion of security vulnerabilities is in the public interest:

> Although presentations on security vulnerabilities often discuss how weaknesses might be exploited, prohibition of open discussion and publication of security vulnerabilities greatly harms the ability of researchers to function, and has a chilling effect not only on publication, but on whether some important research is done in the first place, greatly stifling scientific advancement.

Johanson Decl. (Dkt. No. 14) at ¶ 16; *see generally id.* at ¶¶ 12-18.

Moreover the question of whether or not the MBTA, "a political subdivision of the commonwealth," MGL § 161A-2, is adequately performing its public services remains clouded. Media from Boston and all over the world are now inquiring as to whether the MBTA has adequate security. Hofmann Decl. at ¶ 6. Again the students are unable to participate meaningfully in that debate. *Id.*

It is in the public interest for the residents of the commonwealth to know truthful information about the performance of the security operations of a political subdivision of the commonwealth, which is subsidized by billions in public funds. *See* Complaint at ¶ 19-20 (detailing the billions of tax dollars MBTA received since the 1960s); *see also News Group Boston, Inc. v. National R.R. Passenger Corp.*, 799 F. Supp. 1264 (D. Mass. 1992) (recognizing public interest in opening the operations of a quasi-government transportation agency to the

scrutiny of the public and allowing oversight of operations of a company which is subsidized by taxpayer monies).

I. THE COMPUTER FRAUD AND ABUSE ACT PROHIBITS THE TRANSMISSION OF INFORMATION OR CODE TO A PROTECTED COMPUTER THAT HARMS THAT COMPUTER, NOT THE COMMUNICATION OR DELIVERY OF NON-CLASSIFIED INFORMATION OR CODE TO ANY PERSON OR PERSONS

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A), is a criminal statute targeting unauthorized access to computers, and not the communication of information to other individuals, as Judge Woodlock has held. This is based on five arguments.

First, the text of the section indicates--by the placement of a comma before the clause "to a protected computer"--that the offender must both transmit information to the protected computer and cause damage to that same computer. An offender must transmit information to and harm a protected computer, not to another person, to violate section 1030(a)(5)(A). That section reads:

> Whoever … knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; and [causes or would have caused certain specified loss or harm] shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(5)(A). If possible, the Court must "'give effect ... to every clause and word of a statute.'" *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (*quoting United States v. Menasche*, 348 U.S. 528, 538-39 (1955)). There is a comma between the word "authorization" and the clause "to a protected computer." That comma indicates that "to a protected computer" modifies both the preceding clauses. Both the transmission and the damage must be to a protected computer.

Second, the plain language of the statute indicates that "transmission of information" does not mean "communication of information." This is most easily seen by comparison to

section 1030(a)(1) , which expressly includes a prohibition on "communication" of information about computers deemed to be protected for national defense and related specific purposes.

Section 1030(a)(1) states that:

> Whoever— having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained [Government classified] information … with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully **communicates, delivers,** transmits, or causes to be **communicated**, **delivered**, or transmitted, or attempts to **communicate**, **deliver**, transmit or cause to be **communicated**, **delivered**, or transmitted the same **to any person** not entitled to receive it … shall be punished as provided in subsection (c) of this section.

(Emphasis added.). Where Congress intended to prohibit the dissemination of information to other persons, it clearly indicated so with specific language to that effect. It did not do so in section 1030(a)(5)(A) relied on by the plaintiffs here.

Thus, as the statute itself makes clear, when Congress seeks to control the dissemination of information, it uses the words "communicate" and "deliver" in addition to "transmit," and specifies that the information it seeks to control may not be given "to any person" not entitled to receive it. These phrases are not included in section 1030(a)(5)(A), showing that that section does not apply to or regulate the dissemination of information to persons.

Third, the legislative history of the CFAA shows that Congress intended "transmission" as a technological term used to refer to sending digital programs, software, code or information to a computer. ""Transmission does not refer speech or other forms of communication to human beings. *See* The Introduction of the National Information Infrastructure Protection Act, 104th Congress (1996) (Statement of Hon. Bob. Goodlatte in the House of Representatives) (The provision at issue here "would . . . penalize any person who uses a computer to cause the transmission of a computer virus or other harmful computer program to Government and financial institution computers."). This interpretation has been confirmed by the United States in a criminal prosecution under the statute. See *Government's Motion for Reversal of Conviction, Memorandum of Points and Authorities, Declaration of Ronald L. Cheng,* filed in *United States*

v. McDanel, Ninth Circuit Court of Appeals No. 03-50135 and attached as Exhibit B to the Hofmann Decl.

Because the Court misread section 1030, there is no legal basis for the TRO, which was expressly based only on that provision. For this reason, the order was erroneously entered and should be dissolved. Furthermore, to the extent that the CFAA provision is read to allow the prior restraint of communication of truthful information to people-- as distinguished from transmission from one computer that harms another -- the statute would be in tension with the First Amendment. As such, the doctrine of constitutional avoidance should lead the court to adopt an interpretation of the CFAA that does not raise questions about whether the statute impermissibly burdens First Amendment-protected speech.

The legislative history of the CFAA shows that Congress intended "transmission" as a technological term used for sending digital programs, software, code or information to a computer, and not including speech to other human beings. Until 1994, the CFAA generally prohibited unauthorized access to computers. By that point, however, Congress had become familiar with the problem of computer viruses that damage computers but do not give a trespasser unauthorized access. As such, the statute was amended to include a prohibition on damaging computers through unlawful transmissions of viruses from one computer to another. *See* 18 U.S.C. § 1030(a)(5) (1994). As Senator Leahy explained:

> [C]omputer abusers have developed an arsenal of new techniques which result in the replication and transmission of destructive programs or codes that inflict damage upon remote computers to which the violator never gained "access" in the commonly understood sense of that term. The new subsection of the CFAA created by this bill places the focus on harmful intent and resultant harm, rather than on the technical concept of computer "access."

Violent Crime and Control and Law Enforcement Act of 1994 - Conference Report, 103rd Cong. (1994) (Statement of Sen. Leahy).

In 1996, Congress adjusted the 1994 provisions to the language we see in section 1030(a)(5)(A) today. The legislative history shows that Congress intended the provision to prohibit damaging transmissions of computer viruses and the like from one computer to another:

> The bill would also penalize any person **who uses a computer** to cause the transmission of a computer virus or other harmful computer **program to Government and financial institution computers** not used in interstate communications, such as intrastate local area networks used by Government agencies that contain sensitive and confidential information.

The Introduction of the National Information Infrastructure Protection Act, 104th Congress (1996) (Statement of Hon. Bob. Goodlatte in the House of Representatives), (emphasis added). The legislative history is further proof that the CFAA does not regulate speech about computers, but attacks on computers, whether through unauthorized access or through computer viruses, "worms" and the like.

"'[I]t is a cardinal principle' of statutory interpretation … that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.'" *See, e.g., Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (*quoting Crowell v. Benson*, 285 U.S. 22, 62 (1932); *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 (1936) (Brandeis, J., concurring)). To the extent that the CFAA regulates information about computer security flaws, it is a content-based speech regulation, presumptively unconstitutional and subject to strict constitutional scrutiny.

II. THE TEMPORARY RESTRAINING ORDER IS AN UNCONSTITUTIONAL PRIOR RESTRAINT ON PROTECTED SPEECH AND MUST BE OVERTURNED

This TRO is an unconstitutional prior restraint that must be overturned, and no preliminary injunctive relief could constitutionally issue in the alternative. A prior restraint is a government regulation that limits or conditions in advance the exercise of protected First Amendment activity. Prior restraints are extremely disfavored and rarely, if ever, upheld. The Supreme Court has rejected prior restraints in cases involving national security, and cases where

the information to be published has been illegally obtained, whether by a third party or by the speaker. The TRO here, which has already resulted in preventing the students from presenting their research publicly and which continues to gag them from discussing their factual findings, is unjustified, vague and overbroad. It must be rejected and no TRO or other restraining order should issue at least until there has been a full trial on the merits to determine whether the students have (1) committed the alleged torts and (2) whether their conduct or the content of their research means that their research findings are not constitutionally protected.

A judicial injunction that prohibits speech prior to a determination that the speech is unprotected constitutes a prior restraint. *Near v. Minnesota*, 283 U.S. 697, 719 (1931). Any prior restraint is the most dangerous imposition on individuals' freedom of speech. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976) ("Prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights"). Therefore, request for such a restraint "comes to [the] Court bearing a heavy presumption against its constitutional validity." *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971). See also *Auburn Police Union v. Carpenter*, 8 F.3d 886, 903 (1st Cir. 1993).

"In the case of a prior restraint on pure speech, the hurdle is substantially higher [than for an ordinary preliminary injunction]: publication must threaten an interest more fundamental than the First Amendment itself. Indeed, the Supreme Court has never upheld a prior restraint, even faced with the competing interest of national security or the Sixth Amendment right to a fair trial." (*Proctor & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 226-227 (6th Cir. 1996); *cf. Nebraska Press Assn. v. Stuart,* 427 U.S. 539, 563 (1976) (the Sixth Amendment right of a criminal defendant to a fair trial does not outrank the First Amendment right of the press to publish information); *New York Times Co. v. United States* (1971) 403 U.S. 713, 718-726 ("national security" interest in suppressing classified information in the Pentagon Papers did not outrank First Amendment right of press to publish classified information). "[I]t is clear that few things, save grave national security concerns, are sufficient to override First Amendment interests." *United States v. Progressive, Inc.* 467 F. Supp. 990, 992 (DC Wisc. 1979) (court

issued prior restraint on publication of technical information about hydrogen bomb only because it found that such information was analogous to information about troop movements which posed a grave threat to national security).

The Plaintiff has not and cannot justify a prior restraint on the speech at issue in this case, as explained below. First, truthful scientific speech, including instructions that enable the recipient to use the scientific information for an illegal purpose, are constitutionally protected.[1] For example, information about how to cultivate marijuana or how to pick a lock is constitutionally protected. Second, the speech remains protected even if the students obtained the information illegally (which they did not) or if another party could use the information for illegal purposes. Third, the information is on a matter of public interest. In contrast, the MBTA's interests do not come close those of the government in the Pentagon Papers case, which also failed to justify a prior restraint on publication.

This TRO limits the exercise of the students' free speech, despite the fact that the First Amendment protects scientific speech. Courts have subjected restrictions on the dissemination of technical scientific information and scientific research to First Amendment scrutiny. *United States v. Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979); Board of Trustees of *Stanford University v. Sullivan*, 773 F. Supp. 472, 473 (D.D.C. 1991). Instructions are also constitutionally protected expression. *See*, *e.g.*, *United States v. Raymond*, 228 F.3d 804, 815 (7th Cir. 2000) (First Amendment protects instructions for violating the tax laws, but not where such instructions are an incitement to imminent unlawful activity); *United States v. Dahlstrom*, 713 F.2d 1423, 1428 (9th Cir. 1983) (same); *Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017, 1020-25 (5th Cir. 1987) (First Amendment protects instructions for engaging in a dangerous sex act); *see also Bernstein v. United States Department of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) ("Instructions, do- it-yourself manuals, [and] recipes" are all "speech"). Thus the TRO in

[1] Nor do First Amendment protections disappear if the MBTA does not approve of the tone of the speech. As Justice Frankfurter wrote, the right of free expression "means not only informed and responsible criticism but the freedom to speak foolishly and without moderation." *Baumgartner v. United States*, 322 U.S. 665, 674 (1944).

this matter, which continues to prevent the students from publicly discussing scientific facts and research that they have conducted, is an unconstitutional prior restraint.

The TRO as initially granted restricted the students from providing true, publicly known, legally acquired information about the MBTA's CharlieCards and CharlieTickets in violation of the First Amendment. See *Veilleux v. National Broadcasting Co.*, 206 F.3d 92, 127 (1st Cir. 2000) (truthful information is more deserving of protection than false information). The current TRO as the MBTA suggests that it be modified still restricts the students from providing true, legally acquired information about these cards This restriction also violates the First Amendment. *Id. See also Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (the publication of even illegally-acquired information enjoys some First Amendment protection).

This conclusion does not change even if other people could use the information contained in the students' presentation for criminal purposes. Settled precedent provides that even such information is constitutionally protected. The Supreme Court has stated that while there are some rare occasions in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another, these occasions are extremely rare, and only occur when the speech at issue is of extremely low value. *Id.* at 530 (referring to child pornography). The speech at issue here is of much higher value than child pornography, consisting of facts learned from scientific investigation and analysis. Most speech that is alleged to be "crime facilitating" has both harmful and valuable uses, including some that are not initially obvious. Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1105 (2005).

For example, the letter from computer science professors and computer scientists discusses the ways in which disclosure of security vulnerability information promotes security rather than defeats it, regardless of the wishes of the entity whose systems are weak. Hofmann Decl. Exhibit A at 2 ("Researchers discover flaws. They invent new and improved ways to detect and correct flaws, and they invent new and improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward at an

extraordinary pace for more than half a century"); *see also* 5 ("When large public security systems are at issue, the norm in our field is that researchers take reasonable steps avoid inadvertently teaching others how to exploit the flaw. … Yet at the same time that researchers need to act responsibly, vendors should not be granted complete control of the publication of such information, as it appears MBTA sought here.")

Because disclosure can benefit security and because security researchers need to make careful decisions about how much detail about a particular security risk they should make public, prohibiting vulnerability disclosure before any adjudication of criminality or constitutionality is unconstitutional. Recognition that it is hard to judge whether speech is "good" or "bad" ahead of time is the basis for the constitutional distaste for prior restraints.

Even if the information contained in the students' presentation was itself obtained illegally, which it was not, that information is constitutionally protected and my not be the subject of a prior restraint. In *In re King World Productions, Inc.*, 898 F.2d 56 (6th Cir. 1990), the Sixth Circuit overturned a temporary restraining order prohibiting a news program from airing video footage it illegally taped of a doctor allegedly engaging in malpractice. Similarly, in *CBS, Inc. v. Davis*, 510 U.S. 1315 (1994), a television network obtained undercover footage at a South Dakota meat packing plant that it intended to air. The packing plant operator obtained an order restraining the network from broadcasting its footage. The Court vacated the temporary restraining order: "Although the prohibition against prior restraints is by no means absolute, the gagging of publication has been considered acceptable only in 'exceptional circumstances.'" *Id*. at 1317.

These are not exceptional circumstances. The students' research on the MBTA's fare payment system is a matter of great public concern. Even before this case occurred, both the Boston Globe and the Boston Herald published articles on security flaws with the CharlieCard. Bray, Hiawatha, "*T Card Has Security Flaw, Says Researcher*", Boston Globe, March 6, 2008; Szaniszlo, Marie, "*Research: Charlie Card is Far From Hack Proof*", Boston Herald, March 6, 2008. On the other hand, the MBTA's interest in keeping this information quiet is certainly no

greater than that of the government in squelching the Pentagon Papers. Nor is the possibility that someone may use the information to get free subway rides sufficient reason to suppress publication of the research.

Finally, the scope of this TRO is both overbroad and vague. The initial TRO unconstitutionally prohibited discussion even of information the plaintiff placed in the public record. MBTA has moved to narrow the TRO to only "non-public" information in recognition of this problem, but this limitation does not resolve the issue. is the TRO remains vague because it is uncertain what information materially helps another person to circumvent the security of the Fare Media System. As the court stated, merely drawing attention to a security problem could focus an attacker on the fact that a particular attack can be done and might be worth trying. The attacker no longer has to wonder whether it is possible; it is. Just that fact might materially assist someone. It is impossible to know in advance, and neither the court nor MBTA could give any clear guidance, which is why counsel felt compelled to advise the students that they could not give their presentation at the Defcon conference. As the Court itself recognized, red-penciling the student presentation to delete objectionable material was not a viable option, the injunction meant that the students might choose not to go forward with their talk, and that if they did, they faced the possibility of contempt charges. Thus, the TRO chilled protected speech.

///

CONCLUSION

For the foregoing reasons, the students request that this court vacate the temporary restraining order.

DEFENDANTS ANDERSON, RYAN AND CHIESA

By their attorneys,

Dated: August 12, 2008

/s/ Emily A. Berger

Emily A. Berger, BBO No. 650,841
emily@eff.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	)	CIVIL ACTION NO. 08-11364-GAO

DECLARATION OF MARCIA HOFMANN IN SUPPORT OF DEFENDANTS' RESPONSE TO PLAINTIFF'S "MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER" AND CROSS MOTION FOR RECONSIDERATION

1. The Electronic Frontier Foundation ("EFF") represents Defendants Anderson, Ryan and Chiesa (hereafter "students") in this matter. I am a staff attorney with the EFF and a member in good standing of the California State Bar. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

2. This declaration is submitted in support of the Defendants' Motion for Reconsideration of Temporary Restraining Order.

3. The DEFCON conference in Las Vegas concluded on August 10, 2008. As a result of the temporary restraining order issued by this Court on August 9, 2008, the students did not present their research on the security of the Boston T fare system at that conference.

4. The students do not intend to give the presentation scheduled for Defcon at any future conference.

5. On August 8, 2008, the students provided the Massachusetts Bay Transportation Authority ("MBTA") a confidential report containing sensitive information derived from their research. The report disclosed all important aspects of the students' research into the security of the Boston T fare system, including details that they never intended to make public. This report has now been revealed to the public through the MBTA's unsealed filings in this case. As a result, the August 9, 2008 temporary restraining order improperly serves to prevent the students from disclosing to the public information that MBTA itself has already made public.

6. As a result of the students' research and the attention drawn to it by the above-captioned lawsuit, media in Boston and throughout the world are inquiring as to whether the MBTA's fare system has adequate security. Because of the August 9, 2008 temporary restraining order, the students are unable to participate meaningfully in that debate.

7. Attached hereto as Exhibit A is a true and correct copy of the Department of Justice's Motion for Reversal of Conviction, Memorandum of Points and Authorities, Declaration of Ronald L. Cheng filed on October 15, 2003 in *United States v. McDanel,* No. 03-50135 (9th Cir. dismissed Dec. 15, 2003).

8. Attached hereto as Exhibit B is a true and correct copy of a letter to the Court from computer science professors and computer scientists concerning the above-captioned case and dated Aug. 11, 2008.

I declare under penalty of perjury of the laws of the State of California that the foregoing

is true and correct to the best of my knowledge and belief. Executed August 12, 2008 in San Francisco, California.

/s/ Marcia Hofmann
Marcia Hofmann

EXHIBIT A

IN THE

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRET McDANEL, Defendant-Appellant.	C.A. No. 03-50135 D.C. No. CR 01-638-LGB (Central Dist. Cal.) GOVERNMENT'S MOTION FOR REVERSAL OF CONVICTION; MEMORANDUM OF POINTS AND AUTHORITIES; DECLARATION OF RONALD L. CHENG

Plaintiff-Appellee United States of America, pursuant to Federal Rule of Appellate Procedure 27, and by and through its attorney of record, Assistant United States Attorney Ronald L. Cheng, hereby respectfully requests this Court to reverse defendant's conviction in this case. Defendant has served his term of imprisonment and is currently serving his term of supervised release.

//

//

//

//

//

//

//

//

This motion is based upon the files and records of this case, the attached memorandum of points and authorities and the attached declaration of Ronald L. Cheng.

Dated: October 14, 2003

Respectfully submitted,

DEBRA W. YANG
United States Attorney

STEVEN D. CLYMER
Special Assistant U.S. Attorney
Chief, Criminal Division

RONALD L. CHENG
Assistant United States Attorney
Chief, Criminal Appeals Section

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

MEMORANDUM OF POINTS AND AUTHORITIES

I

INTRODUCTION

Defendant-appellant Bret McDanel has appealed his conviction after court trial (before the Hon. Lourdes G. Baird, United States District Judge) on one count of causing damage to a protected computer, under former 18 U.S.C. § 1030(a)(5)(A) (2000) ("Section 1030"). Among his claims, defendant asserts that the statute of conviction, which requires that one intend to "damage" in the sense of "impairment to the integrity" of a protected computer, does not extend to his conduct, in which defendant transmitted information concerning a means of accessing a computer system to the computer system's users. After further review of this matter in light of the arguments made by defendant on appeal, the government concedes that the evidence did not establish an intent to "damage" within the meaning of the statute, and requests that this Court reverse defendant's conviction.

II

FACTUAL BACKGROUND

Defendant was a systems administrator at Tornado Development, Inc. ("Tornado"). Tornado provided a "unified messaging" service to its customers, which included accounts that held e-mail, voice mail, paging, and faxing services in one place. (Reporter's Transcript ("RT") [6/11/02] 101; Defendant's

Excerpts of Record ("ER") 155). As the company's systems administrator, defendant understood how to test the limits of the system by sending large numbers of e-mail through it to cause it to "crash." In addition, defendant learned that, when a user logged onto the system, the Tornado system would provide a numerical code, known as the "NID," which allowed a user to remain on the system. (RT [6/11/02] 103-13; ER 157-67). If, however, the user linked to an outside website through an e-mail, the Tornado system would transmit the NID to that site and an outsider could theoretically gain access to the user's account through the NID. (Trial Exhibit ("Ex.") 147; RT [6/18/02] 116; ER 288, 545-47). No one had actually broken into the Tornado system through the NID, and the existence of the NID was confidential. (RT [6/11/02] 115, 116; ER 169, 170). As a systems administrator, defendant told Tornado he believed the NID disclosure problem should be fixed, but Tornado declined to do so. (Ex. 19; ER 517-19).

Because of difficulties defendant had with other employees, defendant left Tornado. Afterwards, defendant sent three e-mail attacks between August 31, 2000, and September 5, 2000, through Tornado's server to the company's customers. (RT [6/12/02] 45-48, 76, 90-92; RT [6/14/02] 132-36; ER 175-78, 181, 182-84, 251-55). The volume of e-mails overloaded the capacity of the server and caused the Tornado system to "crash," so that the system was

inoperable until technicians could bring the system back on line. (Id.). Each e-mail, which included a link to a website that defendant operated, informed the reader about the existence and operation of the NID, which defendant characterized as a security flaw that Tornado declined to repair. (Exs. 30-31; ER 520-22).

III

AFTER REVIEW OF THIS MATTER, THE GOVERNMENT CONCEDES THAT DEFENDANT'S CONVICTION SHOULD BE REVERSED

In the district court, the government argued, and the court found, that the evidence supported a conviction for a single violation of § 1030(a)(5). Upon further consideration, in light of arguments presented by defendant on appeal, the government has concluded that these contentions, which the government believed at the time of trial were a proper, good faith construction of the statute, led the district court into error. The government now acknowledges that the evidence adduced below was insufficient to support a finding beyond a reasonable doubt that defendant intentionally caused "damage" to Tornado's computer system (within the meaning of § 1030(a)(5)) that resulted in $5,000 in loss. Accordingly, the government asks that this Court reverse the judgment of conviction entered against defendant.

Section 1030(a)(5), as it existed in 2000, penalizes one who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected

computer . . . ." The government argued below that defendant's transmission of over 5,000 electronic mail messages to Tornado's customers on September 1, 2000, caused "damage" to Tornado's computer system. As the term "damage" was defined in 18 U.S.C. § 1030(e)(8) (2000), "any impairment to the integrity or availability of data, a program, a system, or information" that causes loss aggregating $5,000 in value to one or more individuals constituted "damage."[1]

The government argued that defendant intentionally caused damage under two theories, both of which were necessary to support the guilty verdict on this charge. The government argued, first, that defendant intentionally caused damage to Tornado's computer system by impairing its availability, in that McDanel knowingly and intentionally sent a sufficient number of messages to cause Tornado's messaging system to overload and fail, and that he intended to have it so fail. All elements under this theory were proven before the district court. This first theory of the case was supported by the evidence, but the total loss connected to the impairment of availability was insufficient by itself to meet the $5,000 threshold required by the statute.

---

[1] The statute permits proof of consequences other than $5,000 in monetary loss to meet this element. 18 U.S.C. § 1030(e)(8)(A)-(D) (2000). The monetary loss element was the only one attempted to be proven at trial, however, and is the only one arguably applicable to this case.

The government also argued that defendant's transmission of electronic mail messages had intentionally caused damage to Tornado's computer system by impairing its integrity, based on the government's good faith belief at the time of trial that a valid interpretation of the statute supported this meaning of "damage." The government now acknowledges that the evidence introduced was insufficient to meet the elements of the statute beyond a reasonable doubt as to this second theory. Without the monetary loss attributable to this second theory, the necessary $5,000 threshold required by the statute cannot be proven, and thus all elements of the charged offense were not proven beyond a reasonable doubt.

In the district court, the government advanced the theory that defendant had intentionally "impaired the integrity" of Tornado's computer system by revealing confidential information relating to the operation of the Tornado server. This information made it easier for outsiders to access this system. It also required Tornado's staff to undertake immediate and expensive corrective action to counteract defendant's actions. These corrective actions included changing Tornado's messaging system so that the vulnerability identified by defendant was patched, testing the system, and consulting with customers concerned that their data may have been accessible. Because Tornado expended significant resources to respond to defendant's

conduct, the government argued that the $5,000 damage threshold had been met.

On further review, in light of defendant's arguments on appeal, the government believes it was error to argue that defendant intended an "impairment" to the integrity of Tornado's computer system. Despite defendant's actions to transmit and publish the vulnerability to Tornado's customers, and the harm to Tornado's business that resulted, there was no proof that defendant intended his messages to aid others in accessing or changing the system or data.[2] Instead, the evidence established that defendant informed Tornado's customers -- the people whose data may have been vulnerable to unauthorized access -- about the vulnerability, an action that could have brought about repair of the problem. Accordingly, because the government did not prove that there was an intent to "impair the integrity" of the computer system in the sense set forth above, the loss directly resulting from the disclosure of the vulnerability itself should not have been attributed to defendant.[3]

---

[2] The government did not argue or seek to prove in the district court that anyone outside of Tornado acted on defendant's message to actually access or change Tornado's system or data. Title 18, United States Code, Section 1030(a)(5), requires that a defendant knowingly cause the transmission of a program, information, code or command, and that intentional damage occur "as a result of" that conduct.

[3] Defendant's actions were not wholly blameless, particularly when viewed in light of the Rule 404(b) evidence admitted relating to his intrusion activity at his former

Defendant's release of vulnerability information did not by itself cause an "impairment to the integrity" of a computer system where there is no proof that "data, a program, a system, or information" has been accessed or changed as a result of that release of information nor that defendant intended such an outcome. It is on this principle that the government confesses error in this case. While distribution of this information with specific intent that someone use it to access or damage a computer system could potentially be illegal, that case is not presented here.

---

employer in New Jersey. Defendant revealed confidential information relating to the operation of Tornado's system and undertook these actions with at least the partial intent to embarrass Tornado and harm its relationship with its customers, as well as to crash its computers, thus disrupting the services it provided. The public revelation of this vulnerability increased the likelihood that someone would access the private correspondence of Tornado's customers. If defendant's specific intent to bring about such a harm to Tornado or its customers had been proven, his conduct might have violated Section 1030 or constituted another crime. For example, knowingly trafficking in "passwords or similar information through which a computer may be accessed without authorization" violates 18 U.S.C. § 1030(a)(6). If defendant had specifically intended that his release of vulnerability information would aid another in committing an intrusion into or damage to Tornado's computers, it could constitute aiding and abetting a violation or an attempted violation of 18 U.S.C. § 1030. An individual could also pass on vulnerability information to another in furtherance of a conspiracy to commit a violation of 18 U.S.C. § 1030 or another crime. Similarly, if an employee reveals confidential business information for profit or with the purpose of defrauding an employer, that conduct could potentially form the basis for a mail or wire fraud charge. 18 U.S.C. §§ 1341, 1343. See Carpenter v. United States, 484 U.S. 19 (1987). Defendant was not charged, however, under any of these theories, and the court need not reach these issues in this case.

Accordingly, the government concedes that there was insufficient evidence to prove a violation of 18 U.S.C. § 1030(a)(5)(A) (2000), the sole offense for which defendant was tried.

IV

CONCLUSION

For the reasons stated above, the government requests that this Court reverse the conviction in this case.

DECLARATION OF RONALD L. CHENG

I, RONALD L. CHENG, hereby declare the following:

1. I am an Assistant United States Attorney in the Central District of California and am the Chief of the Criminal Appeals Section in this office. In that capacity, I am coordinating the preparation of the government's response in United States v. Bret McDanel, D.C. No. 01-638-LGB and C.A. No. 03-50135. I have knowledge of the facts set forth herein and, if called as a witness, could and would testify competently thereto.

2. On October 14, 2003, I attempted to contact defense counsel, Jennifer Stisa Granick, Esq. According to Ms. Granick's voicemail message, Ms. Granick is out of the office until October 20, 2003. and spoke with her assistant, Ms. Joanne Newman. In my voicemail message for Ms. Granick and in my conversation with Ms. Newman, I stated that the government would be filing a motion to reverse defendant's conviction.

//

//

3. Defendant has served his term of imprisonment and is currently on supervised release.

I declare under penalty of perjury, pursuant to the laws of the United States, that this declaration is true and correct.

Executed October 14, 2003, Los Angeles, California.

RONALD L. CHENG

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRET MCDANEL, Defendant-Appellant.	C.A. No. 03-50135 D.C. No. CR 01-638-LGB (Central Dist. Cal.) DECLARATION OF SERVICE BY MAIL

I, Nancy Johnson, declare:

That I am a citizen of the United States and a resident of Los Angeles County, California; that my business address is 312 North Spring Street, Los Angeles, California 90012; that I am over the age of 18 years, and am not a party to the above-entitled action; that on **October 14, 2003**, I deposited in the United States mail in Los Angeles, California, in the above-entitled action, in an envelope bearing the requisite postage, a copy of: **GOVERNMENT'S MOTION FOR REVERSAL OF CONVICTION; MEMORANDUM OF POINTS AND AUTHORITIES; DECLARATION OF RONALD L. CHENG**

addressed to:

Jennifer Stisa Granick
Center for Internet and Society
Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610

at the last known address, at which place there is a delivery service by United States mail.

I declare under penalty of perjury that the foregoing is true and correct.

DATED: This **14th** day of **October, 2003.**

Nancy Johnson

NANCY JOHNSON

EXHIBIT B

August 11, 2008

Hon. George A. O'Toole, Jr.
United States District Court
Federal District of Massachusetts
John Joseph Moakley U.S. Courthouse
Courtroom 9, 3rd Floor
1 Courthouse Way
Boston, MA 02210

Re: *Massachusetts Bay Transportation Authority v. Anderson, et. al,*
Case # 08-11364-GAO
Letter from Computer Science Professors and Computer Scientists

Dear Judge O'Toole:

We are computer scientists and researchers, many from the nation's top research and educational institutions. We write in letter form because we understand that time is short and that a temporary restraining order is currently in effect preventing the MIT student researchers from discussing their work. We hope this letter will assist you in your consideration of the Motion for Reconsideration.

Each of us engages in scientific research relating to computer systems and technologies. Each of us also engages in the routine publication and public discussion of that work. Our specific titles are listed with our signatures below.

We were quite troubled to learn that the Court has enjoined the students from discussing their research on the MBTA's fare payment system because that research might materially assist another person in defrauding the system. We write to express our firm belief that research on security vulnerabilities, and the sensible publication of the results of the research, are critical for scientific advancement, public safety and a robust market for secure technologies. Generally speaking, the norm in our field is that researchers take reasonable steps to protect the individuals using the systems studied. We understand that the student researchers took such steps with regard to their research, notably by planning not to present a critical element of a flaw they found. They did this so that their audience would be unable to exploit the security flaws they uncovered. We also believe that restraining orders such as that issued by the court over the weekend could have a devastating chilling effect on such research in the future.

Factual Background to this Letter

The focus of our letter is not on the specifics of this security research done by the MIT student researchers. Instead, we wanted to provide you with information about publishing computer security research and the dangerous impact that restraining orders such as the one issued here could have on that research.

This letter is based on our understanding of the following facts: the MIT students performed security research on the payment mechanisms for the MBTA fare collection system as part of a class project for which they received a superior grade. The students then submitted a presentation based on that research to the DEFCON security conference held in Las Vegas from August 6-10, 2008.

The students presented their research to technical representatives of the MBTA and to the FBI a few days before the conference. They also provided a confidential paper detailing the problems they found and proposed solutions. The confidential paper contained technical information not contained in their planned public presentation. The students informed the MBTA that they were not intending to release the entire results of their research, but instead were intending to withhold key pieces of information that could allow replication of their exploits. We also understand that the students engaged in puffery in advertising their presentation, stating that it would allow "free subway rides for life."

We are aware that both the slides for the intended presentation and the confidential paper have now been made widely publicly available, both through the conference materials submitted prior to the filing of the lawsuit and through filings in the public docket in this case by the MBTA.

The Nature Of Computer Systems Research

Much research in computer systems is based upon analysis - the careful examination of existing systems and approaches in order to understand what works well and what works poorly. Researchers discover flaws. They invent new and improved ways to detect and correct flaws, and they invent new and improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward at an extraordinary pace for more than half a century.

Analysis is no less important when the system being studied is used to pay for public transit or any other public function. The best security systems are not one-off systems designed from scratch for single use, but designs that build upon prior

research. For this reason, it is critical that the researchers and engineers developing new systems be able to study existing ones for advantages and flaws. In turn, a system's ability to withstand repeated attacks best allows engineers and the public to trust its security. At a recent major computer security conference, for instance, about 15% of the papers presented were papers describing attacks on technical systems. Such research is broadly accepted in the profession.

The Importance Of Open Discussion And Publication To Computing Research

Open discussion of computing research and publication of its results is essential to the conduct of computing research. The computing research community is large - many thousands of individuals who follow the literature of security research. In computer science research, the "literature" includes code, algorithms, and their analysis.

Broad review and critique are fundamental to the advancement of research. There is a long history of open research in computer security and information hiding. It is no exaggeration to say that most of the security and information hiding technologies upon which we rely today are the products of this open research process.

The Importance Of Open Discussion And Publication On Public Safety And The Market

The restraining order at issue in this case also fosters a dangerous information imbalance. In this case, for example, it allows the vendors of the technology and the MBTA to claim greater efficacy and security than their products warrant, then use the law to silence those who would reveal the technologies' flaws. In this case, the law gives the public a false sense of security, achieved through law, not technical effectiveness. Preventing researchers from discussing a technology's vulnerabilities does not make them go away - in fact, it may exacerbate them as more people and institutions use and come to rely upon the illusory protection. Yet the commercial purveyors of such technologies often do not want truthful discussions of their products' flaws, and will likely withhold the prior approval or deny researchers access for testing if the law supports that effort.

As an example, computer anti-virus experts rely heavily on public dissemination of timely information about threats on the horizon. For instance, the "Code Red" worm released a few years ago was designed to spread rapidly for about a week, and it was very successful at infecting more than 200,000 computers. Security

researchers across the country rallied together in a concerted effort to blunt the attack, and discovered through last-minute reverse engineering (disassembly) that the worm was designed to make all infected machines attack the White House web server on a specified date. With only a few days to counter this threat, experts were able to study the reverse engineered worm to identify a weakness of the attack and counter it, protecting the White House web server and others. This containment of the Code Red worm would not have been possible without immediate, unrestricted public dissemination of full information about its spread, which included open discussion of the flaws it exposed in other computer software.

Similarly, in 1989 complexity theorists Adi Shamir and Eli Biham invented the technique called differential cryptanalysis, which called into question the strength of various ciphers. The research prevented weaker systems from being adopted to replace the famous DES block cipher, which was then being used by all commercial banking systems and by the U.S. government. Nonetheless, the two scientists were treated as heroes rather than criminals. The publication of a new means of attacking encryption – called differential cryptanalysis - made it possible for the research community to design the AES block cipher, which is vastly more secure as a result of this understanding and is now the federal encryption standard.

This free flow of information also helps the market. With free flow of information about the cost and quality of different payment and security schemes, market forces should lead to the production of better and cheaper schemes. By chilling the flow of information about the quality of competing fare collection schemes, orders such as that issued by the court cripple the market's ability to reward higher quality schemes.

The analogy to the research done by the MIT students is obvious. A break in the security system for payments on the MBTA system teaches how to design better systems. If a break exists it will be discovered. It is much better from everyone's perspective if researchers discover the break and publish it than if unscrupulous discoverers of the break exploit it without public notice. While the publication need not always contain every detail necessary to allow criminal exploitation of the flaw, as the students here rightly decided, the fact of the security flaw should not have been hidden from the public.

Responsible Security Disclosures

It is the case that security researchers need to make careful decisions about how much detail of a particular security break they should make public. Generally

speaking, when large public security systems are at issue, the norm in our field is that researchers take reasonable steps avoid inadvertently teaching others how to exploit the flaw. From what we understand of the facts, the MIT student researchers took such steps in planning their presentation, withholding key information about the flaws they discovered. They also intended to do the same in the future, although this might not be necessary any more since we understand that the MBTA has now voluntarily placed that same information in the public record in this case.

Yet at the same time that researchers need to act responsibly, vendors should not be granted complete control of the publication of such information, as it appears MBTA sought here. As noted above, vendors and users of such technologies often have an incentive to hide the flaws in the system rather than come clean with the public and take the steps necessary to remedy them. Thus, while researchers often refrain from publishing the technical details necessary to exploit the flaw, a legal ban on discussion of security flaws, such as that contained in the temporary restraining order, is especially troubling.

Chilling Effect of the Court's Order

The court's order, if not lifted, will chill research and publication when the technologies or systems in question are used to collect payments on public transportation. Fears of violating vaguely-defined prohibitions are expected to lead researchers to choose "safer" topics of study and to censor their publications rather than risk lawsuits.

In particular, the court's ruling that "transmission" of a computer program to a computer system could include a public presentation about flaws in the security of the system is especially troubling. It is even more so here because we understand that key portions of the research needed to duplicate the attack were not going to be presented at the conference and will not be presented in the future.

Conclusion

In sum, we are concerned that the pall cast by the temporary restraining order will stifle research efforts and weaken academic computing research programs. In turn, we fear the shadow of the law's ambiguities will reduce our ability to contribute to industrial research in security technologies at the heart of our information infrastructure. We urge that you reconsider and remove the temporary restraining order issued on August 10, 2008.

Sincerely,

Professor David Farber[1]
Distinguished Career Professor of Computer Science and
Public Policy in the School of Computer Science
Carnegie Mellon University

Professor Steven M. Bellovin
Professor of Computer Science
Columbia University

Professor David Wagner
Associate Professor of Computer Science
University of California at Berkeley

Professor Dan Wallach
Associate Professor of Computer Science
Rice University

Professor Tadayoshi Kohno
Assistant Professor of Computer Science and Engineering
University of Washington

Professor David Touretzky
Research Professor
Computer Science Department &
Center for the Neural Basis of Cognition
Carnegie Mellon University

[1] All titles are for affiliation purposes only.

Patrick McDaniel
Co-Director Systems and Internet
Infrastructure Security Laboratory (SIIS)
Pennsylvania State University

Professor Lorrie Faith Cranor
Associate Professor of Computer Science
and Engineering and Public Policy
Carnegie Mellon University

Professor Matthew Blaze
Associate Professor of Computer and Information Science
University of Pennsylvania

Stefan Savage
Associate Professor
Department of Computer Science and Engineering
University of California, San Diego

Bruce Schneier
Chief Security Technology Officer, BT

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	)	CIVIL ACTION NO. 08-11364-GAO

DECLARATION OF JENNIFER GRANICK REGARDING SCHEDULING OF DEFENDANTS' RESPONSE TO PLAINTIFF'S "MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER" AND CROSS MOTION FOR RECONSIDERATION

1. The Electronic Frontier Foundation ("EFF") represents Defendants Anderson, Ryan and Chiesa in this matter. I am Civil Liberties Director with the EFF and a member in good standing of the California State Bar. I have been allowed to appear before this Court *pro hac vice* in this matter and am in the process of identifying local counsel. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

2. This declaration is submitted in support of the Defendants Anderson, Ryan, and Chiesa's Response To Plaintiff's "Motion To Modify Terms But Not Duration Of Temporary Restraining Order" And Cross Motion For Reconsideration. Defendants (hereafter "students") respectfully request that the Court hold a hearing on their Motion for Reconsideration this week, preferably on August 14, 2008.

3. The Court should hear the cross motion for reconsideration at the same

time as the motion to amend because the motions address identical issues, the propriety of the TRO issued against the students on August 8, 2008.

4. The facts have changed since the issuance of the TRO. The DEFCON conference at which the students planned to present their research is now over, the students did not present, and have no plans or desire to give the presentation elsewhere.

5. A prompt hearing is also necessary because the information that the original TRO sought to keep confidential has now been publicly disclosed by MBTA. Specifically, the students disclosed to the MBTA sensitive information derived from their research on August 8, 2008 in a confidential vulnerability report ("CVR"). The CVR, which contained details of the students' research that they never intended to publicly disclose, has now been revealed to the public through the MBTA's unsealed filings in this case.

6. The CVR reveals all the important aspects of the students' research into the security of the Boston T fare system. As a result, the temporary restraining order now serves only to prevent them from disclosing information already available to the public.

7. Media from Boston and all over the world are now inquiring as to whether the MBTA has adequate security. The MBTA has called the student research "a prank" and the students are unable to explain or clarify their work.

8. For these reasons, as more fully discussed in the motion for reconsideration, the students respectfully request that this Court calendar the cross motion at the same time as the hearing on MBTA's motion to modify.

9. On the morning of August 11, 2008, I informed Ieuan Mahony, counsel for MBTA, that we would be filing a motion for reconsideration on shortened time. I

inquired as to what days this week he would be available or unavailable, but he has not responded to that inquiry. Meanwhile, he informed me that MBTA would be filing this motion to modify. The Court Clerk called today to tell me that the hearing would be Thursday, August 14, 2008 at 11A

I declare under penalty of perjury of the laws of the State of California that the foregoing is true and correct to the best of my knowledge and belief. Executed August 12, 2008 in San Francisco, California.

/s/ Jennifer Granick
Jennifer Granick

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

MOTION FOR ADMISSION *PRO HAC VICE*

Pursuant to Massachusetts Local Rule 83.5.3(b), Emily Berger, Esq., a member in good standing of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, moves for the admission of Jennifer Stisa Granick, a member of the Bar of the State of California, to this Court for the purpose of representing defendants in the above-captioned matter, and states as follows:

1. Jennifer Granick is counsel at the Electronic Frontier Foundation. Her business address is 454 Shotwell Street, San Francisco, CA 94110. Her telephone number is (415) 436-9333.

2. Jennifer Stisa Granick is a member in good standing of the Bar of the State of California, as evidenced by the Certificate of Good Standing attached hereto as Exhibit A. There are no disciplinary proceedings pending against her as a member of the bar in any jurisdiction. See Affidavit of Jennifer Stisa Granick, attached hereto as Exhibit B.

3. Jennifer Stisa Granick is familiar with the applicable provisions of the

Local Rules of the United States District Court for the District of Massachusetts.

4. Emily Berger, a member of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, will continue to represent defendants if this motion is granted.

5. In accordance with this Court's fee schedule, a fifty dollar ($50) filing fee will be paid for the admission of Jennifer Stisa Granick to this Court within 24 hours after this document is submitted electronically.

6. Pursuant to Local Rule 7.1(a), Defendants have conferred with counsel for the Plaintiff and he has no objection to granting this motion.

WHEREFORE, the defendants respectfully request that Jennifer Stisa Granick be admitted to practice before this Court *pro hac vice* for the purpose of appearing as counsel for defendants in the above referenced proceeding in accordance with the Rules of this Court.

DEFENDANTS ANDERSON, RYAN AND CHIESA

By their attorneys,

Dated: August 13, 2008

/s/ Emily A. Berger

Emily A. Berger, BBO No. 650,841
emily@eff.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

CERTIFICATE OF SERVICE

In accordance with Local Rule 5.2(b), I, Emily Berger, hereby certify that this document filed through the ECF system on August 13, 2008 will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Emily Berger
Emily Berger, Esq.

EXHIBIT A

Supreme Court of California

FREDERICK K. OHLRICH
Clerk of the Court

CERTIFICATE OF THE CLERK OF THE SUPREME COURT

OF THE

STATE OF CALIFORNIA

JENNIFER STISA GRANICK

I, FREDERICK K. OHLRICH, *Clerk of the Supreme Court of the State of California, do hereby certify that* ***JENNIFER STISA GRANICK*** *was on the 14th day of December 1993, duly admitted to practice as an attorney and counselor at law in all the courts of this state; and that her name now appears on the Roll of Attorneys as a member of the bar of this state in good standing.*

Witness my hand and the seal of the court,
this 23d day of MAY, 2008.

FREDERICK K. OHLRICH
Clerk of the Supreme Court

By Joseph Cornetta
Joseph Cornetta, Deputy Clerk

EXHIBIT B

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

AFFIDAVIT OF JENNIFER STISA GRANICK

I, JENNIFER STISA GRANICK, depose and state as follows:

1. I am an attorney licensed to practice law in the State of California, as well as the United States District Court for the District of California.

2. I am a resident of California.

3. I am counsel at the Electronic Frontier Foundation, located at 454 Shotwell Street, San Francisco, CA 94110. The office telephone number is (415) 436-9333 and my direct extension is 134.

4. I am authorized to practice law in the following federal court districts: United States District Court for the Northern District of California and United States District Court for the Central District of California.

5. I was admitted to practice law in the State of California on December 14, 1993. My California Bar Registration number is 168423.

6. I am a member in good standing and duly licensed and admitted to

practice in each of the jurisdictions listed above.

7. I have never been suspended or disbarred in my jurisdiction, and there are no disciplinary actions pending against me in any federal or state court.

8. I am familiar with the Local Rules of the United States District Court for the District of Massachusetts.

9. If the Court allows the Motion for me to appear pro hac vice in this matter, I will represent Defendants in this proceeding until the final determination thereof, and with reference to all matters, incidents, or proceedings, I agree that I shall be subject to the orders and to the disciplinary action and the civil jurisdiction of this Court in all respects as if I were regularly admitted.

Signed under the penalties of perjury on this 13th day of August, 2008.

/s/ Jennifer Stisa Granick

Jennifer Stisa Granick, Esq.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

PLAINTIFF'S REQUEST FOR RULE 16 SCHEDULING CONFERENCE AND INTERIM DISCOVERY ORDER

Introduction

Pursuant to Fed. R. Civ. P. 16(a) and Local Rule 16.1, the plaintiff, Massachusetts Bay Transportation Authority ("MBTA") hereby requests (a) a Scheduling Conference for the limited purposes set out below, and (b) the issuance of an Interim Scheduling Order requiring the defendants to comply with the pending discovery, identified in paragraph 3. The MBTA request that this Conference take place at the close of the Hearings set for 11:00 A.M. on Thursday, August 14, 2008.

As grounds for this Request, the MBTA states as follows:

The Record for the Preliminary Injunction Hearing; Absence of Testimony from the Defendants

1. The Temporary Restraining Order ("TRO") currently in place will expire on Tuesday, August 19. The MBTA currently plans to move this Court to convert the TRO to a Preliminary Injunction on or before Tuesday, August 19.

2. Although the MBTA has provided a range of affidavit testimony in this matter, none of the defendants has yet to provide any such testimony. The MBTA believes that discovery from the defendants, including time-limited deposition discovery, will aid in a ruling on the MBTA's anticipated Preliminary Injunction Motion.

The MBTA's Targeted Discovery Requests

3. On Wednesday, August 13, 2008, the MBTA served the following discovery requests on the defendants:

- A Request for Production containing seven (7) Requests (not including sub-parts). A copy of this Request is included as Exhibit 1.
- A Notice of Deposition of Zack Anderson. This deposition is limited to four (4) hours, on Friday, August 15, from 9:00 to 1:00. A copy of this Notice is attached as Exhibit 2.
- A Notice of Deposition of Professor Ron Rivest. This deposition is limited to two (2) hours, on Friday, August 15, from 2:30 to 4:30. A copy of this Notice is attached as Exhibit 3.

4. The MBTA has provided Initial Disclosures (Exhibit 4). Given the parties' disputes over the MIT Undergrads' refusal even to produce the "A" paper they wrote for Professor Rivest's class (the paper that set in motion the events that led to the current state), more detailed conferences on discovery issues would not be productive, in the MBTA's view.

The Relevance of the Discovery to the Preliminary Injunction Issues

What Threat Is Posed

5. The defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads") through counsel argue that "the information the original TRO sought to keep confidential has now been publicly disclosed by MBTA." Declaration of Jennifer Granick, ¶5. The MIT Undergrads therefore seek to be released from the TRO.

6. Yet the EFF in its Motion papers admits that "more" information is available. *See* Motion at 5 ("most … of the significant facts known to the students … are now public").

7. With its discovery requests, the MBTA seeks to determine what relevant, non-public information exists, and to obtain the "disclosure" element of the "Responsible Disclosure".

8. Indeed, the EFF provided a document to the MBTA on Wednesday August 13, 2008 at 5:52, which the EFF, the MBTA understands, intends to reference during the Thursday August 14 hearing. This document appears to contain a volume of new information concerning MBTA Fare Media security issues.

9. Given the history of delayed and partial disclosure in this matter, the MBTA is entitled to discovery to test and verify the MIT Undergrads' disclosure.

Advocacy of Violations of Law

10. The MIT Undergrads claim that the TRO represents an unlawful prior restraint on their claimed First Amendment rights.

11. The requested discovery, in addition, is targeted toward showing the existence of improper "advocacy of illegal activity", which conduct removes First Amendment protections.

Balancing of Harms

12. The MIT Undergrads did not disclose their Presentation to the MBTA until the morning of the TRO hearing. Yet the Undergrads claim "clean hands," and assert that they "sought to help the MBTA." These arguments are relevant to, among other points, the "balancing of the harms" and "equities" element in a preliminary injunction analysis.

13. The MBTA is entitled to discovery to demonstrate that the MIT Undergrads in fact were not forthcoming about their plans, refused when requested to provide their

Presentation, and otherwise sought to block attempts by the MBTA to determine whether their threatened "get free subway rides for life" was merely a prank, or a significant threat.

Conclusion

Wherefore, the plaintiff, Massachusetts Bay Transportation Authority, respectfully requests (a) a Scheduling Conference after the hearings set for August 14, 2008 at 11:00, and (b) an Interim Scheduling Order requiring the defendants to comply with the pending discovery, identified in paragraph 3.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 13, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 13th day of August, 2008, I served the foregoing **Plaintiff's Request For Rule 16 Scheduling Conference and Interim Discovery Order** by e-mail upon the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Kurt Opsahl, Esquire Email: kurt@eff.org Marcia Hofmann, Esquire Email: marcia@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5542779_v1

EXHIBIT 1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

PLAINTIFF'S REQUEST TO DEFENDANTS ZACK ANDERSON, RJ RYAN, AND ALESSANDRO CHIESA FOR EXPEDITED PRODUCTION OF DOCUMENTS AND THINGS FOR PURPOSES OF PRELIMINARY INJUNCTION HEARING

Introduction

Pursuant to Fed. R. Civ. P. 26 and 34, the plaintiff, Massachusetts Bay Transportation Authority ("MBTA") hereby requests that the defendants Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads") produce for inspection and copying at the offices of Holland & Knight LLP, 10 St. James Avenue, Boston, Massachusetts, all of the documents and things described below which are within the MIT Undergrad's possession, custody or control and to respond in writing to this request on an expedited basis, for purposes of the Preliminary Injunction Hearing, on or before Thursday, August 14, at 5:00 PM eastern.

Definitions

The definitions of Local Rule 26.5 are incorporated in these Requests, with the additional definitions, and modifications, below. Further terms are defined in context:

"And" as well as "or" shall be construed either conjunctively or disjunctively so as to bring within the scope of the request any documents that might otherwise be considered outside the scope of the request.

"Communication" or "communication" shall mean any oral or written transmittal of information or request for information made from one person to another person whether made in person, by telephone, by voicemail, by e-mail, or by any other means; or documents made for the purpose of recording a communication, an idea, statement, opinion or belief.

"Complaint" shall refer to the Complaint filed by MBTA in this lawsuit against the MIT Undergrads, and all allegations therein.

"Concerning" or "concerning" shall mean referring to, describing, evidencing or constituting.

"Correspondence" or "correspondence" shall mean any letter, telegram, telex, e-mail message, voicemail message, notice, memorandum, or other written communication or transcription or notes of a communication.

"DEFCON Conference" means the 2008 DEFCON 16 Conference, held at the Riviera Hotel & Casino in Las Vegas, Nevada, during the period August 8-10, 2008. *See* https://www.defcon.org/

"DEFCON" means the entity organizing and hosting the DEFCON Conference.

"Document" or "document" shall mean the original and each copy that is not identical with the original or that contains any commentary or notation that does not appear on the original of any written, printed, digital, recorded, or graphic matter, including but not limited to correspondence, emails, minutes of meetings, reports, records, lists, memoranda, manuals, schedules, calendars, diaries, voicemails, notes of telephone conversations, notebooks, audio or

video recordings, advertisements, press releases, and/or opinions or reports of consultants, whether stored in tangible, electronic, mechanical or electric form or representation of any kind (including (i) digital materials on or in network storage, laptop or desktop storage, computer tapes, disks, and other memory devices or media, and (ii) backup copies and 'deleted' files on a computer or computer storage device or media), wherever located.

"MBTA" or "plaintiff" shall refer to the plaintiff in this lawsuit, Massachusetts Bay Transportation Authority, and its employees, agents, trustees and representatives.

"MIT Undergrads," "Individual Defendants" or "you" shall mean the individual defendants in this lawsuit, Zack Anderson, RJ Ryan, and Alessandro Chiesa, individually, collectively, and in any combination, as well as their agents, representatives, or anyone acting on their behalf or for their benefit.

"Person" or "person" shall mean any natural person, individual, proprietorship, partnership, corporation, association, organization, trust, or other entity.

"Presentation" means the 87 page set of PowerPoint slides prepared by the MIT Undergrads and entitled "*Anatomy of a Subway Hack*." A copy of the Presentation is attached as Exhibit 7 to the Supplemental Affidavit of Ieuan G. Mahony.

"Report" means the five page document entitled "*Fare Collection Vulnerability Assessment Report: Analysis and Recommendations*," dated as of Friday, August 8, 2008. A copy of the Report is attached as Exhibit 1 to the Declaration of Scott Henderson.

"Tangible things" or "things" is defined to be synonymous in meaning and equal in scope to the usage of this term in Fed. R. Civ. P. 34(a)(1)(B), and shall include but not be limited to (i) objects that embody human compiled or generated information, including computers, laptops, hard drives, storage media, and other devices from which information can be obtained or which,

if necessary, can be translated into reasonably usable forms; (ii) transit system fare media; (iii) equipment to modify, evaluate, copy, or derive information from transit system fare media; and (iv) equipment to modify, evaluate, copy, or derive information from fare media systems employed for public transit purposes.

Document Requests

1. **DEFCON relationship**. Please provide documents that evidence, discuss, or relate to your relationship with DEFCON concerning the DEFCON 16 Conference. Please include in your response:

1.1. Permissions, waivers, and other agreements between the MIT Undergrads and DEFCON concerning submission of the Presentation.

1.2. Written communications (including email) between the MIT Undergrads and DEFCON

1.3. Documents that evidence, discuss, or relate to the date(s) on which the MIT Undergrads submitted the Presentation to DEFCON.

2. **Class Paper**. Please provide documents that evidence, discuss, or relate to the paper the MIT Undergrads submitted for Professor Rivest's class concerning MBTA security system(s) (the "**Class Paper**"). Please include in your response:

2.1. A copy of the Class Paper.

2.2. Drafts, notes, and other materials used or consulted by the MIT Undergrads in connection with the preparation of the Class Paper.

2.3. Copies of any comments, critiques, or evaluations by Professor Rivest (i) of the Class Paper, (ii) of any outlines underlying or summaries of the Class Paper, and (iii) of any of its drafts.

2.4. Copies of any comments, critiques, or evaluations by anyone other than Professor Rivest or an MIT Undergrad (i) of the Class Paper, (ii) of any outlines underlying or summaries of the Class Paper, and (iii) of any of its drafts.

3. **Transit Police and FBI Meeting**. Please provide documents that evidence, discuss, or relate to the face-to-face meeting that included (a) the MIT Undergrads, (b) the MBTA Transit Police, and (c) the FBI (the "**August Law Enforcement Meeting**"). Please include in your response:

3.1. Documents that evidence, discuss, or relate to the date on which August Law Enforcement Meeting took place.

3.2. Copies of any documents provided to the MBTA Transit Police or the FBI by the MIT Undergrads, Professor Rivest, or MIT Counsel at the August Law Enforcement Meeting.

3.3. Notes or transcriptions of any discussions that occurred during the August Law Enforcement Meeting.

3.4. Documents that evidence, discuss, or relate to communications between the MIT Undergrads and the MBTA concerning the August Law Enforcement Meeting, including concerning any discussions that took place during the August Law Enforcement Meeting.

3.5. Copies of any information in written form that the MIT Undergrads had prepared, as of the August Law Enforcement Meeting, to assist or aid the MBTA with respect to correct security vulnerabilities perceived by the MIT Undergrads ("**Assistive Materials**").

3.6. Documents that evidence, discuss, or relate to the date(s) on which the MIT Undergrads (a) began preparation of the Assistive Materials; and (b) provided Assistive Materials to the MBTA.

4. **Fare Media**. Please provide documents and things that constitute, evidence, discuss, or relate to any physical MBTA fare media that the MBTA Undergrads altered, manipulated, or created (collectively, "**Altered MBTA Fare Media**"). Please include in your response:

4.1. All physical MBTA fare media that the MBTA Undergrads altered, manipulated, or created (collectively, "**Altered MBTA Fare Media**"). Include in this response (a) all Altered MBTA Fare Media employed for purposes of the Class Paper; (b) all Altered MBTA Fare Media employed for purposes of the Presentation; and (c) all Altered MBTA Fare Media employed for any other purpose.

4.2. Documents and things that evidence, discuss, or relate to any individuals other than the MIT Undergrads who received Altered MBTA Fare Media created by the MIT Undergrads.

4.3. All physical equipment and software used by the MIT Undergrads in connection with analyzing CharlieTickets and CharlieCards.

4.4. All physical equipment and software used by the MIT Undergrads in connection with analyzing MBTA systems that process, manage, deliver, or otherwise interact with CharlieTickets and CharlieCards.

4.5. All physical equipment and software used by the MIT Undergrads in connection with creating Altered MBTA Fare Media.

4.6. Documents that evidence, discuss, or relate to any use of Altered MBTA Fare Media on MBTA equipment, including use (a) on Fare Gates; and (b) on Fare Vending Machines.

5. **The Presentation**. Please provide documents and things that constitute, evidence, discuss, or relate to the Presentation. Please include in your response:

5.1. Documents that evidence, discuss, or relate to the date(s) on which the MIT Undergrads (a) began preparation of the Presentation; and (b) completed preparation of the Presentation.

5.2. Drafts, notes, and other materials used or consulted by the MIT Undergrads in connection with the preparation of the Presentation.

5.3. Copies of any comments, critiques, or evaluations by anyone other than an MIT Undergrad (i) of the Presentation, (ii) of any outlines underlying or summaries of the Presentation, and (iii) of any of its drafts.

5.4. Provide copies of all software tools, software modules, lines of code, and software applications the MIT Undergrads intended to distribute or demonstrate at DEFCON (collectively, "**DEFCON-related Software Tools**").

5.5. Provide copies of all materials, other than (a) the Presentation, and (b) the DEFCON-related Software Tools, that the MIT Undergrads intended to distribute or demonstrate at DEFCON ("**Additional DEFCON Materials**").

5.6. Documents that evidence, discuss, or relate to any requests by the MBTA for copies of materials that the MIT Undergrads planned to present at DEFCON.

5.7. Documents that evidence, discuss, or relate to any requests by the MBTA for discussions with the MIT Undergrads, after completion of the August Law Enforcement Meeting, concerning DEFCON or perceived security vulnerabilities.

5.8. Documents that evidence, discuss, or relate to the date(s) on which the MIT Undergrads (a) provided the Presentation to the MBTA; (b) provided DEFCON-related Software Tools to the MBTA; and (c) provided Additional DEFCON Materials to the MBTA.

6. **The Report**. Please provide documents and things that constitute, evidence, discuss, or relate to the Report. Please include in your response:

6.1. Documents that evidence, discuss, or relate to the date on which the MIT Undergrads began preparation of the Report.

6.2. Drafts, notes, and other materials used or consulted by the MIT Undergrads in connection with the preparation of the Report.

7. **Responsible Disclosure.** Please provide documents and things that constitute, evidence, discuss, or relate to the MIT Undergrads' their understanding of the concept of "responsible disclosure" (the "**Documented MIT Undergrad-Defined Responsible Disclosure**"). Please include in your response:

7.1. Copies of documents (if any) upon which the MIT Undergrads rely to define or support the Documented MIT Undergrad-Defined Responsible Disclosure.

7.2. Documents that evidence, discuss, or relate to the MIT Undergrads' compliance with Documented MIT Undergrad-Defined Responsible Disclosure.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony_____
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III_____
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 13, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 13th day of August, 2008, I served the foregoing **Request For Production of Documents** by hand delivery and by e-mail upon the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Lowrie, Lando & Anastasi, LLP One Main Street Cambridge, MA 02142 E-mail: emily@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue Boston, Massachusetts 02199 USA Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5530567_v1

EXHIBIT 2

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

NOTICE OF DEPOSITION

NOTICE OF DEPOSITION OF ZACK ANDERSON

To: Emily Berger, Esquire
Lowrie, Lando & Anastasi, LLP
One Main Street
Cambridge, MA 02142

NOTICE OF DEPOSITION

PLEASE TAKE NOTICE that plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), by and through its counsel, will take an abbreviated deposition upon oral examination of the defendant, Zack Anderson ("Anderson"), pursuant to Federal Rule of Civil Procedure Rules 30(b)(6), at the offices of Holland & Knight LLP, 10 St. James Avenue, Boston, Massachusetts, for purposes of the preliminary injunction hearing. The abbreviated deposition will begin on **August 15, 2008** at **9:00 a.m**. and conclude for these limited purposes at 1:00. The deposition will be taken upon oral examination before a notary public or other officer authorized by law to administer oaths.

You are invited to attend and cross-examine.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Dated: August 13, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 13th day of August, 2008, I served the foregoing **Notice of Deposition** by hand delivery and by e-mail upon the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Lowrie, Lando & Anastasi, LLP One Main Street Cambridge, MA 02142 E-mail: emily@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue Boston, Massachusetts 02199 USA Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5526720_v3

EXHIBIT 3

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

NOTICE OF DEPOSITION

NOTICE OF DEPOSITION OF RON RIVEST

To: Emily Berger, Esquire
Lowrie, Lando & Anastasi, LLP
One Main Street
Cambridge, MA 02142

NOTICE OF DEPOSITION

PLEASE TAKE NOTICE that plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), by and through its counsel, will take the abbreviated deposition upon oral examination of the defendant, Professor Ron Rivest ("Rivest"), pursuant to Federal Rule of Civil Procedure Rules 30(b)(6), at the offices of Holland & Knight LLP, 10 St. James Avenue, Boston, Massachusetts for purposes of the preliminary injunction hearing. The abbreviated deposition will begin on **August 15, 2008 at 2:30 p.m**. and conclude for these limited purposes at 4:30. The deposition will be taken upon oral examination before a notary public or other officer authorized by law to administer oaths.

You are invited to attend and cross-examine.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Dated: August 13, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 13th day of August, 2008, I served the foregoing **Notice of Deposition** by hand delivery and by e-mail upon the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Lowrie, Lando & Anastasi, LLP One Main Street Cambridge, MA 02142 E-mail: emily@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue Boston, Massachusetts 02199 USA Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5526720_v3

EXHIBIT 4

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

PLAINTIFF MASSACHUSETTS BAY TRANSPORTATION AUTHORITY'S RULE 26(a)(1) INITIAL DISCLOSURES

Pursuant to Rule 26(a)(1) of the Federal Rules of Civil Procedure, Plaintiff Massachusetts Bay Transportation Authority (the "MBTA") hereby makes the following initial disclosures based upon information it has acquired to date, without yet having had the benefit of formal discovery or production of documents. The MBTA's disclosures are based on the current status of the pleadings. Moreover, the MBTA reserves the right, consistent with its obligation under Rule 26(e) of the Federal Rules of Civil Procedure, to modify, amend, retract, and/or supplement the disclosures made herein as additional evidence and information becomes available.

DISCLOSURES

A. The name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information.

- Zack Anderson, East Campus, 3 Ames St., Hall 2W, Room W210, Cambridge, MA 02142: information concerning the Fare Media System.[1]

- RJ Ryan, East Campus, 3 Ames St. Hall 2W, Room W214, Cambridge, MA 02142: information concerning the Fare Media System.

- Alessandro Chiesa, East Campus, 3 Ames St., Hall 4W, Room 409, Cambridge, MA 02142: information concerning the Fare Media System.[2]

- Massachusetts Institute of Technology ("MIT"), 77 Massachusetts Avenue, Cambridge, MA 02139: information concerning the MIT Undergrads and MIT policies.

- Ron Rivest, 77 Massachusetts Avenue, Cambridge, MA 02139: information concerning the MIT Undergrads.

- Jacob Shaver, Agent for the FBI, (to be supplemented later).

- Massachusetts Bay Transportation Authority, the State Transportation Building, 10 Park Plaza, Boston, MA 02116: information regarding the MBTA.

- Joseph Kelley, Deputy General Manager for Systemwide Modernization for the MBTA, the State Transportation Building, 10 Park Plaza, Boston, MA 02116: information regarding the MBTA.

- Gary Foster, Chief Technology Officer for the MBTA, the State Transportation Building, 10 Park Plaza, Boston, MA 02116: information concerning the MBTA.

- Scott Henderson, Systems Project Manager for the Automated Fare Collection System for the MBTA, the State Transportation Building, 10 Park Plaza, Boston, MA 02116: information concerning the MBTA.

- Richard Sullivan, Sergeant Detective in the Transit Police of the MBTA, the State Transportation Building, 10 Park Plaza, Boston, MA 02116: information regarding fare media and communications with Defendants.

---

[1] The term "Fare Media System" means the system that meets the following two criteria: the system (i) is employed by the MBTA to manage, track, charge for, and collect fares; and (ii) relies on CharilieTicket passes and/or CharlieCard passes.

[2] Zack Anderson, RJ Ryan and Alessandro Chiesa are collectively referred to as the "MIT Undergrads."

- Daniel Terryn, Technical Software Manager of Scheidt & Bachmann: information on the Fare Media System.

B. A copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody or control of the party, and that the disclosing party may use to support its claims and defenses, unless solely for impeachment.

The MBTA identifies the following categories of documents, data compilations, and tangible things in its possession, custody, or control under Fed. R. Civ. P. 26(a)(1)(B), located to date. The documents described below are located at the MBTA's offices in Boston, Massachusetts. Certain of these documents may contain sensitive information, and will be provided pursuant to a protective order.

- Technical documents regarding the MBTA's Fare Media System including related security measures.
- Communications with MIT Undergrads.
- Communications requesting disclosure of presentation.
- Communications with MIT.
- Communications with Professor Rivest.
- Public statements made by Defendants and Defendants' counsel regarding these proceedings.
- Documents concerning the relationship of the parties with the DEFCON conference.
- Documents relating to the MIT Undergrads' class paper.
- Documents concerning the Transit Police and the FBI meeting.
- Documents concerning fare media.
- Documents concerning the presentation.
- Documents concerning the MIT Undergrads' report.
- Documents concerning responsible disclosure.

C. A computation of any category of damages claimed by the disclosing party, making available for inspection and copying as under Rule 34 the documents or other

evidentiary material, not privileged or protected from disclosure, on which such computation is based, including materials bearing on the nature and extent of the injuries suffered.

Because these proceedings have just begun and the parties have not disclosed sufficient documents, the MBTA is currently unable to compute the damage caused by the Defendants. Accordingly, the MBTA reserves the right to supplement its disclosure after receiving sufficient information from the Defendants.

D. For inspection and copying as under Rule 34 any insurance agreement under which any person carrying on an insurance business may be liable to satisfy part or all of a judgment which may be entered in the action or to indemnify or reimburse for payments made to satisfy the judgment.

The Defendants have not raised claims that would implicate potential insurance.

The MBTA's initial disclosures are made without it waiving: (i) the right to object to discovery on the grounds of competency, protection from discovery including the attorney client privilege or work product doctrine, undue burden, relevancy and materiality, or any other proper ground, (ii) the right to object to the use of any such information, for any purpose, in whole or in part, in any subsequent proceeding in this action or any other action; and (iii) the right to object on any and all grounds, at any time, to any discovery request or proceeding involving or relating to the subject matter of this disclosure.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue

Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building, 7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 13, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Counsel for Plaintiff the Massachusetts Bay Transportation Authority, hereby certify that on this 13th day of August, 2008, I served the foregoing document on Plaintiffs' counsel of record, via hand delivery, as follows:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger Lowrie, Lando & Anastasi, LLP One Main Street Boston, MA 617-395-7000 Fax: 617-395-7070 Email: emily@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope Edwards Angell Palmer & Dodge LLP 111 Huntington Avenue Boston, Massachusetts 02199 USA 617-239-0100 Fax: 617-227-4420 Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony
Ieuan G. Mahony

5536574_v1

AO 458 (Rev. 10/95) Appearance

UNITED STATES DISTRICT COURT

DISTRICT OF Massachusetts

APPEARANCE

MBTA v. Anderson, et al

Case Number: 08-11364-GAO

To the Clerk of this court and all parties of record:

Enter my appearance as counsel in this case for

MBTA

I certify that I am admitted to practice in this court.

8/12/09
Date

Signature

Thomas F. S. Darling, III 558848
Print Name Bar Number

MBTA, 10 Park Plaza, Room 7760
Address

Boston MA 02144
City State Zip Code

617.222.3174 617.222.3194
Phone Number Fax Number

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

PLAINTIFF'S OPPOSITION TO CROSS MOTION FOR RECONSIDERATION OF DEFENDANTS ANDERSON, RYAN, AND CHIESA

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 14, 2008

Table of Contents

Introduction 3

Factual Background 3

I. The Information At Issue. 4

A. Three Relevant Categories of Information. 4

B. The Existence of Non-Public Sensitive Materials. 4

C. The Sensitivity of the Three Categories of Information. 5

II. The Points At Which The Individual Defendants Disclosed Pertinent Information to the MBTA. 6

Argument 7

I. The CFAA Prohibits The Defendants' Conduct. 7

A. The Defendants Would Have Knowingly Transmitted Information That The Defendants Knew Would Cause Damage To Protected Computers. 7

B. The Defendants' Construction Of The CFAA Is Illogical. 8

1. The Statute Covers "Chains" Of Actors And Actions, And Is Not Limited To "Solo" Actors As The Individual Defendants' Argue. 8

2. The Term "Transmission" Includes Verbal Transmissions, And Cannot Be Restricted In The Manner The Defendants Claim. 9

II. The TRO Does Not Prevent The Defendants From Engaging In Any Of The Activities They Identify. 10

III. The First Amendment Does Not Protect The Individual Defendants' Activities. 11

A. The Presentation Advocates Violation Of The Law And -- In The Context Of One Largest Hacker Conferences In The World -- Is Directed To, And Likely To Incite Imminent Lawless Action. 11

B. The Presentation And Related Materials Constitute Commercial Speech And, Given Their Advertisement Of Illegal Conduct, Receive No First Amendment Protection. 12

IV. The Individual Defendants' Formulation Of The "Responsible Disclosure" Doctrine Is Illogical. 13

Conclusion 14

Introduction

The plaintiff, Massachusetts Bay Transportation Authority (the "MBTA"), hereby opposes the Cross Motion for Reconsideration of the defendants, Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "Individual Defendants" or the "Defendants"). The Individual Defendants:

(a) Misconstrue the Computer Fraud and Abuse Act (the "CFAA");

(b) Ignore major exceptions to First Amendment jurisprudence;

(c) seek to avoid the fact that their Defcon Presentation (i) expressly promises "you now have free subway rides for life"; (ii) expressly admits "THIS IS VERY ILLEGAL"[1], and (iii) thus represents black-letter "advocacy to violate the law," directed to incite or produce imminent lawless action;

(d) incorrectly assume that the Presentation is "research," where it is at best commercial speech;

(e) overlook the fact that their own arguments demonstrate the propriety of the TRO, as they claim they wished only to discuss publicly available information, and would voluntarily withhold key sensitive information;[2] all conduct permitted by the TRO, and particularly the TRO as modified by the plaintiff's Motion to Modify;

Each of the above points is demonstrated below, and the Cross Motion must accordingly be denied.

Factual Background

The MBTA relies on its earlier papers for relevant facts with respect to this Cross Motion, supplemented as follows with respect to Responsible Disclosure. As argued previously,

[1] *See* Compilation of Previously Submitted Exhibits, Now Submitted In Opposition to Defendants' Cross Motion for Reconsideration ("Compilation Ex.") 16 at 109, 129 (emphasis added; capitalizations in original) (the "Presentation").

[2] As noted below, there is no record support for the MIT Undergrads' claims in this regard, as their EFF counsel has chosen not to submit any affidavits from the MIT Undergrads.

Responsible Disclosure requires (i) a disclosure sufficient to correct flaws; and (ii) a period of time sufficient, with reasonable diligence, to correct.[3]

I. The Information At Issue.

A. Three Relevant Categories of Information.

There are three categories of information and data that are relevant to this matter: (i) public domain materials ("Universal Public Domain Materials"); (ii) materials relevant to the MBTA's AFC System that became public domain in connection with the DEFCON conference ("Recent AFC-Related Public Domain Materials"); and (iii) non-public materials that relate to the AFC system and potential security vulnerabilities ("Non-Public Sensitive Materials").

The category "Recent AFC-Related Public Domain Materials" consists of two elements: (i) a four page Report that the Individual Defendants provided to the MBTA on Friday evening, August 8, the night before the initial TRO hearing was to take place (the "Report")[4] and (ii) an 87 page PowerPoint slide presentation that the Individual Defendants' EFF counsel refused to provide to the MBTA until 4:38 AM on Saturday morning, August 9, hours before the 11:00 AM Court hearing (the "Presentation").[5] Contrary to the Individual Defendants' assertions (unsupported by affidavit testimony), the MBTA after the August 4 meeting made numerous requests for this information

B. The Existence of Non-Public Sensitive Materials.

The Individual Defendants seek to argue that no sensitive information remains to be disclosed, and that the protection afforded to the MBTA by the TRO is unnecessary. For example, the Individual Defendants argue that:

---

[3] *See* Memorandum in Support of Motion for Temporary Restraining Order [3] at iv-vi.

[4] Compilation Ex. 20. *See* Henderson Decl. [10] ¶¶7-12.

[5] Compilation Ex. 16. *See* Mahony Supp. Decl. [9] ¶¶2-13.

> most, if not all, of the significant facts known to the students about the Fare Media System are now public, either because they are contained in the slides prepared for and distributed at DEFCON before the TRO issued, or because the MBTA filed research information provided to it by the students on the public docket in this case.[6]

This claim is inaccurate. First, the Presentation on its face indicates the Individual Defendants' intent to provide additional materials, including software code.[7] In addition, the Individual Defendants' EFF counsel state that the Undergrads received an "A" on the paper they prepared for Professor Rivest, a widely known and respected security and encryption expert. The MBTA's internal expert, Scott Henderson, testified in his Declaration, for example, that the Report appeared incomplete, and was "not original work or an original attack."[8] Indeed, the Individual Defendants state that the Presentation "does not contain the key information about the flaws."[9] It is unlikely that Professor Rivest would award an "A" for the work represented by the Report and the Presentation, indicating that additional sensitive materials exist in the possession of the Individual Defendants. The MBTA notes that the Individual Defendants have been unwilling, to date, to produce the "A" paper they prepared for Professor Rivest.

C. The Sensitivity of the Three Categories of Information.

The sensitivity of the three overall categories of materials is as follows:

---

[6] Cross Motion [26] at 5 (emphasis added).

[7] Compilation Ex. 17 at 105 ("For updated slides and code, see http://web.mit.edu/zacka/www/subway/"); at 142 ("wrote Python libraries for analyzing magcards"); at 171-172 (examples of code); at 191 ("Wrote code to read and clone MIFARE cards (given the key)").

[8] Henderson Decl. [10] ¶¶18-22.

[9] Cross Motion [26] at 5.

Category	Illustrative Materials	Sensitivity
Universal Public Domain Materials	Kostin Nohls, a UVA PhD candidate : information regarding weaknesses in MIFARE card Industry known-magnetic stripe vulnerabilities.	None.
Recent AFC-Related Public Domain Materials	DEFCON Presentation and Report	None/Low
Non-Public Sensitive Materials	Additional information, to be discussed at the hearing	**High**, it appears, pending expert review

II. The Points At Which The Individual Defendants Disclosed Pertinent Information to the MBTA.

The MBTA understands that the Individual Defendants first provided the Presentation to the DEFCON Conference organizers approximately a month before the Conference, or on or about July 5, 2008. Accordingly, when the Individual Defendants met with law enforcement, they knew the Presentation was already "in the pipeline" for the Conference. The timeline for disclosure of the materials can be summarized as follows:

Document	First Discloser	Recipients	Date of first receipt
Presentation	Individual Defendants	DEFCON Administrators	Approx. 7/5/2008
		DEFCON Attendees	Thursday, 8/7/2008
		MBTA	Saturday, 8/9/2008 at 4:38 AM
Report	Individual Defendants	MBTA	Friday, 8/8/2008 at approx. 6:00 PM
	MBTA	Court hearing attendees	Saturday 8/9/2008 at 11:00 AM
		Public (through docket)	Saturday 8/9/2008 at 2:00 PM

As can be seen, the Individual Defendants declined providing the MBTA with promised materials,[10] even after, in the case of the Presentation, the undergrads knew the information was being publicly distributed.[11]

Argument

I. The CFAA Prohibits The Defendants' Conduct.

Courts read a statute in accordance with its plain meaning, and unambiguous statutory language controls. *Tobib v. Radloff*, 501 U.S. 157, 162 (1991); *United States v. Ron Pair Enterprises*, 489 U.S. 235, 241 (1989). Courts, moreover, caution against reading limiting words into broad statutory language. *Tobib, 501 U.S. at 161-62* (refusing to "engraft" a requirement onto a statute's "plain language"); *Maine v. Taylor*, 477 U.S. 131, 135 (1986) (refusing to read a limitation into "the straightforward and unambiguous terms of [a] statute"); *United Union of Roofers, Waterproofers & Allied Workers v. Meese*, 823 F.2d 652, 657 (1st Cir. 1987) (Breyer, J.). The Individual Defendants' interpretation the CFAA violates each of these well settled rules of statutory interpretation.

A. The Defendants Would Have Knowingly Transmitted Information That The Defendants Knew Would Cause Damage To Protected Computers.

The CFAA applies to the Individual Defendants' conduct. Judge Woodlock made detailed inquiry into each of the elements of the CFAA, and nothing has changed factually since the Saturday Hearing. For purposes of the Individual Defendants' challenge, only section (a)(5)(A)(i) is relevant.[12] This section reads in relevant part:

> Whosoever … knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct,

[10] *See* Kelley Decl. [6] ¶¶23-26; Henderson Decl. [10] ¶13-17.

[11] *See* Mahony Supp. Decl. [9] ¶13.

[12] Cross Motion [23] at 9.

> intentionally causes damage without authorization, to a protected computer [violates the statute][13]

The provision thus has two operative events: (i) the defendant knowingly transmits information and (ii) as a result of this conduct, the defendant intentionally – not inadvertently – causes damage to a protected computer. Here, but for the TRO, the Individual Defendants would have transmitted information, in the form of the Presentation and verbal presentation accompanying it, and would have transmitted code, as the Presentation also shows that Individual Defendants planned to provide open source software tools, to enhance attendees' hacking abilities.[14] The plain language of the Presentation demonstrates that the transmission of this information and code was knowing. Moreover, the Presentation's plain language demonstrates that the Individual Defendants' conduct would intentionally – and not inadvertently – cause damage to a protected computer, as evidenced by the Defendants' recognition of the illegal nature of the conduct. The conduct, therefore, falls squarely within the statute.

B. The Defendants' Construction Of The CFAA Is Illogical.

The Individual Defendants' construction of the CFAA leads to anomalous results. Due to time constraints, the MBTA addresses the Defendants' two primary arguments.

1. The Statute Covers "Chains" Of Actors And Actions, And Is Not Limited To "Solo" Actors As The Individual Defendants' Argue.

First, the Defendants argue that a single defendant must both (i) transmit the information, and (ii) him or herself damage the protected computer.[15] The Defendants thus argue that only "solo" actors are covered by the statute. This is incorrect.

---

[13] 18 U.S.C. §1030(a)(5)(A)(i).

[14] Compilation Ex. 16 at 1, 37, 66.

[15] Cross –Motion [23] at 9 ("the offender must both transmit information to the protected computer and cause damage to that same computer.")

Certain varieties of malicious code do not become effective until an unsuspecting user opens an executable file, such as one attached to an email, that then activates the malicious code. In this situation, the individual who physically damages the computer is the unsuspecting user. Under the Individual Defendants' proposed interpretation, the perpetrator of the malicious code in this scenario would be free from exposure, as the perpetrator did not both "transmit" the information and damage the computer. Congress revised and updated the CFAA in part to handle more sophisticated viruses. *Violent Crime and Control and Law Enforcement Act of 1994 - Conference Report*, 103rd Cong. (1994) (Statement of Sen. Leahy). By seeking to limit the CFAA to exclude "chains" of actors and actions, the Individual Defendants' improperly limit the statute.

2. The Term "Transmission" Includes Verbal Transmissions, And Cannot Be Restricted In The Manner The Defendants Claim.

Second, the Individual Defendants claim that the term "transmission" in section (a)(5) cannot be read to include verbal transmissions of information. This is incorrect. First, the plain meaning, dictionary definition of "transmit" is as follows:

> Transmit: 1. to send or cause to go from one person or place to another, esp. across intervening space of distance; transfer; dispatch; convey. … 4. to communicate (news, etc.) … 7. to send out (radio or television broadcasts, etc. by electromagnetic waves…. Webster's New World Dictionary (2d Ed) at 1511 (emphasis added).

The plain meaning of the term, therefore, requires the interpretation employed by Judge Woodlock.

Second, the Defendants own arguments conflict on this point. First, they assert that section (a)(1) includes a term "communicates" and the absence of this term in (a)(5) means verbal transmissions are excluded. Then the Individual Defendants argue that, if "transmissions"

includes verbal transmissions, the CFAA would conflict with the First Amendment.[16] The Defendants thus argue (i) that inclusion of verbal transmissions in the CFAA creates an improper conflict with the First Amendment, yet (ii) at a minimum section (a)(1) includes verbal transmissions. The argument, therefore, is inconsistent.

II. The TRO Does Not Prevent The Defendants From Engaging In Any Of The Activities They Identify.

The Individual Defendants' own arguments demonstrate that the TRO does not prevent them from undertaking any activities they had intended. EFF counsel asserts that:[17]

> [T]he students have repeatedly told the MBTA that the students never intended to disclose key details in the public presentation.[18]

Further, EFF counsel states, in arguing that the Individual Defendants have, and will comply with the EFF's formulation of "Responsible Disclosure":

> Withholding key information about the flaws one discovers while publishing other information, as the students here did, is responsible.[19]

Nothing in the original TRO, or in the TRO with proposed modifications by the MBTA, would prohibit the Individual Defendants from publishing or speaking about their project, provided they withheld this "key information" and "key details." The original TRO reads, in operative part, as follows:

> That the Individual Defendants are hereby enjoined and restrained, in accordance with Fed. R. Civ. P. 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System.

---

[16] Cross-Motion [23] at 11 ("the statue would be in tension with the First Amendment").

[17] As with all statements concerning the MIT Undergrads, no MIT Undergrad testimony is presented in support.

[18] Cross Motion [23] at 6 (emphasis added).

[19] Cross Motion [23] at 5 (emphasis added).

The phrase "assist another in any material way" excludes the provision of public domain materials. Because the materials are already in the public domain, the discloser is not "materially assisting" the recipient. In any event, in its Motion to Modify [16], the MBTA seeks further to ensure that the Individual Defendants are permitted wide scope, provided they withhold the "key information" and "key details." In sum, the TRO language does not prohibit the Individual Defendants from engaging in any conduct they originally planned.

III. The First Amendment Does Not Protect The Individual Defendants' Activities.

A. The Presentation Advocates Violation Of The Law And -- In The Context Of One Largest Hacker Conferences In The World -- Is Directed To, And Likely To Incite Imminent Lawless Action.

First Amendment protection does not extend to speech that advocates a violation of law, where the advocacy "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969). *See also, Stewart v. McCoy*, 537 U.S. 993 (2002) (Justice Stevens' statement accompanying denial of certiorari). The Individual Defendants' conduct falls squarely within this well established zone of no protection.

First, unless restrained, the Individual Defendants would have given their Presentation, and related materials (which have not yet been made available) to one of the world's largest hacker conferences. Advocacy in favor of illegal behavior, in this context, is likely to incite or produce illegal behavior.

Second, the Presentation, and likely the related code and materials, unequivocally constitute advocacy in favor of a violation of law. The Presentation, standing alone, shows this. For example, the Individual Defendants (i) expressly promise "you now have free subway rides

for life";[20] (ii) admit "THIS IS VERY ILLEGAL"[21]; and (iii) recognize the risks of court involvement, stating for example, "what this talk is not: evidence in court (hopefully)."[22]

Moreover, in the Presentation, the Individual Defendants promise attendees that:

> "You'll learn how to generate stored-value fare cards; reverse engineer magstripes; hack RFID cards; use software radio to sniff; use FPGAs to brute force; tap into the fare vending network; social engineer; WARCART![23]

And they further instruct attendees "to execute these attacks we need to interact with the card."[24] As a final example, the Individual Defendants provide a photo of an MBTA network switch, which can only be accessed via a trespass onto MBTA property, and then they visually associate the network switch with "Wireshark," a software application that sniffs and captures data from a network: further illegal activity. In sum, the Individual Defendants are vigorously and energetically advocating illegal activity, and this advocacy, in the context of the DEFCON Conference, is both directed to inciting or producing imminent lawless action, and likely to produce such action. Therefore, the Individual Defendants enjoy no protections under the First Amendment.

B. The Presentation And Related Materials Constitute Commercial Speech And, Given Their Advertisement Of Illegal Conduct, Receive No First Amendment Protection.

It is black-letter law that "[t]he Constitution ... affords a lesser protection to commercial speech than to other constitutionally guaranteed expression." *United States v. Edge Broadcasting Co.*, 509 U.S. 418 (1993). Indeed, no protection extends to commercial speech

[20] *See* Compilation Ex. at 129 (emphasis added).

[21] *See* Compilation Ex. 16 at 109 (emphasis added; capitalizations in original) (the "Presentation").

[22] Compilation Ex. 16 at 107 (emphasis added).

[23] Compilation Ex. 16 at 4.

[24] Compilation Ex. 16 at 47.

that advertises an illegal product or service. *See Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. at 566 (1980).

The Individual Defendants' DEFCON presentation constitutes commercial speech. Commercial speech is any "speech that proposes a commercial transaction." *Board of Trustees of the State University of New York v. Fox*, 492 U.S. 469,482 (1989) (emphasis in original). Here, the Presentation is full of marketing, and self-promotional statements. It is not a research paper. As commercial speech advertising illegal activity, it receives no First Amendment protection.

IV. The Individual Defendants' Formulation Of The "Responsible Disclosure" Doctrine Is Illogical.

The Individual Defendant's proposed definition of "Responsible Disclosure" is illogical, and self contradictory.[25] Examine Statement (1): "disclosure is necessary in order for the scientific community to understand key details of research." Then examine Statement (2): "Responsible Disclosure means withholding the 'key details' so as not to teach others of the flaw." Specifically, the Individual Defendants state:

> The "responsible disclosure" norm is not to withhold all details until the vendor or insecure party has a chance to fix, but to take reasonable steps to avoid inadvertently teaching others how to exploit the flaw. … Withholding key information about the flaws one discovers while publishing other information, as the students here did, is responsible.[26]

Yet Statement (1) and Statement (2) conflict. If a researcher complies with Statement (2), he or she must necessarily contravene Statement (1). In sum, the MBTA's definition of Responsible Disclosure, employed in industry, is the logical, and proper definition, as the Individual Defendants' is poorly thought-out.

---

[25] The Professors and others who assented to the "Letter From Computer Science Professors and Computer Scientists" attached as Exhibit A to the Declaration of Marcia Hofmann, fall to the same illogic.

[26] Cross Motion [23] at 5 (emphasis added).

Conclusion

Wherefore, the plaintiff, Massachusetts Bay Transportation Authority, respectfully requests that this Court (a) deny the Cross Motion for Reconsideration, (b) set a hearing date for converting the TRO to a Preliminary Injunction; and (c) permit the plaintiff to complete the discovery specified in its related Motion.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 14, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

1. I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above- captioned proceedings, hereby certify that on this 14th day of August, 2008, I served the foregoing **Opposition to Defendants' Cross Motion For Reconsideration** by e-mail upon the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Kurt Opsahl, Esquire Email: kurt@eff.org Marcia Hofmann, Esquire Email: marcia@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5542832_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08-11364-GAO

SECOND SUPPLEMENTAL DECLARATION OF IEUAN G. MAHONY

1. I am a partner at Holland & Knight, LLP, representing the Massachusetts Bay Transportation Authority ("MBTA") in this matter. The following further supplements my earlier Declaration in this matter, and is submitted in opposition to the Individual Defendants' Cross Motion for Reconsideration.

2. Attached as Exhibit 1 is a true and accurate copy of an article published in MIT's The Tech: Online Edition entitled "*Students' Subway Security Talk Canceled by Court Order*," by Michael McGraw-Herdeg and Marissa Vogt dated, before updating, August 8, 2008. *See* http://www-tech.mit.edu/V128/N30/subway.html.

3. The Article reads in relevant part:

> Though the presentation itself has been canceled, the presentation slides and confidential vulnerability report the students wrote for the MBTA are now widely available online. Still unavailable is some key information that would complete the attack and let people copy transit cards or add money to their CharlieTickets. It is unclear whether the students had managed to copy or edit the content of the CharlieCard, but their presentation included a detailed discussion of weaknesses in the card's encryption. *Id.* at 2 (emphasis added).

4. The Article further reads in relevant part:

> Phil Zimmerman, the individual who provided the MIT Undergrads with a Declaration immediately prior to the Security expert Phil Zimmerman said that traditionally researchers give at least a month after notification before they disclose a vulnerability in a software system. In hardware systems such as the MBTA's magnetic-stripe and RFID card system, where fixing the vulnerability could possibly take more time, researchers usually offer more time, he said. "If it was me, I would've tried to give them more time to fix it," Zimmerman said. But, he said, "public disclosure is a good thing," because intense public scrutiny can help force people to fix systems. *Id.* at 4 (emphasis added).

5. The Article further reads in relevant part:

> Dan Kaminsky, a security researcher who recently discovered a serious vulnerability in the domain name system underlying the Internet, said that the students' disclosure could have been handled more gracefully. But the MBTA also responded inappropriately, he said, by suing the students instead of just asking for time. *Id.* at 5 (emphasis added).

Signed under the penalties of perjury this 14th day of August, 2008.

Ieuan G. Mahony

5542844_v1

EXHIBIT 1

The Tech Established 1881 ONLINE EDITION

Volume 128 >> Issue 30 : Friday, August 8, 2008 PDF of This Issue

CORRECTION TO THIS ARTICLE:
The Saturday, Aug. 9 Web update "Students' Subway Talk Canceled by Court Order" inaccurately stated that software used to analyze the MBTA's CharlieCard was made available online and was removed after legal action. The software had not been placed online, according to Zackary M. Anderson '09, one of the students whose talk was canceled. (This article has been revised to reflect this correction.)

WEB UPDATE

Students' Subway Security Talk Canceled by Court Order

By Michael McGraw-Herdeg and Marissa Vogt
STAFF REPORTERS
August 8, 2008

Three MIT students will not be presenting their security research at the annual DEF CON hacker convention this weekend because of a temporary restraining order filed by the Massachusetts Bay Transportation Authority on Friday afternoon. The students — legally represented by the Electronic Frontier Foundation, a nonprofit advocacy group — are appealing the order.

Zackary M. Anderson '09, Russell J. Ryan '09, and Alessandro Chiesa '09 planned to present research on Sunday that would have shown how the MBTA's CharlieTicket could be reprogrammed to contain up to $655.36 using a $200 magnetic stripe writer. The students would also have



MARISSA VOGT—THE TECH

(from left) Alessandro Chiesa '09, Russell J. Ryan '09, and Zackary M. Anderson '09 appear at a press conference held by the Electronic Frontier Foundation to discuss their canceled presentation titled "The Anatomy of a Subway Hack." The presentation, which would have been held Sunday at the 2008 DEF CON hacker convention, was pulled because of a temporary restraining order filed by the Massachusetts Bay Transportation Authority.

discussed the CharlieCard. According to a vulnerability assessment written by the students for the MBTA, the CharlieCard can be read wirelessly and also stores information about its balance on the card.

Article Tools

The MBTA's complaint says that they intend to sue the students on several charges. In "Count III: Conversion," the complaint alleges that "the MIT Undergrads exerted dominion over MBTA's property by traveling on the MBTA lines without paying fares." But Anderson said in an e-mail that "we never rode the T for free." Anderson said that

at Saturday's hearing, the MBTA alleged they anticipated a loss of more than $5,000 in fares because of the students' research. EFF attorney Marcia Hofmann said that the EFF would represent the students defending against the subpoena, but that the EFF would rethink its support of the students if the MBTA files further suits. (The EFF has no staff attorneys licensed to practice in Massachusetts.)

The CharlieTicket vulnerabilities were discovered in the spring by a team of four 6.857 (Computer and Network Security) students working on a final project, but the MBTA was not notified. Three of the students are those named in the MBTA's suit. The fourth student, Samuel G. McVeety G, did not participate in the DEF CON presentation preparation, Anderson said, and was not named in the MBTA's complaint. Anderson, Ryan, and Chiesa continued to research the CharlieCard and they submitted their findings to DEF CON.

Though the presentation itself has been canceled, the presentation slides and confidential vulnerability report the students wrote for the MBTA are now widely available online. Still unavailable is some key information that would complete the attack and let people copy transit cards or add money to their CharlieTickets. It is unclear whether the students had managed to copy or edit the content of the CharlieCard, but their presentation included a detailed discussion of weaknesses in the card's encryption.

According to the presentation, the students wrote software to generate and analyze cards like the CharlieCard to crack encryption keys on those cards, and they wrote software to read and duplicate cards like the CharlieCard. That software was to have been put online days ago, but the students did not put it on a Web site advertised in their presentation, Anderson said. Researchers around the world have studied for several years the MIFARE Classic card, used by the CharlieCard, London's Oyster card, and the Dutch public transit system.

For court documents and a copy of the presentation, which was distributed to all DEF CON attendees, see *http://www-tech.mit.edu/V128/N30/subway/*.

Lawsuit surprised students

The lawsuit surprised many DEF CON attendees, who are accustomed to relatively cordial relations with software companies who are informed of security holes. It also surprised the students, who said they had until then gotten positive reactions from the MBTA.

The lawsuit was filed late Friday afternoon, just two days before the presentation. But MBTA officials had been aware of the talk since at least July 30, when a vendor told them about a description of the talk online at defcon.org. The students had also been in contact with the MBTA since July 31 through Ronald L. Rivest, the professor who had overseen their 6.857 project. Rivest could not immediately be reached for comment.

On Monday, Aug. 4, MBTA representatives met with Rivest, the three students, and an MIT staff attorney to discuss the planned presentation. Anderson said that the students met in order to tell MBTA representatives information about the vulnerabilities which they did not intend to disclose publicly. As a result of that meeting, the students wrote a confidential report for the MBTA explaining the vulnerabilities they had discovered. Leaving the Monday meeting, the students felt that the issue had been resolved based on verbal comments and that they would not face legal action, Anderson said.

At around the time that they delivered their five-page vulnerability assessment report on Friday afternoon, the three students learned that the MBTA had filed a complaint in Massachusetts District Court. The students were not provided notice until the MBTA had already sent lawyers to the court to file the complaint, said Kurt Opsahl, a senior staff attorney for the Electronic Frontier Foundation.

The students worked with EFF staff throughout Friday night to prepare a response. "We haven't slept since Thursday," Anderson said Saturday afternoon. EFF attorneys participated in a Saturday morning hearing via teleconference.

On Saturday afternoon, Judge Douglas P. Woodlock issued an order prohibiting the students and "all persons in active concert or participation with any of them" from "providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System." Most of the information about the vulnerabilities were publicized by the MBTA's inclusion of the presentation slides and the vulnerability assessment report in their complaint, available online.

A temporary restraining order is issued when a judge believes a future lawsuit is likely to succeed on its merits, that the restraint will prevent an irreparable harm, that the order will not irreparably harm the restrained party, and that the public interest weighs in favor of the restraint. A detailed explanation of the judge's reasoning was presented orally at the hearing; an audio recording was made by the court but is not yet available.

"The court's order is an illegal prior restraint on legitimate academic research in violation of the First Amendment," Jennifer Granickpeech, an EFF representative, said in a press release issued by the EFF. Nevertheless, the students cancelled their talk on the EFF's advice. "We disagree with the ruling," but they intend to follow it, Opsahl said. Opsahl said that the court's ruling was based on a misinterpretation of the Computer Fraud and Abuse Act.

The complaint lists Anderson, Ryan, and Chiesa as defendants, as well as Rivest, MIT, President Susan J. Hockfield, Chancellor Phillip L. Clay PhD '75, and the MIT Corporation. Opsahl said that only the three students were treated as defendants by the courts. "We can't comment on pending litigation," said Pamela D. Serfes, an MIT News Office representative.

MIT lawyers were helpful but did not represent the students. "We have aligned interests, but they're not representing us," Anderson said.

Representatives of the MBTA were not available for comment.

Responsible disclosure?

The students did not successfully talk with the MBTA about the problems they discovered until July 31, only 10 days before the research was to be proposed. (They tried to contact the MBTA through Rivest about a week earlier, but he did not get in touch until July 31.) Computer security researchers traditionally tell companies about problems they find, give them some time to correct the problems, and only then disclose the vulnerabilities in public, in a process called "responsible disclosure" within the community.

Security expert Phil Zimmerman said that traditionally researchers give at least a month after notification before they disclose a vulnerability in a software system. In hardware systems such as the MBTA's magnetic-stripe and RFID card system, where fixing the vulnerability could possibly take more time, researchers usually offer more time, he said. "If it was me, I would've tried to give them more time to fix it," Zimmerman said. But, he said, "public disclosure is a good thing," because intense public scrutiny can help force people to fix systems.

Should security researchers explore systems which could be critical to security, like public transportation? Well, Zimmerman said, "try not to do anything that involves hiring a criminal defense lawyer."

When an important problem has been discovered with little time until it is publicly announced, Zimmerman said, an organization like the MBTA should fix it immediately. Because lawsuits generally result in security vulnerabilities becoming even more visible, the MBTA should "be thinking a lot about engineering right now and not litigation," in

terms of loss mitigation, he said. If the system is irreparably broken, Zimmerman said, the MBTA might consider switching back to an older form of subway authentication: tokens.

"It's very easy to fix," said Brenno de Winter, a Dutch journalist and security analyst. "In the Netherlands, we've got a system that works. It's called paper," he said.

Dan Kaminsky, a security researcher who recently discovered a serious vulnerability in the domain name system underlying the Internet, said that the students' disclosure could have been handled more gracefully. But the MBTA also responded inappropriately, he said, by suing the students instead of just asking for time.

Many computer software vendors are accustomed to learning of security vulnerabilities from researchers in the responsible disclosure model, Kaminsky said. "You can expect cooperation from software vendors in a way that you could not expect six years ago," Kaminsky said. But the MBTA is not a software company, Kaminsky noted. They may never have before encountered people interested in testing their security for free, a common occurrence outside of the software realm, Kaminsky said. This was an unpredictable "first-contact scenario," he said.

"If your goal is to limit discussion, this [restraining order] is not the way," Kaminsky said. "Suppressing talks in a culture that values freedom of speech just highlights the speech you're trying to suppress."

Patrick Cruce contributed to the reporting of this article.

Copyright 2008 • The Tech

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

Plaintiff

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Defendants

Civil Action No. 08-11364-GAO

PLAINTIFF'S MOTION FOR INTERIM PROTECTIVE ORDER

Pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, Plaintiff Massachusetts Bay Transportation Authority requests that this Court grant Plaintiff's Motion for Interim Protective Order. As grounds for this Interim Protective Order, Plaintiff states that it served to Defendant's counsel discovery requests on August 13, 2008, at 2:36 pm via email. Moreover, any such discovery should take place under the protection of this Interim Protective Order.

Attached to this Motion for Interim Protective Order is the Interim Protective Order that Plaintiff revised to apply only to the Preliminary Injunction discovery, which was done in light of the time that Defendant has to consider the terms of the Protective Order.

To allow discovery to proceed, Plaintiff respectfully requests the Court to allow entry of the Interim Protective Order.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Maximillian J. Bodoin
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

/s/ Thomas F.S. Darling III
Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 14, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above- captioned proceedings, hereby certify that on this 14th day of August, 2008, I served the foregoing **Plaintiff's Motion for Protective Order** by e-mail upon the following interested persons:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Kurt Opsahl, Esquire Email: kurt@eff.org Marcia Hofmann, Esquire Email: marcia@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5542857_v2

EXHIBIT 1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

INTERIM PROTECTIVE ORDER

To apply to discovery in connection with the Preliminary Injunction hearing in this matter, this Court hereby enters this Interim Protective Order. The Parties are free to request revisions to this Interim Protective Order after completion of the Preliminary Injunction discovery period.

1. Definition of "Confidential Information." The term “Confidential Information” means information that is disclosed in discovery or pursuant to disclosure rules that is designated as confidential by any party or non-party to this litigation.

2. Scope. This Interim Protective Order shall apply to all information, documents and things subject to discovery in this action, including without limitation (a) testimony adduced at depositions upon oral examination or upon written questions pursuant to Rules 30 and 31, (b) answers to interrogatories pursuant to Rule 33, (c) documents produced pursuant to Rule 34, (d) information obtained from inspection of premises or things pursuant to Rule 34, and (e) answers to requests for admission pursuant to Rule 36.

3. Limitations on Designating Materials as "Confidential." Only information that is a trade secret or constitutes or contains sensitive non-public business or academic information may be designated as Confidential Information. By way of clarification and not by way of limitation, the following information shall not constitute Confidential Information: (a) information that is in or falls into the public domain (through no fault of the receiving party); (b) information that the receiving party obtains from a third party, who is authorized to disclose such information to the receiving party on a non-confidential basis; (c) information that the receiving party rightfully had in its possession prior to the producing party's disclosure; and (d) information the receiving party independently develops, without reference to the producing party's Confidential Information.

4. Method for Designating. Written information or documents, or any portion thereof, should be designated as Confidential Information by placing on each page a stamp or notice stating “CONFIDENTIAL” in a manner that will not interfere with the legibility of the written information. If information or documents are produced on a computer storage medium such as a CD-ROM, such information or documents should be designated as Confidential Information by placing a stamp or notice stating “CONFIDENTIAL” on the CD-ROM or other storage medium. If any Confidential Information is inadvertently produced without such stamp or notice, the producing party will provide written notice to the receiving party that the information or documents shall be treated as Confidential Information under the Interim Protective Order, and the producing party will promptly thereafter furnish the receiving party with a substitute set of documents bearing the correct stamp or notice and the receiving party will return or destroy the original set.

5. Timing of Designation. With respect to all original documents or things that are made available for inspection, designation by stamping as “CONFIDENTIAL” need not be made

until copies of the materials (or photographs or other facsimiles of things) are requested after inspection and selection by counsel. Making documents or things available for inspection shall not constitute a waiver of any claim of confidentiality, and all materials made available for inspection shall be treated as if designated as "Confidential" at the time of inspection.

6. Application to Depositions. Information disclosed at the deposition of (a) a party, (b) one of its past or present officers, directors, employees, agents, or vendors, or (c) an expert retained by a party, may be designated as Confidential Information by a statement on the record, or within thirty days of the receipt of the transcript of the deposition, that the testimony, or that part of the testimony, is confidential and subject to the provision of this Interim Protective Order.

7. Permitted Recipients. Confidential Information shall be used only for the purposes of this litigation, shall not be used by any recipient for any commercial purpose and shall not be disclosed, given, shown, made available, or communicated in any way to anyone other than:

a. The attorneys of record for each of the parties to this litigation, and their partners, associates, paralegals, secretaries, and employees;

b. The receiving party or parties;

c. Not more than three (3) consulting or testifying experts retained by counsel for the receiving party in this action; provided, however, that no Confidential Information shall be revealed to such experts until the conditions detailed in paragraph 9 have been met;

d. Graphics or design services retained by the parties in connection with this litigation;

e. The Court and its personnel, including clerks and court reports; and

f. The author(s) or prior recipient(s) of the Confidential Information.

8. License Permissions Not Covered. This Interim Protective Order does not hinder or effect the parties' ability to agree that the receiving party shall be entitled to copy, modify, transmit, or otherwise use Confidential Information provided by the producing party.

9. Responsible Disclosure Materials. This Interim Protective Order is intended to cover materials that one party produces to the other, where the receiving party is the one primarily interested in preserving the material's confidentiality, such as with respect to materials the producing party may provide that discusses potential or actual security vulnerabilities in the receiving party's computer systems and other software, systems ("**Responsible Disclosure Materials**"). With respect to Responsible Disclosure Materials, the receiving party shall have the right, within ten (10) days of its receipt of the disclosure (the "**Evaluation Period**"), to designate Responsible Disclosure Materials as "Confidential Information" of the receiving party under this Interim Protective Order, provided such Materials otherwise qualify as Confidential Information. If the receiving party does not designate Responsible Disclosure Materials as "Confidential Information" before expiration of the Evaluation Period, upon written notice to the receiving party (and a 48 hour opportunity in the receiving party to reconsider) the producing party shall not be required to treat Responsible Disclosure Materials as Confidential Information under this Interim Protective Order. Otherwise, the producing party shall treat Responsible Disclosure Materials as Confidential Information, unless an exception under this Interim Protective Order applies.

10. Disclosure to Experts. If any party desires to disclose or make available Confidential Information to any consulting or testifying expert, it must first identify the expert in writing to counsel for each of the other parties, who shall have ten (10) business days from receipt of such notice to object to disclosure to any of the experts so identified. Such identification shall include, at least, the full name and business address and/or affiliation of the proposed expert and a current curriculum vitae of the expert. The parties shall attempt in good faith to resolve any objections informally. If the objections cannot be resolved, the party seeking to disclose the Confidential Information to the expert may move for an Order of the Court allowing the disclosure.

In the event that objections are made and not resolved informally, disclosure of Confidential Information to the expert shall not be made except by Order of the Court.

11. Expert's Agreement to Order. Before Confidential Information may be disclosed to any expert, he or she must read this Interim Protective Order and execute a copy of the Affidavit attached as Exhibit A agreeing to be bound by the terms of this Interim Protective Order. The party disclosing such Confidential Information shall be responsible for retaining the original of the Affidavit signed by the expert to whom such Confidential Information is disclosed.

12. Use in Depositions. Nothing in this Interim Protective Order shall prohibit the use of, or reference to, any Confidential Information in court or in any deposition; provided, however, that the party using or planning to use such information shall take reasonable steps to eliminate or minimize the risk of disclosure to unauthorized persons.

13. Filing Confidential Information in Court. If a party wishes to file Confidential Information with the Court, such filing shall be accomplished in accordance with Local Rule 7.2.

14. Exception. Notwithstanding paragraph 12, upon no less than five (5) days notice to the producing party, Confidential Information identified in accordance herewith may be disclosed in testimony at an evidentiary hearing in this action, or disclosed at a hearing on a motion for preliminary injunction or a motion for summary judgment or other dispositive motion in this action, subject to the rules of evidence and subject to such further order as the Court may enter.

15. No Application to Trial. This Interim Protective Order applies only to the pre-trial phase of this action. Prior to the trial of the action, counsel for the parties shall attempt to reach agreement on the handling of Confidential Information. Counsel for the parties shall submit such agreement (or their respective proposals, if no agreement can be reached) to the Court for consideration.

16. Obligations to Safeguard. The recipient of Confidential Information that is provided under this Order shall maintain such information in a secure and safe area and shall exercise the same standard of due and proper care with respect to the storage, custody, use and/or dissemination (including dissemination to persons identified in paragraph 7) of such information as is exercised by the recipient with respect to its own proprietary information. Each individual who receives Confidential Information pursuant to this Order shall be deemed to have consented to the personal jurisdiction of this Court for the purpose of enforcement of this Order.

17. No Admissions. Nothing contained in the Interim Protective Order shall be construed as an admission by any party that receives documents or other materials designated "Confidential" that such materials are, in fact, Confidential within the meaning of this Interim Protective Order. For good cause, any party may request that the Court revoke, modify, or amend a party's designation of information as Confidential. Such a motion may be filed five days after the moving party serves a written request for modification or revocation to the party that designated the information as confidential. The party that initially made the designation of "Confidential" shall bear the burden of proving that such information is Confidential within the meaning of this Interim Protective Order. All documents and other materials designated as "Confidential" shall be treated by any recipient as such under the terms of this Interim Protective Order unless and until such designation is revoked by the designating party or by the Court pursuant to this paragraph.

18. Disclosure to Other Persons. In the event that a party shall desire to provide access to information, documents or things identified as Confidential hereunder to any person or category of persons not included in paragraph 7 hereof, and if the other party objects thereto, it shall move this Court for an order that such person or category of persons may be given access to the Confidential Information. In the event that the motion is granted, such person or category of

persons may have access to the Confidential Information provided that such person or persons have agreed in writing before such access is given to be bound by the terms of this order, in the form set out in Exhibit A to this Interim Protective Order.

19. No Waiver. Nothing contained in this Interim Protective Order shall be construed as a waiver by any party of its right to object to any discovery request made in this action. The execution of this Interim Protective Order shall not constitute a waiver by any party of any applicable privilege.

20. Attorney-Client Materials. Inadvertent production of attorney-client privileged or attorney work-product information shall not waive the attorney-client privilege or attorney work-product immunity if a request for return of such documents or information is made promptly after a producing party learns of its inadvertent production. This provision is not intended to affect the status of any document previously produced by any party in previous litigation.

21. No Restrictions on a Party's Own Confidential Information. Nothing contained in this Interim Protective Order shall affect the right of the designating party to disclose its own Confidential Information to any person or entity, except with respect to Responsible Disclosure Materials under paragraph 9.

22. Application to Non-Parties. The terms of this Interim Protective Order are applicable to Confidential Information provided by a non-party in connection with this litigation, and such Confidential provided by a non-party shall be protected by the remedies and relief provided by this Interim Protective Order, and subject to its exceptions.

23. Effective Date. This Interim Protective Order shall become effective between the parties upon their execution hereof, and shall govern the exchange of Confidential Information between them prior to entry of this Interim Protective Order as an Order of the Court.

24. Conclusion of Proceedings. Upon final termination of this action, including all appeals, the attorneys for each party shall assemble and return to the opposing party all Confidential documents and Confidential things produced by the opposing party and shall destroy all copies thereof made by the party which the respective parties have in their possession, custody or control. The attorneys for the parties shall be entitled to retain all litigation documents, including exhibits and their own memoranda, containing Confidential Information but such litigation documents and memoranda shall be used only for the purpose of preserving a file on this action, and shall not, without the written permission of the opposing party or an order of this Court, be disclosed to anyone other than those to whom such information was actually disclosed, in accordance with this Stipulation and Order, during the course of this action.

25. Modifications. This Interim Protective Order may be modified by written stipulation of the parties without further Order of the Court; provided that any material modifications, or modifications that alter practice under the Local Rules or Federal Rules, require Court approval.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

_____

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

_____

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA

By their attorneys,

_____

Jennifer Stisa Granick, CA No. 168423
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134

_____

Marcia Hofman, Esq.
ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Ave., Suite 650
Washington, DC 20009

7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

202-797-9009

_____
Kurt Opsahl
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
415-436-9333
Fax: 415-436-9993
Email: kurt@eff.org

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

By its attorneys

_____
Jeffrey Swope
Edwards Angell Palmer & Dodge LLP
111 Huntington Avenue
Boston, Massachusetts 02199 USA
617-239-0100

_____
Emily A. Berger, BBO No. 650841
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
415.436.9333 x 134

August ___, 2008

SO ORDERED:

_____
GEORGE A. O'TOOLE, JR.
UNITED STATES DISTRICT JUDGE

Date:

EXHIBIT A

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

AFFIDAVIT

I, _____, state under the penalties of perjury that I have read the Interim Protective Order entered by the Court in this action, and acknowledge that I am bound and agree to be bound by its terms. I hereby consent to the personal jurisdiction of the above-referenced Court for any proceedings involving the enforcement of that Order.

Signature:_____

Print Name:_____

Date:_____

5536403_v3

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,	)	
Plaintiff,	)	
v.	)	No. 08CV11364 GAO
ACK ANDERSON et al.,	)	
Defendants.	)	

NOTICE OF APPEARANCE OF JOHN REINSTEIN

Please take notice that John Reinstein hereby appears for defendants Zack Anderson, R.J. Ryan and Alessandro Chiessa

/s/ John Reinstein
John Reinstein, BBO 416120
ACLU of Massachusetts
211 Congress Street
Boston, Massachusetts 02110
(617) 482-3170

Dated: August 15, 2008

Certificate of Service

I, John Reinstein, hereby certify that this notice of appearance filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ John Reinstein
John Reinstein

United States District Court
District of Massachusetts

NOTICE
TRANSCRIPT REDACTION POLICY

Effective May 5, 2008, the District of Massachusetts, in accordance with Judicial Conference Policy and the amendments to Rule 5.2 of the FRCvP and Rule 49.1 of the FRCrP, will implement a *Transcript Redaction Policy* regarding official court transcripts.

A copy of the policy is attached to this notice, and may be found on the court's web site at www.mad.uscourts.gov.

Summary of the Policy:

1. Counsel of record are obligated to review the transcript for personal identifying information.

2. Any transcript filed with the clerk of court by a court reporter or transcriber will be available electronically at the office of the clerk of court, for inspection only, for a period of ninety (90) days.

3. During the ninety (90) day period, a copy of the transcript may be obtained from the court reporter or transcriber at the rate established by the Judicial Conference. The transcript will be available electronically at the public terminal at the courthouse and remotely available through PACER to any attorneys of record who have purchased a copy from the court reporter.

4. If personal identifiers are found in the transcript, a "Notice of Intent to Redact" must be filed with the clerk (via CM/ECF) within seven (7) business days of the date the transcript was filed.

5. A "Redaction Request" that includes the specific page and line numbers to be redacted must be filed with the clerk (via CM/ECF) within twenty one (21) calendar days of the date the transcript was filed.

6. The transcript (or redacted transcript) will be made available electronically to the public ninety (90) days after the transcript was filed, without further notice to the parties.

Counsel are urged to share this notice with their clients so that an informed decision about the inclusion of certain materials may be made. Every transcript filed electronically in the Court's CM/ECF database will be accompanied by a notice to counsel regarding their duties under the policy. **The responsibility for redacting personal identifiers rests solely with counsel and the parties.** Neither the clerk nor the court reporter will review transcripts for compliance with this policy.

May 1, 2008

Sarah Allison Thornton
Clerk of Court

United States District Court
District of Massachusetts
Office of the Clerk

TRANSCRIPT REDACTION POLICY - AMENDED MAY 5, 2008

INTRODUCTION

The United States District Court for the District of Massachusetts shall make transcripts of court proceedings, filed on and after May 5, 2008, available through its electronic case files (CM/ECF) system.

The primary purpose of the Transcript Redaction Policy is to provide guidance to the Court's Official Court Reporters and the attorneys of this bar when preparing and reviewing transcripts of official court proceedings to be filed with the Court.

AUTHORITY

At its September 2007 session, the Judicial Conference approved a new policy regarding the availability of transcripts of court proceedings.

In addition, amendments to the Federal Civil and Criminal Rules of Procedure implementing requirements of the E-Government Act of 2002 to protect the privacy and security of publicly available electronic filings took effect on December 1, 2007. The amendments to Rule 5.2 of FRCvP and Rule 49.1 of FRCrP require that personal identification information (social security numbers, names of minor children, financial account numbers, dates of birth, and, in criminal cases, home addresses) be redacted from documents filed with the Court.

POLICY DESCRIPTION

The effective date of this Policy is May 5, 2008.

It applies only to transcripts of proceedings held before a Judicial Officer of this Court, not depositions taken outside of court or proceedings of state courts or other jurisdictions.

It establishes a procedure for counsel to request the redaction from the transcript of specific personal data identifiers before the transcript is made electronically available to the general public.

It does not change any rules or policies with respect to sealing or redaction of court records for any other purpose.

TRANSCRIPT REDACTION POLICY - AMENDED MAY 5, 2008

It does not affect or limit the right of any party (or any other person or entity) to order production of a transcript on an expedited basis. This policy does not affect any court rules or ruling requiring the sealing of materials or the protection of sealed materials.

There is no obligation on the part of the Office of the Clerk to perform any redaction. It is the responsibility of counsel to advise the court reporter what to redact, and the responsibility of the court reporter to perform the redaction.

Redaction responsibilities apply to counsel, even if the requestor of the transcript is a judge or a member of the public or media.

Unless otherwise ordered by the Court, counsel shall review the following portions of the transcript:

- opening and closing statements made on the party's behalf;
- statements of the party;
- the testimony of any witnesses called by the party; and
- any other portion of the transcript as ordered by the Court.

PROCEDURES

Notice of Intent to Redact

Within seven (7) business days of the filing of an official court transcript, each party wishing to redact a transcript shall inform the Court by filing (via CM/ECF) with the Clerk's Office a "Notice of Intent to Redact ." A sample form is available on the Court's website and is attached to this policy.

Redaction Request

If a redaction is requested, unless the Court shall otherwise order, counsel shall file (via CM/ECF) with the Clerk's Office, a "Redaction Request" within twenty one (21) days from the filing of the transcript, indicating where the personal identifiers appear in the transcript by page and line, and how they are to be redacted. A sample form is available on the Court's website and is attached to this policy.

TRANSCRIPT REDACTION POLICY - AMENDED MAY 5, 2008

This procedure is limited to the redaction of the specific personal data identifiers listed below:

- Social security numbers to the last four digits;
- Financial account numbers to the last four digits;
- Dates of birth to the year;
- Names of minor children to the initials; and
- Home addresses to the city and state.

If counsel files a "Notice of Intent to Redact," but later determines that no redaction is necessary, counsel shall file a "Withdrawal of Notice of Intent To Redact."

If counsel fails to timely file a Redaction Request or Motion to Extend Time or a Withdrawal of the Intent to Redact, the Office of the Clerk shall issue an Order to Show Cause requiring the attorney to file the redaction request, a notice of withdrawal of the intent to redact, or show cause why the transcript should not be released to the public after ninety (90) calendar days from the date the original transcript was filed.

Additional Copies of Transcript Purchased

The court reporter shall notify the court reporter supervisor if additional copies of the transcript are purchased by other counsel of record. The court reporter supervisor will provide electronic access for those additional attorneys during the ninety (90) day period.

Redacted Transcript

If a redaction is requested, the court reporter shall file the redacted transcript with the Office of the Clerk within thirty one (31) days after the filing of the original transcript. The title page of the redacted transcript shall indicate that it is a redacted transcript by including "REDACTED TRANSCRIPT" immediately below the case caption and before the volume number and the name and title of the Judge.

TRANSCRIPT REDACTION POLICY - AMENDED MAY 5, 2008

Sealed and Partially Sealed Transcripts

If a transcript is to be filed under seal, the court reporter shall submit that transcript clearly labeled as "SEALED." The court reporter supervisor shall electronically file the PDF document with the appropriate restrictive setting.

If only a portion of a transcript has been ordered sealed, the court reporter shall extract the sealed portions from the original transcript as a separate PDF document (clearly labeled as "SEALED"). The remaining public portion of the transcript shall be created and both PDF documents, clearly labeled, submitted to the court reporter supervisor for electronic filing.

Counsel shall review the remaining public portion of the transcript for any necessary redactions.

Requests for Additional Redactions

Further redactions require the filing of a "Motion for Redaction of Electronic Transcript." Until the Court has ruled on any such motion, the transcript shall not be electronically available, even though the ninety (90) day restriction period may have expired.

Remote Public Access to Transcripts

If the original transcript is filed without redaction, that original transcript shall be remotely electronically available through PACER after ninety (90) calendar days.

If a redacted transcript is filed with the Court, that redacted transcript shall be remotely electronically available through PACER ninety (90) calendar days from the date of filing of the original transcript. The original transcript shall not be made publicly available.

CJA Panel Attorneys

An attorney who is serving as appointed "standby" counsel for a *pro se* litigant must review the transcript as if the *pro se* party were his/her client. If an attorney represents a client pursuant to the Criminal Justice Act (CJA), including serving as standby counsel, the attorney conducting the review of the transcript is entitled to compensation under the CJA for functions reasonably

performed to fulfill that obligation, and for reimbursement of reasonable expenses related to the transcript review.

PACER Fees

PACER fees shall be applied both during and after the ninety (90) day restriction period. Charges shall accrue for all pages of the transcript. The user shall incur PACER charges each time the transcript is accessed even though he/she may have purchased it from the court reporter and obtained remote access through CM/ECF. Unlike other documents filed electronically, there is no 'free look' for transcripts.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

_____
Plaintiff(s)

vs. Docket No. : _____

_____
Defendant(s)

NOTICE OF INTENT TO REQUEST REDACTION

Notice is hereby given that a Redaction Request shall be filed electronically with the Court, via CM/ECF, within 21 days from the filing of the transcript. The transcript for proceedings on _____ was transcribed by _____, Official Court Reporter.

SAMPLE

Submitted by

_____
(Party name)

Through Counsel:

Date: _____ /s/_____
BBO: _____
_____
_____
_____

CERTIFICATE OF SERVICE

I hereby certify that this document(s) filed through the ECF system shall be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies shall be sent to those indicated as non-registered participants on _____.

/s/_____

NOTE: *This Notice should be filed electronically using 'Notice of Intent to Request Redaction' found under the Other Documents menu in CM/ECF. It will be available only to Court staff and case participants.*

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

_____
Plaintiff(s)

vs. Docket No. : _____

_____
Defendant(s)

REDACTION REQUEST

Now comes _____, by counsel and submits this Redaction Request. The transcript for proceedings on _____ was transcribed by _____, Official Court Reporter. The Transcript Redaction Policy requires redaction of the following personal identifiers from the transcripts made electronically available:

- Social security numbers to the last four digits,
- Financial account numbers to the last four digits,
- Dates of birth to the year,
- Names of minor children to the initials, and
- Home addresses to the city and state.

SAMPLE

It is requested that consistent with the Court's Transcript Redaction Policy, the following information be redacted prior to the transcript being made remotely electronically available:

Document # of Transcript (from docket)	**Page**	**Line(s)**	**Identifier (Example: SSN 009-99-9999)**	**Reaction Requested (Example: SSN XXX-XX-1234)**	**Court Reporter**

(Use additional sheets if necessary)

The undersigned understands that redactions other than the personal identifiers listed in the Transcript Redaction Policy require a separate Motion for Additional Redactions be filed within 21 days of the filing of the transcript and requires court approval.

/s/_____
Attorney for _____
Date: _____

NOTE: *This Request should be filed electronically using 'Redaction Request - Transcript' found under the Other Documents menu in CM/ECF. It will be available only to Court staff and case participants.*

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

SUPPLEMENTAL DECLARATION OF RICHARD SULLIVAN

1. I am a Sergeant Detective in the Transit Police of the plaintiff, Massachusetts Bay Transportation Authority ("MBTA"). I am the Transit Police liaison to the Federal Bureau of Investigation (the "FBI"). I make this declaration as a supplement to my first declaration, which I incorporate herein by reference, and to further describe my meeting with the MIT Undergrads that I referenced in my previous declaration.

2. As an initial matter, in preparing for this supplemental declaration I realized that the meeting actually took place on August 4, 2008 and not, as I stated in my first declaration, on August 5, 2008.

3. At the beginning of the meeting I told those in attendance, including the MIT Undergrads and Professor Rivest, that I was there as an agent of the MBTA. I told them that I was there because of claims that were posted on the DEFCON website and to mitigate any harm

to the MBTA. I informed them that I was there to protect the MBTA from economic and other harm.

4. I asked about the presentation that they were planning on giving in Las Vegas. They told me that they were building on information that was already available and that they wanted to take it further. They told me several times during the meeting that they did not hack into the MBTA's computer system while doing research for their presentation and that they did not attempt to defraud the MBTA by making counterfeit cards.

5. The MIT Undergrads assured me that their presentation was on the MIFARE system and the Magstripe system only, and that they would withhold key elements that would allow others to exploit the vulnerabilities that they claimed to have discovered in the MBTA's CharlieCard System.

6. During the meeting, FBI Agent Jacob Shaver explained to them that enabling others to hack into the MBTA's computer system would be the same as if they hacked into the system themselves. The MIT Undergrads reiterated that they did not exploit the supposed vulnerabilities that they had identified in the MBTA's computer system, they promised that they would not do so in the future, and they promised that they would not teach others how to.

7. I asked the students to prepare a written summary of every vulnerability that they claimed to have discovered and how to fix these vulnerabilities. The MIT Undergrads agreed to provide me with such a paper within two weeks. In addition, their professor thought that it was a good idea and confirmed with the MIT Undergrads during the meeting that they would write this summary. I did not request any other documents from the MIT Undergrads, and they did not offer to provide me with any other documents.

8. I told the MIT Undergrads that, based on their statements that they did not hack into the MBTA's computer system, defraud the MBTA, or would teach others how to do so, that they would not be subject to criminal prosecution.

9. On August 6, 2008, both myself and Agent Shafer personally met with Joseph Kelley and others to discuss the meeting that had taken place. I conveyed to all in attendance that we were confident that the students did not violate any state or federal criminal statues. Moreover, I conveyed that we were both comfortable and confident that the students would honor their declaration to us that they would not disclose any information that would enable others to harm the MBTA. After that meeting, I contacted Professor Rivest to let him know that Mr. Kelley may be reaching out to him.

Signed under the penalties of perjury this 15th day of August, 2008.

Richard Sullivan
MBTA Transit Police

5542470_v4

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 15th day of August, 2008, the **Supplemental Declaration of Richard Sullivan** was served via the ECF system on the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org John Reinstein, Esquire Email: reinstein@aclum.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5546413_v1

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	CIVIL ACTION NO. 08-11364-GAO

MOTION FOR AN EXTENSION OF TIME TO RESPOND TO AUGUST 14, 2008 DISCOVERY ORDER

Defendants Anderson, Ryan and Chiesa ("students") hereby move for a short extension of time to respond to the Court's August 14, 2008 order requiring production or responses to particular document requests submitted by the plaintiff no later than 1:00 PT/4:00 ET today, August 15, 2008.

This extension is necessary because the students' lead counsel, Jennifer Granick, has encountered numerous travel-related complications that have delayed her return to San Francisco and rendered her unable to review the response to the document requests underlying the Court's order. Declaration of Kurt Opsahl ("Opsahl Decl.") ¶ 3. Ms. Granick's flight is expected to land in San Francisco at approximately 12:00 PT/3:00 ET this afternoon, and she will be unable to review the response in consultation with her colleagues until late afternoon ET today, after the Court-ordered discovery deadline has passed. Opsahl Decl. ¶ 4.

Counsel for the students have requested opposing counsel's consent to an

extension of the deadline, but opposing counsel has not responded. Opsahl Decl. ¶ 5. To permit Ms. Granick a reasonable opportunity to review the response to the discovery request and confer with her colleagues, we respectfully request that the Court extend the discovery deadline to 4:00 PT/8:00 ET on August 16, 2008.

Respectfully submitted,

/s/ John Reinstein
John Reinstein, BBO #416120
ACLU of Massachusetts
211 Congress Street, 3rd Floor
Boston, MA 02110
Tel: (617) 482-3170
reinstein@aclum.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

Counsel for Defendants Anderson, Ryan and Chiesa

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	CIVIL ACTION NO. 08-11364-GAO

DECLARATION OF KURT OPSAHL IN SUPPORT OF MOTION FOR AN EXTENSION OF TIME TO RESPOND TO AUGUST 14, 2008 DISCOVERY ORDER

1. The Electronic Frontier Foundation ("EFF") represents Defendants Anderson, Ryan and Chiesa (hereafter "students") in this matter. I am a Senior Staff Attorney with the EFF and a member in good standing of the California State Bar. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

2. This declaration is submitted in support of the Motion for an Extension of Time to Respond to the August 14, 2008 Discovery Order.

3. An extension of the deadline imposed by the Court's August 14, 2008 discovery order is necessary because the students' lead counsel, Jennifer Granick, through no fault of her own, has encountered numerous travel-related complications that have delayed her return to San Francisco and rendered her unable to review the response to the document requests underlying the Court's order.

4. Ms. Granick's flight is expected to land in San Francisco at approximately 12:00 PT/3:00 ET this afternoon, and she will be unable to review the response in consultation with her colleagues until late afternoon ET today, after the Court-ordered discovery deadline has passed.

5. I emailed Ieuan Mahony at 12:06 PT/3:06 ET this morning to request his consent to extend the deadline, in response to a message he had sent about 30 minutes before. Mr. Mahony has not responded.

I declare under penalty of perjury of the laws of the State of California that the foregoing is true and correct to the best of my knowledge and belief. Executed August 15, 2008 in San Francisco, California.

/s/ Kurt Opsahl
Kurt Opsahl

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	)	CIVIL ACTION NO. 08-11364-GAO

[PROPOSED] ORDER GRANTING MOTION FOR AN EXTENSION OF TIME TO RESPOND TO AUGUST 14, 2008 DISCOVERY ORDER

After considering the defendants' Motion for an Extension of Time to Respond to August 14, 2008 Discovery Order, the declaration submitted in support of that motion, and the entire record, it is hereby ordered that the motion is GRANTED. The defendants shall produce or respond to the Court's August 14, 2008 Discovery Order no later than 5:00PT/8:00 ET on Saturday, August 16, 2008.

ORDERED this 15th day of August 2008.

_____

UNITED STATES DISTRICT COURT JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	Civil Action No. 08-11364-GAO

DEFENDANTS' MOTION FOR RECONSIDERATION AND/OR MODIFICATION OF AUGUST 14, 2008 DISCOVERY ORDER

INTRODUCTION

Defendants Zack Anderson, Alessandro Chiesa and RJ Ryan ("Defendants" or "the students") respectfully move for this Court to reconsider its August 14 Interim Discovery Order directing Defendants to produce an unpublished student research paper and related unpublished research materials pursuant to Plaintiff's requests for documents numbered 2.1 and 5.4 ("Discovery Order").[1] First and foremost, Plaintiff has failed to state a claim upon which relief can be granted under the Computer Fraud and Abuse Act, *see* Mot. for Reconsideration of TRO at 9-12, and thus any discovery at all is unwarranted and improper. Moreover, the Discovery Order runs directly contrary to the law of this Circuit as set forth in *Cusumano v. Microsoft Corp.*, 162 F.3d 708, 714 (1st Cir.1998), and violates the First Amendment prohibition against pre-publication review. In essence, it unjustifiably allows the Massachusetts Bay Transportation Authority ("MBTA") to use the discovery process to demand and review the students' research, a request they made before Judge Woodlock on August 8, and which he rejected.[2] Justice delayed may sometimes be justice denied, but rushed decisions can also inadvertently deny justice. For the reasons explained in detail below, the students respectfully request that this Court reconsider or modify the order issued on August 14, 2008.

BACKGROUND

As the Court is familiar with the background of this fast-moving dispute, Defendants will address only the most pertinent facts and procedural history here. Defense counsel and the Court were first presented with the discovery requests and Rule

[1] Subject to and without waiving objections not germane to this Motion, the students produced documents responsive to requests 1.1 and 1.2, *i.e.,* communications with the DEFCON organizers. Due to the short time frame for responding to the request, the students were unable to provide materials responsive to request 5.5 in time.

[2] Specifically, the MBTA requested, without providing advanced notice to the students of the hearing, an emergency court order prohibiting the students, *inter alia*, "[f]rom declining to provide the MBTA and its vendors with information sufficient to replicate, test, and repair the purported security flaws in the Fare Media system."

16 motion just minutes before the August 14 hearing. The late filing ensured that defense counsel had no opportunity to review the arguments presented in the papers before the hearing on the motion. Given the shortened time-frame, neither the parties nor the Court had an opportunity to apply the test for production of pre-publication research required by *Cusumano v. Microsoft* and its progeny or address the First Amendment issues raised by the discovery request. As a result, the Discovery Order was based on a manifest error of law that must be corrected.

Currently pending before the Court is a Motion for Reconsideration of a Temporary Restraining Order as well as a Motion to Modify Terms But Not Duration of Temporary Restraining Order (Dkt. No. 16). The hearing on these motions was scheduled for August 14, 2008, and then continued until August 19. On the afternoon of August 13, the Massachusetts Bay Transportation Authority ("MBTA") issued a series of discovery requests—just five days after filing its Complaint on August 8, and prior to any Rule 16 or Rule 26 conference. Less than 24 hours later, just minutes before the August 14, 2008 hearing, Plaintiff's counsel handed the students' counsel a copy of Plaintiff's motion for an "Interim Scheduling Order requiring the defendants to comply with the pending discovery." (Dkt. No. 28.) On August 14, this Court continued the hearing on Defendants' Motion to for Reconsideration and ordered the students to respond to some of the MBTA's discovery requests. Specifically, the Court ordered the students to produce or respond to the discovery requests seeking a research paper, related research materials, and communications with DEFCON conference organizers, initially by 4 pm ET on Friday, August 15, 2008. The Court subsequently extended the response deadline to 7:00 pm ET on August 16.

STANDARD FOR GRANTING A MOTION FOR RECONSIDERATION

A court may grant a motion for reconsideration when the court has misunderstood a party, or there is a significant change in the law or facts since the submission of the issues to the court by the parties. *Reyes Canada v. Rey Hernandez*, 224 F.R.D. 46, 48 (D.P.R. 2004) (citing *Bank of Waunakee v. Rochester Cheese Sales, Inc.*, 906 F.2d 1185, 1191 (7th Cir. 1990)). Under Fed. R. Civ. P. 59(e), a party may direct the district court's attention to newly discovered material evidence or a manifest error of law or fact enabling the court to correct its own errors. *Aybar v. Crispin-Reyes*, 118 F.3d 10, 15 (1st Cir. 1997).

ARGUMENT

A. The Discovery Order Was Based On a Manifest Error of Law Because the Court Failed to Apply the Balancing Test Required by This Circuit.

After failing to get a court order requiring the students to provide information directly, the MBTA is now seeking to use discovery to obtain the research paper that the students submitted to MIT Professor Ronald Rivest regarding MBTA security vulnerabilities (the "Class Paper"), as well as copies of software and other materials relating to the research that the students intended to discuss at DEFCON. The MBTA appears to be motivated by a misguided notion that the law somehow requires that the students show the agency all of their academic research.[4] While the students intended to disseminate a *version* of their research to the public, none of this preliminary material has been published. Declaration of Russell J. Ryan ("Ryan Decl.") ¶¶ 4-5, 7. Thus, the material remains privileged.

The unpublished academic materials sought in MBTA's discovery request are privileged under the law of this Circuit. The First Circuit has established that in the

[4] Whether or not the students should, as good citizens, help the MBTA is not the issue. The students want to help the MBTA. It is undisputed that the students voluntarily met with the MBTA on August 4, and provided an extensive security analysis to the MBTA. (*See* Dkt. No. 32.)

course of conducting the balancing test articulated in Rule 26(b)(2)(c)(iii), the Court must consider whether the materials sought comprise confidential information entitled to special consideration and then must determine "the type and kind of protection" afforded to them. *In re Bextra and Celebrex Mktng. Sales Practices and Prod. Liab. Litig.*, 249 F.R.D. 8, 12 (D.Mass. 2008) (citing *Cusumano v. Microsoft*, 162 F.3d 708, 714 (1st Cir. 1998). Under *Cusumano*, parties may not use the discovery process to obtain pre-publication review of unpublished academic research unless the discovery request can pass a balancing test. First, the party seeking pre-publication information compiled by an academic researcher must first make a *prima facie* showing that its "claim of need and relevance is not frivolous." *Id.* at 716.

Upon such a showing, the burden shifts to the objector to demonstrate the basis for withholding the information. The court then must "place those factors that relate to the movant's need for the information on one pan of the scales and those that reflect the objector's interest in confidentiality and the potential injury to the free flow of information that disclosure portends on the opposite pan." *Id.; see also In re Bextra*, 249 F.R.D. at 15 (publisher need not respond to subpoena seeking communications between publisher and authors of articles concerning peer review of author's studies of the medical drugs at issue in litigation). *Cusumano* and *In re Bextra* involved discovery under Rule 45, but the principles behind the rulings apply equally to the materials sought from the students here in light of the serious First Amendment issues raised by this case.

In *Cusumano*, the court affirmed the denial of a motion to compel responses to a subpoena issued by Microsoft Corporation for notes, tapes, and transcripts of interviews relating to a forthcoming book on then-pending antitrust litigation between Microsoft and the U.S. government. The court noted, *inter alia*, that requiring production of such material could chill the future scholarly research efforts, impairing in turn the free flow of information to the public:

> Courts afford journalists a measure of protection from discovery initiatives in order not to undermine their ability to gather and disseminate information. Journalists are the personification of a free press, and to withhold such protection would invite a "chilling effect on speech," *id.,* and thus destabilize the First Amendment. The same concerns suggest that courts ought to offer similar protection to academicians engaged in scholarly research. After all, scholars too are information gatherers and disseminators.

Cusumano, 162 F.3d at 714 (citation omitted); *see also Summit Tech., Inc. v. Healthcare Capital Group, Inc*., 141 F.R.D. 381 (D. Mass. 1992) (finding that the reports of an investment analyst whose business was to perform independent research and analysis of publicly traded companies for institutional investors were entitled to protection under the reporter's privilege, since they involved the dissemination of investigative information to the public).

In *In re Bextra,* the District Court of Massachusetts held that a third party academic publisher need not produce communications between a publisher and authors of articles concerning drugs at issue in litigation, noting that the disclosure requested, which included peer review comments, "will be harmful to the [journal's] ability to fulfill both its journalistic and scholarly missions, and by extension harmful to the medical and scientific communities, and to the public interest." 249 F.R.D. at 14.

This test should have been applied here. Neither the interviews in *Cusumano* nor the peer review comments in *In re Bextra* were perfectly confidential, but each was sufficiently far along the continuum of confidentiality to justify inquiry into whether the materials should be privileged. As in *Cusumano* and *In re Bextra,* the materials sought here are privileged because the students had an expectation that they would be kept confidential. The students submitted the Class Paper, along with draft code for a single research tool, to Professor Rivest and the Computer and Network Security course staff. Ryan Decl ¶ 2. The students also gave a presentation to their classmates describing their research. *Id*. The Class Paper was also posted online briefly at a private link so it could be easily accessed by a DEFCON conference organizer in connection with the student's

application to present the information in a talk at the conference. Ryan Decl. ¶ 3. The students did not otherwise publish the Class Paper. Ryan Decl. ¶ 4. Nor were the research materials published. Ryan Decl. ¶ 5. The students never decided what research materials, if any, they would include in their final presentation at DEFCON. Ryan Decl. ¶ 6. Their efforts to re-evaluate the materials after the MBTA expressed its concerns delayed the decision-making process and, in light of those concerns and the subsequent filing of this lawsuit, the students ultimately did not finalize any software or demonstration plans for the DEFCON presentation. *Id*. Like the *Cusumano* interviews and the *In re Bextra* comments, here the students expected that their Class Paper, drafted software and demonstration would be confidential or shared only with their professor and course staff. The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, protects student papers from unauthorized disclosure and the students reasonably expected that the Class Paper would not be shared more widely.

As with the documents sought in *In re Bextra* and *Cusumano*, the material is confidential pre-publication material. *Cusumano* withheld discovery of interviews and drafts to prevent a chilling effect on book authors. *In re Bextra* withheld discovery of communications about peer reviews on journal articles to prevent a chilling effect on medical research. This Court should withhold discovery of a class paper that was an unpublished precursor to a proposed talk to prevent a chilling effect on students and other academic researchers who intend to share information at conferences. See *In re Bextra*, 249 F.R.D. at 12.

Further, even where material is not confidential, courts are required to proceed with extreme caution. *Cusumano*, 162 F.3d at 714 (where discovery request seeks only nonconfidential information from researchers, there is "a lurking and subtle threat to journalists and their employers if disclosure of outtakes, notes, and other unused information, even if nonconfidential, becomes routine and casually, if not cavalierly,

compelled.") (quoting *United States v. LaRouche Campaign*, 841 F.2d 1176 (1st Cir. 1988). Thus, this Court must apply the *Cusumano* test before compelling discovery.

MBTA's requests do not pass muster, particularly at this stage in the litigation. The MBTA has not met its burden to demonstrate its need for the material. The pending motion for reconsideration[5] depends on two main questions: whether the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A), a statute targeting unauthorized access to computers, encompasses the communication of information to other individuals; and whether the continued enforcement of a gag order on the dissemination of academic research is a permissible prior restraint in light of the First Amendment and binding Supreme Court precedent. As set forth in Defendants' Motion for Reconsideration of the Temporary Restraining Order (Dkt. No. 23), the answer to both questions is "no."

Further, all this Court can enjoin is what the students are going to say in the future. Thus, the factual issues before the Court must be tethered to the question of what the students will say moving forward. The Court and the MBTA already know exactly what the students want the right to say. Specifically, the students have submitted a detailed confidential "Security Analysis" report detailing everything they would want to the right say about the MBTA's security systems, including details they do not intend to reveal to the public.[6] (Dkt. No. 32.) It is undisputed that DEFCON is over, and the students' presentation was never given. Nor are the students scheduled to give the

[5] The MBTA also asserts that it "currently plans to move this Court to convert the TRO to a Preliminary Injunction on or before Tuesday, August 19." Pl. Request for Rule 16 Scheduling Conference and Interim Discovery Order ¶ 1 (Dkt. No. 28).

[6] It is undisputed that the students have continually asserted that they would leave out key details in any public disclosure. *See, e.g.,* Supplemental Declaration of Richard Sullivan ¶ 5 (Dkt. No. 37); Declaration of Scott Henderson ¶ 11 (Dkt. No. 10). Moreover, the MBTA asserts that the information provided publicly so far is not sensitive. Pl. Opp. to Cross Mot. for Reconsideration 5-6 (Dkt. No. 30).

presentation at any point the future. Whether the student's speech can constitutionally be enjoined requires only the review of the actual proposed speech.[7] (Dkt. No. 32).

The MBTA takes a different view. Citing no law (for there is none), the MBTA has asserted a right to "determine what relevant, nonpublic information exists, and to obtain the 'disclosure' element of the 'Responsible Disclosure.'" Pl. Request for Rule 16 Scheduling Conference and Interim Discovery Order ¶ 7 (Dkt. No. 28). The MBTA also asserts that it "is entitled to discovery to test and verify the MIT Undergrads' disclosure." *Id.* at ¶ 9; *see also* ¶ 13 (questioning whether the students are engaged in a "prank"). These arguments are meritless. No court has ever based an injunction merely on what information *exists*. Indeed, the students do not dispute that a security vulnerability *exists*. If a flaw does not exist, and the MBTA is not in danger of losing fares, this would be a reason *not* to issue an injunction, but it would not help the MBTA's case in any way. *See In re Bextra*, 249 F.R.D. at 14 (denying discovery where, *inter alia,* information sought is of limited probative value). Second, to the extent that the MBTA's purpose really is to test whether vulnerability exists, this is properly the subject of expert testimony reviewing the MBTA's system. *Id.* at 12 (drug company not entitled to coopt the expertise of others in lieu of or in addition to hiring its own experts to attack the plaintiffs theories).

In addition, the MBTA's argument that it is "entitled to discovery to demonstrate that the MIT Undergrads in fact were not forthcoming about their plans" (Dkt. No. 28 at ¶ 13) is meritless. It is based on the unconstitutional notion that the MBTA, a government agency, is legally *entitled* to pre-publication review of the student's "plans." *See Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931) and discussion in Section B below.

[7] Accordingly, the MBTA's argument that it needs the material to show the "existence of improper 'advocacy of illegal activity'" to respond to the students' First Amendment arguments fails. Pl. Request for Rule 16 Scheduling Conference and Interim Discovery Order ¶ 11 (Dkt. No. 28). The Court can decide for itself whether the "Security Analysis" is protected speech, based on the document's actual content.

Furthermore, after this Court ruled on the MBTA's motion, new facts have come to light, showing that the root of this lawsuit appears to be a simple misunderstanding. Much of the MBTA's motion was premised on the argument that the students allegedly promised to provide certain information to the MBTA and did not do so. *See* Pl. Request for Rule 16 Scheduling Conference and Interim Discovery Order ¶¶ 8, 12 (Dkt. No. 28); *see also* MBTA Media Statement (asserting that "[t]he MIT Undergrads … promised … to provide the MBTA with a copy of the Presentation. When no call or information was forthcoming, the MBTA instructed its legal counsel to begin drafting Court papers, *so that the MBTA could obtain this information*.") (emphasis added).[8]

Even if that were a valid basis for these discovery requests (which it is not, see discussion *supra*), the Supplemental Declaration of Richard Sullivan clarifies that that, at the August 4 meeting between the MBTA and the students, he:

> asked the students to prepare a written summary of every vulnerability that they claimed to have discovered and how to fix these vulnerabilities. The MIT Undergrads agreed to provide me with such a paper *within two weeks* [i.e. August 18].

Supp. Sullivan Decl. (Dkt. No. 37) at ¶ 7; *compare* Kelly Decl. (Dkt. No. 6) at ¶¶ 23-24 (discussing a request for further information made to Prof. Rivest) and Henderson Decl. (Dkt. No. 10) (not specifying when or to whom he made a request for the presentation materials). Notably, neither Henderson nor Kelley was at the August 4 meeting. *See* Sullivan Decl. ¶¶ 6-7 (Dkt. No. 4). Accordingly, it appears that a key basis for the discovery request is a misunderstanding of what the student agreed to provide after the August 4 meeting.

Finally, it is undisputed that the MBTA has had the June 30 slides outlining the students' original proposed presentation for more than a week. (Dkt. No. 9-7.) The students never finally decided what research materials, if any, they would demonstrate at

[8] *Available at* http://www-tech.mit.edu/V128/N30/subway/MBTA-press-office-fact-sheet.pdf.

DEFCON, and do not currently intend to demonstrate any such materials. Ryan Decl. ¶¶ 6-8. Thus, the MBTA does not need the requested pre-publication research materials to assess the potential harm of any presentation if the injunction does not issue (assuming that there would be a presentation, which is disputed). And even if the material requested were minimally relevant to the merits of the underlying CFAA claim (assuming the claim was legally cognizable, which it is not), detailed information about the students' research is already available to MBTA. (*See* Dkt. No. 32.)

Even if the MBTA could make a prima facie showing of need, the court must still balance that purported need against the harm of ordering disclosure. That harm is extraordinary here. Researchers, especially students, depend on the ability to share and test ideas with each other and their professors without fear that their initial thoughts and related evidence might be disclosed.[9] *See Healy v. James*, 408 U.S. 169, 180 (1972) ("The college classroom with its surrounding environs is peculiarly the marketplace of ideas" and therefore entitled to vigilant First Amendment protection) (internal quotation marks and citation omitted). The Class Paper was written by the students with the expectation that Professor Rivest and the course staff would be its reviewers. Ryan Decl. ¶ 2.

[9] Indeed, an essential component of academic freedom is the ability to control not just what one publishes, but what one does *not* choose to publish. That is why, for example, the American Association of University Professors has long affirmed that all copyrights in scholarly works must vest in the researchers themselves, rather than their institutional employers. *See* American Association of University Professors, *Statement on Copyright*, available at www.hendrix.edu/WorkArea/linkit. aspx?LinkIdentifier=id&ItemID=14642 (last visited Aug. 15, 2008) ("[copyright ownership included] the powers, for example, to decide where the work is to be published, to edit and otherwise revise it . . . and indeed to censor and forbid dissemination of the work altogether. Such powers, so deeply inconsistent with fundamental principles of academic freedom, cannot rest with the institution."); *see also, e.g., Patent and Copyright Agreement for Stanford Personnel*; *available at* http://www.stanford.edu/dept/DoR/rph/su18.html (last visited Aug. 15, 2008); *see generally* Rochelle Dreyfuss, *The Creative Employee and the Copyright Act of 1976*, 54 U. CHI. L.R. 590, 612-614 (1987).

Imagine how hard it would be for academics to produce class papers or other pre-publication drafts if they believed that the subject of their research later could be subject to compelled disclosure in a lawsuit. Like the peer review system described in *In re Bextra*, the conference review system is essential to the exchange of academic research. Similarly, the pedagogical process depends on a degree of shelter from outside scrutiny. *See Keyeshian v. Board of Regents of Univ. of State of N.Y.*, 385 U.S. 589, 603 (1967) ("Our Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment, which does not tolerate laws that cast a pall of orthodoxy over the classroom."); *Sweezy v. New Hampshire*, 354 U.S. 234, 250 (1957) ("Teachers and students must always remain free to inquire, to study and to evaluate.").

That shelter is particularly important in security research. Security researchers are well aware that the companies that create and use the systems that the researchers study would like nothing more than to get their hands on preliminary research before the researchers themselves have a chance to fully evaluate and assess it. *See generally* Letter from Computer Science Professors and Computer Scientists (Dkt. No. 23-3). A fear that preliminary research could later be demanded in discovery would inevitably chill the free flow of scholarly communication.

While the students understand that the Court was ruling in a very short timeframe, the students must respectfully note that Court plainly erred by failing apply the *Cusumano* test. If it had applied the test, the MBTA's discovery requests would have failed. The Discovery Order should be rescinded on this basis alone. At a minimum, the MBTA must make the showing required by law.

B. The Discovery Order Violates the First Amendment Prohibition Against Prior Restraint, Which Includes a Prohibition on Pre-Publication Review.

More broadly, the Discovery Order amounts to a grant of pre-publication review and, as such, flies in the face of long established free speech principles. Such an order would never be permitted if the content in question were, for example, a reporter's notes, and it should not stand here. Through this discovery process, MBTA has enlisted the court's power to obtain pre-publication review of academic speech by a public authority, and delay publication until its review is complete.

Prepublication review has been long been considered deeply offensive to the First Amendment. Indeed, as explained by the Supreme Court in *Alexander v. United States*, 509 U.S. 544 (1993), the doctrine of prior restraint has its roots in this Nation's aversion to the 16th and 17th century English system of censorship that depended on pre-publication review:

> Under that system, all printing presses and printers were licensed by the government, and nothing could lawfully be published without the prior approval of a government or church censor.

Id. at 553 n. 2 (citation omitted). The common law prior restraint doctrine expressly rejected such a system as offensive to the First Amendment.

In *Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931), the Supreme Court expanded that doctrine to include not only licensing schemes requiring speech to be submitted to an administrative censor for prepublication review, but also injunctions against future speech issued by judges, based in part on a similar aversion to pre-publication review. In that case, the Court held invalid a statute providing for the abatement as a public nuisance of any "malicious, scandalous and defamatory newspaper, magazine or other periodical:

> "[T]he operation and effect of the statute in substance is that public authorities may bring the owner or publisher of a newspaper or periodical before a judge upon a charge of conducting a business of publishing scandalous and defamatory matter and . . . unless the owner or publisher is able . . . to satisfy the judge that the (matter is) true and . . . published with

> good motives . . . his newspaper or periodical is suppressed . . . . This is of the essence of censorship."

Id. at 713. *See also generally Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations*, 413 U.S. 376, 389-390 (1973) ("[T]he protection against prior restraint at common law barred only a system of administrative censorship.... [T]he Court boldly stepped beyond this narrow doctrine in *Near* ").

Thus, prepublication review has been permitted only in the most extraordinary circumstances. For example, a contract requiring such review was held constitutional where the defendant, a former Central Intelligence Agency ("CIA") agent, had voluntarily agreed to limit publications regarding CIA activities. *Snepp v. United States*, 444 U.S. 507 (1980). The Court held that the government had "a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service" and the prepublication review requirement was a reasonable means for protecting that interest. *Id.* at 510. Even in these extraordinary cases, there has never been discovery to determine what the CIA agent *knew* (or court review of the agent's knowledge), just a review of what they proposed to publish.

No such extraordinary circumstance exists here. The MBTA already has ample information about its own security systems, what the students know, what they intended to say at DEFCON, and what they would like to be free to say now if the TRO is lifted. (*See* Dkt. Nos. 32, 37.) The MBTA appears to wish to review everything the students have ever done or thought related to their research in order to pass judgment (in the context of the preliminary injunction proceeding) on anything they might say about it in the future.[10] The First Amendment does not countenance that type of pre-publication review, and neither should this Court.

[10] MBTA has intimated that it will draw adverse inferences if the Class Paper differs from the confidential report, as if these are not different documents for different purposes

Moreover, the Discovery Order effectively expands the scope of the TRO to require pre-publication review already rejected by Judge Woodlock. In its August 8 Motion for TRO, the MBTA sought an order enjoining the students "from declining to provide the MBTA and its vendors with information sufficient to replicate, test, and repair the purported security flaws in the Fare Media system." *See* Compl. at 17, Requested Relief ¶ 3; *see also* Dkt. No. 9-2 (discussing the Aug 8 hearing) Dkt. No. 9-6 (sending a revised proposed order based on Judge Woodlock's Aug. 8 comments, which included removing the language quoted above) and Dkt. No. 12 (the TRO issued on Aug. 9 without the above language). The duty judge's final TRO excluded that mandate, yet provision of "information sufficient to replicate, test, and repair the purported security flaws in the Fare Media system" is exactly what the MBTA seeks now through its document request. *See* Dkt. No. 28, ¶ 9. This Court should decline MBTA's effort to use the discovery process for the improper purpose of obtaining relief that Judge Woodlock already rejected when granting this controversial TRO.[11] *See generally Dorel Juvenile Group, Inc. v. Summer Infant, Inc.*, 2006 WL 2927321 (D.R.I. 2006) (expressing concern that plaintiff was using dispute as pretext to attempt "to obtain confidential and proprietary information"); *see also generally Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 353 n. 17 (1978) ("In deciding whether a request comes within the discovery rules, the court is not required to blind itself to the purpose for which a party seeks information.").

---

and as if the students' thinking or focus should not evolve over the course of their research.

[11] The better course for the MBTA would have been to seek reconsideration of Judge Woodlock's TRO. While the MBTA did seek to modify the TRO (Dkt. No. 16), it did not challenge Judge Woodlock's refusal to grant this portion of the injunctive relief requested.

CONCLUSION

For the foregoing reasons, the students respectfully request that this Court reconsider and modify its August 14, 2008 Discovery Order to exclude production of materials described in 2.1 and 5.4.

August 16, 2008

Respectfully submitted,

*/s/ John Reinstein*_____
John Reinstein, BBO #416120
ACLU of Massachusetts
211 Congress Street, 3rd Floor
Boston, MA 02110
Tel: (617) 482-3170
reinstein@aclum.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

Counsel for Defendants Anderson, Ryan and Chiesa

CERTIFICATE OF SERVICE

I certify that this motion and the attached declaration are being filed through the Court's electronic filing system on August 16, 2008, which serves counsel for other parties who are registered participants as identified on the Notice of Electronic Filing (NEF). Any counsel for other parties who are not registered participants are being served by first class mail on the date of electronic filing.

/s/ Marcia Hofmann
Marcia Hofmann

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

Civil Action No. 08-11364-GAO

DECLARATION OF RUSSELL J. RYAN IN SUPPORT OF MOTION FOR RECONSIDERATION AND/OR MODIFICATION OF DISCOVERY ORDER

I am a student in computer science and electrical engineering at the Massachusetts Institute of Technology. I am a defendant in this matter. I have personal knowledge of the matter stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

1. I have reviewed the Requests for Production issued by the Massachusetts Bay Transportation Authority ("MBTA"). The research materials sought in Requests Nos. 2.1 and 5.4 were created in connection with Computer and Network Security, a class taught by Professor Ronald Rivest at the Massachusetts Institute of Technology.

2. The research materials were shared with Professor Rivest and the Computer and Network Security course staff. Specifically, we submitted the Class Paper to Professor Rivest and the course staff, along with draft code for a single research tool in the appendix of the paper. We also gave a presentation to our classmates describing our research.

3. In addition, the Class Paper was posted online temporarily at a private link provided only to one DEFCON conference organizer.

4. We did not intend to publish the Class Paper.

5. Our research materials were not published.

6. We never decided which research materials, if any, we would include or demonstrate in our final presentation at DEFCON. Our efforts to re-evaluate the materials after the MBTA expressed its concerns delayed the decision-making process. In light of the MBTA's concerns and the subsequent filing of this lawsuit, we ultimately did not finalize any software or demonstration plans for the DEFCON presentation.

7. Our research materials were never presented to the public.

8. We do not currently intend to demonstrate any research materials.

Signed under penalty of perjury this 15th day of August 2008.

Russell J. Ryan

AO 458 (Rev. 10/95) Appearance

UNITED STATES DISTRICT COURT

DISTRICT OF Massachusetts

Massachusetts Bay Transportation Authority

v.

Zack Anderson, RJ Ryan, Alessandro Chiesa, and Massachusetts Institute of Technology

APPEARANCE

Case Number: 08-11364-GAO

To the Clerk of this court and all parties of record:

Enter my appearance as counsel in this case for

Defendants Zack Anderson, RJ Ryan and Alessandro Chiesa

I certify that I am admitted to practice in this court.

8/18/2008
Date

Signature

Adam J. Kessel 661211
Print Name Bar Number

Fish & Richardson P.C., 225 Franklin Street
Address

Boston MA 02110
City State Zip Code

(617) 542-5070 (617) 542-8906
Phone Number Fax Number

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

MOTION FOR ADMISSION *PRO HAC VICE*

Pursuant to Massachusetts Local Rule 83.5.3(b), John Reinstein, Esq., a member in good standing of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, moves for the admission of Cindy Cohn, a member of the Bar of the State of California, to this Court for the purpose of representing defendants in the above-captioned matter, and states as follows:

1. Cindy Cohn is counsel at the Electronic Frontier Foundation. Her business address is 454 Shotwell Street, San Francisco, CA 94110. Her telephone number is (415) 436-9333.

2. Cindy Cohn is a member in good standing of the Bar of the State of California, as evidenced by the Certificate of Good Standing attached hereto as Exhibit A. There are no disciplinary proceedings pending against her as a member of the bar in any jurisdiction. See Affidavit of Cindy Cohn, attached hereto as Exhibit B.

3. Cindy Cohn is familiar with the applicable provisions of the Local Rules

of the United States District Court for the District of Massachusetts.

4. John Reinstein, a member of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, will continue to represent defendants if this motion is granted.

5. Pursuant to Local Rule 7.1(a), Defendants have conferred with counsel for the Plaintiff and he has no objection to granting this motion.

WHEREFORE, the defendants respectfully request that Cindy Cohn be admitted to practice before this Court *pro hac vice* for the purpose of appearing as counsel for defendants in the above referenced proceeding in accordance with the Rules of this Court.

DEFENDANTS ANDERSON, RYAN
AND CHIESA

By their attorneys,

Dated: August 18, 2008

/s/ John Reinstein_

John Reinstein, BBO #416120
reinstein@aclum.org
ACLU of Massachusettes
211 Congress Street, 3rd Floor
Boston, MA 02110
Tel: (617) 482-3170

Cindy Cohn, CA Bar No. 145997
cindy@eff.org
Jennifer Stisa Granick Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

CERTIFICATE OF SERVICE

In accordance with Local Rule 5.2(b), I, John Reinstein, hereby certify that this document filed through the ECF system on August 18, 2008 will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ John Reinstein
John Reinstein, Esq.

EXHIBIT A

Supreme Court of California

FREDERICK K. OHLRICH
Clerk of the Court

CERTIFICATE OF THE CLERK OF THE SUPREME COURT

OF THE

STATE OF CALIFORNIA

CINDY ANN COHN

I, FREDERICK K. OHLRICH, *Clerk of the Supreme Court of the State of California, do hereby certify that* ***CINDY ANN COHN*** *was on the 3d day of May 1990, duly admitted to practice as an attorney and counselor at law in all the courts of this state; and that her name now appears on the Roll of Attorneys as a member of the bar of this state in good standing.*

Witness my hand and the seal of the court,
this 23d day of MAY, 2008.

FREDERICK K. OHLRICH
Clerk of the Supreme Court

By Joseph Cornetta
Joseph Cornetta, Deputy Clerk

EXHIBIT B

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

AFFIDAVIT OF CINDY COHN

I, CINDY COHN, depose and state as follows:

1. I am an attorney licensed to practice law in the State of California, as well as the United States District Court for the District of California.

2. I am a resident of California.

3. I am counsel at the Electronic Frontier Foundation, located at 454 Shotwell Street, San Francisco, CA 94110. The office telephone number is (415) 436-9333 and my direct extension is 108.

4. I am authorized to practice law in the following federal court districts: United States District Court for the Northern District of California and United States District Court for the Central District of California.

5. I was admitted to practice law in the State of California on May 3rd, 1990. My California Bar Registration number is 145997.

6. I am a member in good standing and duly licensed and admitted to

practice in each of the jurisdictions listed above.

7. I have never been suspended or disbarred in my jurisdiction, and there are no disciplinary actions pending against me in any federal or state court.

8. I am familiar with the Local Rules of the United States District Court for the District of Massachusetts.

9. If the Court allows the Motion for me to appear *pro hac vice* in this matter, I will represent Defendants in this proceeding until the final determination thereof, and with reference to all matters, incidents, or proceedings, I agree that I shall be subject to the orders and to the disciplinary action and the civil jurisdiction of this Court in all respects as if I were regularly admitted.

Signed under the penalties of perjury on this 18th day of August, 2008.

/s/ Cindy Cohn

Cindy Cohn, Esq.

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

MOTION FOR ADMISSION *PRO HAC VICE*

Pursuant to Massachusetts Local Rule 83.5.3(b), John Reinstein, Esq., a member in good standing of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, moves for the admission of Marcia Hofmann, a member of the Bar of the State of California, to this Court for the purpose of representing defendants in the above-captioned matter, and states as follows:

1. Marcia Hofmann is counsel at the Electronic Frontier Foundation. Her business address is 454 Shotwell Street, San Francisco, CA 94110. Her telephone number is (415) 436-9333.

2. Marcia Hofmann is a member in good standing of the Bar of the State of California, as evidenced by the Certificate of Good Standing attached hereto as Exhibit A. There are no disciplinary proceedings pending against her as a member of the bar in any jurisdiction. See Affidavit of Marcia Hofmann, attached hereto as Exhibit B.

3. Marcia Hofmann is familiar with the applicable provisions of the Local

Rules of the United States District Court for the District of Massachusetts.

4. John Reinstein, a member of the Bar of the Commonwealth of Massachusetts and the United States District Court for the District of Massachusetts, will continue to represent defendants if this motion is granted.

5. Pursuant to Local Rule 7.1(a), Defendants have conferred with counsel for the Plaintiff and he has no objection to granting this motion.

WHEREFORE, the defendants respectfully request that Marcia Hofmann be admitted to practice before this Court *pro hac vice* for the purpose of appearing as counsel for defendants in the above referenced proceeding in accordance with the Rules of this Court.

DEFENDANTS ANDERSON, RYAN AND CHIESA

By their attorneys,

Dated: August 18, 2008

/s/ John Reinstein

John Reinstein, BBO #416120
reinstein@aclum.org
ACLU of Massachusetts
211 Congress Street, 3rd Floor
Boston, MA 02110
Tel: (617) 482-3170

Cindy Cohn, CA Bar No. 145997
cindy@eff.org
Jennifer Stisa Granick Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

CERTIFICATE OF SERVICE

In accordance with Local Rule 5.2(b), I, John Reinstein, hereby certify that this document filed through the ECF system on August 18, 2008 will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ John Reinstein
John Reinstein, Esq.

EXHIBIT A

Supreme Court of California

FREDERICK K. OHLRICH
Clerk of the Court

CERTIFICATE OF THE CLERK OF THE SUPREME COURT

OF THE

STATE OF CALIFORNIA

MARCIA CLARE HOFMANN

I, FREDERICK K. OHLRICH, *Clerk of the Supreme Court of the State of California, do hereby certify that* ***MARCIA CLARE HOFMANN*** *was on the 8th day of June 2007, duly admitted to practice as an attorney and counselor at law in all the courts of this state; and that her name now appears on the Roll of Attorneys as a member of the bar of this state in good standing.*

Witness my hand and the seal of the court,
this 23d day of MAY, 2008.

FREDERICK K. OHLRICH
Clerk of the Supreme Court

By Joseph Cornetta
Joseph Cornetta, Deputy Clerk

EXHIBIT B

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

Civil Action No. 08-11364-GAO

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY,

Plaintiff,

v.

ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY,

Defendants.

AFFIDAVIT OF MARCIA HOFMANN

I, MARCIA HOFMANN, depose and state as follows:

1. I am an attorney licensed to practice law in the State of California, as well as the United States District Court for the District of California.

2. I am a resident of California.

3. I am counsel at the Electronic Frontier Foundation, located at 454 Shotwell Street, San Francisco, CA 94110. The office telephone number is (415) 436-9333 and my direct extension is 116.

4. I am authorized to practice law in the following federal court districts: United States District Court for the Northern District of California and United States District Court for the Central District of California.

5. I was admitted to practice law in the State of California on June 8th, 2007. My California Bar Registration number is 250087.

6. I am a member in good standing and duly licensed and admitted to

practice in each of the jurisdictions listed above.

7. I have never been suspended or disbarred in my jurisdiction, and there are no disciplinary actions pending against me in any federal or state court.

8. I am familiar with the Local Rules of the United States District Court for the District of Massachusetts.

9. If the Court allows the Motion for me to appear *pro hac vice* in this matter, I will represent Defendants in this proceeding until the final determination thereof, and with reference to all matters, incidents, or proceedings, I agree that I shall be subject to the orders and to the disciplinary action and the civil jurisdiction of this Court in all respects as if I were regularly admitted.

Signed under the penalties of perjury on this 18th day of August, 2008.

/s/ Marcia Hofmann

Marcia Hofmann, Esq.

✎AO 458 (Rev. 10/95) Appearance

UNITED STATES DISTRICT COURT

DISTRICT OF Massachusetts

Massachusetts Bay Transportation Authority

v.

Zack Anderson, RJ Ryan, Alessandro Chiesa, and Massachusetts Institute of Technology

APPEARANCE

Case Number: 08-11364-GAO

To the Clerk of this court and all parties of record:

Enter my appearance as counsel in this case for

Defendant Zack Anderson, RJ Ryan and Alessandro Chiesa

I certify that I am admitted to practice in this court.

8/18/2008
Date

/s/ Thomas A. Brown
Signature

Thomas A. Brown 657715
Print Name Bar Number

Fish & Richardson P.C., 225 Franklin Street
Address

Boston MA 02110
City State Zip Code

(617) 542-5070 (617) 542-8906
Phone Number Fax Number

AO 458 (Rev. 10/95) Appearance

UNITED STATES DISTRICT COURT

DISTRICT OF Massachusetts

Massachusetts Bay Transportation Authority

v.

Zack Anderson, RJ Ryan, Alessandro Chiesa, and Massachusetts Institute of Technology

APPEARANCE

Case Number: 08-11364-GAO

To the Clerk of this court and all parties of record:

Enter my appearance as counsel in this case for

Defendant Zack Anderson, RJ Ryan and Alessandro Chiesa

I certify that I am admitted to practice in this court.

8/18/2008
Date

Signature

Lawrence K. Kolodney 556851
Print Name Bar Number

Fish & Richardson P.C., 225 Franklin Street
Address

Boston, MA 02110
City State Zip Code

(617) 542-5070 (617) 542-8906
Phone Number Fax Number

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

MOTION FOR THREE HOUR EXTENSION OF TIME

Pursuant to Fed. R. Civ. P. 6(b), Plaintiff, Massachusetts Bay Transportation Authority (the "MBTA"), moves to enlarge the time for it to file its Motion for Entry of Preliminary Injunction, supporting Memorandum, Supplemental Declarations and other supporting materials. The current deadline is Monday, August 18, 2008 at 5:00 PM EST and Plaintiff requests an extension until Monday, August 18, 2008 at 8:00 PM EST. As grounds for this motion, Plaintiff states as follows:

1. Given the nature and complexity of the underlying action, the MBTA required additional time to collect materials in support of its Motion for Entry of Preliminary Injunction. The MBTA wishes to provide this Court with a sufficient record for making a decision concerning the Motion for Entry of a Preliminary injunction;

2. Counsel for MIT Students produced documents Saturday night that required careful study, thereby requiring additional time; and

3. Counsel for MIT consents to Plaintiff's Motion for Three Hour Extension of Time, but counsel for the MIT Students does not consent.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
By its attorneys,

/s/ Ieuan G. Mahony
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building, 7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 18, 2008

Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 18th day of August, 2008, the **Motion for Three Hour Extension of Time** was served via the ECF system on the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org John Reinstein, Esquire Email: reinstein@aclum.org
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony

5550067_v1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	Civil Action No. 08-11364-GAO

REPLY TO OPPOSITION TO
MOTION FOR RECONSIDERATION OF TEMPORARY RESTRAINING ORDER

On Tuesday, August 19, 2008, this Court will be asked to decide whether to allow the Temporary Restraining Order ("TRO") in this matter to lapse, or to convert it into a preliminary injunction. This Court should allow the TRO to lapse. The Massachusetts Bay Transportation Authority ("MBTA") has failed to state a claim upon which any relief can be granted. The MBTA has failed to identify how the MIT Students' speech could itself be illegal in any way. The MBTA has failed to meet the standard for a preliminary injunction, never mind a prior restraint on speech. Finally, any preliminary injunction enjoining the MIT Students from engaging in core political speech about a quasi-governmental agency's conduct in a matter of significant public interest is unconstitutional.

The MBTA's Opposition to the MIT Students' Motion for Reconsideration of the Temporary Restraining Order ("MBTA Opp.") errs on two crucial points of law upon which this Motion (and indeed, this entire case) can be decided without the need to resolve any factual issues. Contrary to the MBTA's view:

(1) The Computer Fraud and Abuse Act ("CFAA") does not regulate pure speech. On its face, it prohibits the act of accessing without authorization and causing damage to protected computers. It also prohibits the transmission of viruses, worms and the like with the intent to cause damage to a protected computer. The statute does not prohibit ***talking*** about such intrusions, and the MBTA has failed to explain how the MIT Students could violate the law merely by speaking about the security flaws they discovered. The MBTA has not cited a single case that supports its attempt to apply the CFAA to speech. Nor are we aware of any such cases. For this reason alone, the MBTA has failed to state a claim upon which relief can be granted, and thus both the TRO and the Complaint should be dismissed.

(2) Prior restraints on speech are nearly always unconstitutional. Even where the threatened disclosure implicated national security, the Supreme Court held a prior restraint unconstitutional, *see New York Times Co. v. United States*, 403 U.S. 713 (1971). The prohibition on prior restraint is so strong that the First Circuit has vacated a district court's contempt sanction against a party who willfully violated a temporary restraining order, finding that unlawful prior restraints fell within the narrow range of exceptions to the "collateral bar" rule which ordinarily prohibits the violation of a wrongly-issued court order. *In re Providence Journal Co.*, 820 F.2d 1342, 1344 (1st Cir. 1986). As discussed below, the MBTA's allegations do not even meet the ***general*** standard for injunctive relief, much less the extraordinary standard of imposing a prior restraint on speech.

The Court need go no further than either of these two points to grant the MIT Students' Motion, dissolve the TRO, and refuse to issue a preliminary injunction.

ADDITIONAL FACTS

While the pleadings of the parties to date address most of the factual background, we submit a brief discussion of new developments since the Thursday hearing below.

On Friday, August 15, the MBTA filed without comment a Supplemental Declaration of MBTA Transit Police Office Richard Sullivan. (Docket #37 ("Supp. Sullivan Decl.").) This declaration undermines the MBTA's basic factual allegations. The MBTA's rush to the

courthouse was premised on its claim that the students refused repeated requests by the MBTA to provide them with additional information prior to the DEFCON presentation and that based on these failures, and the DEFCON presentation materials, they felt certain that the students were intending to teach others how to avoid paying subway fares. (*See e.g.* Temporary Restraining Order Request at ii; MBTA Opp. at 6-7.)[1]

The Supplemental Sullivan Declaration belies these assertions. Mr. Sullivan was the only MBTA representative to have spoken with the students prior to the MBTA's seeking of the TRO, and prior to doing so he had reviewed the DEFCON materials that promoted the MIT Students' presentation. Mr. Sullivan refutes the MBTA's claim that it asked the students for their slides and other materials. He says that all he asked of the students was that they prepare a "summary" of their work within *two weeks*, making it due on August 18, 2008. He continues: "I did not request any other documents from the MIT Undergrads, and they did not offer to provide any other documents." (Supp. Sullivan Decl. ¶ 7.)

Moreover, contrary to the MBTA's representations to the Court, Mr. Sullivan states that, well after he and FBI Agent Jacob Shaver both read the Announcement (Complaint ¶ 34) and met with the MIT Students, they told MBTA General Manager for Systemwide Modernization Joseph Kelley that "we were both comfortable and confident that the students would honor their declaration to us that they would not disclose any information that would enable others to harm the MBTA." (*Id.* ¶ 9.)

Strangely, Mr. Kelley does not mention Mr. Sullivan's August 6th report to him in his August 8th declaration. More importantly, Mr. Kelley's declaration admits that he never communicated with the students directly; instead he states that he asked Professor Rivest to ask them for their slides and report. There is no indication that this request, if it was made, was ever conveyed to the students as Mr. Kelley seems to suggest.

[1] In its Opposition, the MBTA even provides a chart, purportedly demonstrating how the students refused to provide them with promised information. *Id.* at 6.

Given this new information, which the MBTA must have known at the time it filed the first declaration from Mr. Sullivan omitting this exculpatory language and the declaration of Mr. Kelley, it is difficult to imagine how the MBTA could have brought this action, and sought an emergency gag order, in good faith, two days after receiving Mr. Sullivan and Special Agent Shaver's report. Indeed, in filing Mr. Sullivan's declaration, the MBTA made no attempt to explain why the information was not included in Mr. Sullivan's first declaration, or in Mr. Kelley's declaration, or indeed what changed between the time Mr. Sullivan made his assessment on Monday and the time the MBTA decided to file suit and seek emergency relief on Friday without any further communication with the students. On this new factual basis alone, the TRO should be dissolved and no injunction should issue.

The MBTA has also repeatedly complained that the MIT Students have yet to submit an affidavit in this case. (*See e.g.*, MBTA Opp. at 3 fn. 2 and 4.) No affidavits are needed to decide any relevant issue, since the MBTA's claim fails on its face, even accepting all allegations in its Complaint as true. However, this Court has indicated that further exposition of the facts would assist in its resolution of the legal issues that are the basis for deciding the validity of any restraining order. For that purpose, we have provided additional details in the Declaration of Zack Anderson ("Anderson Decl.") submitted as Exhibit 1 in support of this motion, and we identify the MBTA's misstatements and inaccuracies here.

Anderson, Ryan, and Chiesa take their academic studies at MIT seriously. (Anderson Decl. ¶¶ 3-7.) They have also acted responsibly with regard to the vulnerabilities they identified in the MBTA CharlieTicket and CharlieCard system. (*Id*. ¶ 10.) The students initiated contact with the MBTA through their professor Ronald Rivest. (*Id*. ¶¶ 15-16.) The students always planned to limit the information they would publicly convey about their findings so as to avoid inadvertently teaching others how to modify or counterfeit cards or tickets. (*Id*. ¶ 20.) The students voluntarily met with the MBTA and with the FBI. (*Id*. ¶ 17.) The students agreed to provide and timely provided a confidential vulnerability report to assist the MBTA in identifying

and repairing vulnerabilities in its system. (*Id*. ¶¶ 18, 22.) The students voluntarily provided a longer and more comprehensive security report, filed under seal in this matter at Docket #32.

ARGUMENT

As stated above and in the MIT Students' Motion for Reconsideration of the Temporary Restraining Order, the TRO should be vacated because (1) the MBTA has no cause of action and any future speech by the MIT Students about fare card vulnerabilities is legal and (2) the TRO is an unconstitutional prior restraint on speech involving the conduct of a quasi-governmental agency in a matter of great public interest. Such speech is entitled to the highest level of protection under the First Amendment.

The MBTA's Opposition to this Motion offers several responses to the MIT Students' arguments, all without merit. As an initial matter, the Order must be dissolved because the MBTA has failed to show that any future violation of law is imminent, as required by controlling case law. To the contrary, the Supplemental Sullivan Declaration indicates that the MBTA had no reason to believe that any violation of law by the MIT Students was *ever* imminent. Moreover, the MBTA's interpretation of the CFAA as controlling speech rather than damaging conduct is contrary to the plain text of the statute and unsupported by any case law. The MBTA's self-serving definition of "responsible disclosure" amounts to nothing more than a bald and unsupported assertion controverted by the description of the issue offered by eleven preeminent computer scientists and security researchers. In any event, to the extent that some computer security professionals might agree with the MBTA, the term "responsible disclosure" carries no legal weight. Finally, the MBTA wrongly characterizes the MIT Students' accused speech as "commercial." Encouraging other researchers to attend even a self-promotional talk is not "commercial" speech, which is defined as speech that merely proposes an economic commercial transaction.

I. The Temporary Restraining Order Must Be Dissolved Because the MBTA Has Not Shown Any Violation of Law Is "Imminent."

The MBTA speculates that but for the Temporary Restraining Order, the MIT Students "***would have*** knowingly transmitted information that defendants knew ***would cause*** damage to protected computers." (MBTA Opp. at 7) (emphasis added). This assertion appears to be directly contrary to the only relevant record evidence. Specifically, the evaluation of the only MBTA official to actually meet with the students, Mr. Sullivan, does not support the MBTA's view. (Sullivan Decl. ¶ 9.)

Moreover, the MBTA's unfounded assertion is irrelevant to the continued validity of the Order.[2] Injunctions are valid only if harm is "imminent" and there is a danger of "recurrent violation." *United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953) ("An injunction issues only if there is some showing that defendant has violated, or imminently will violate, some provision of statutory or common law"); *accord Hibernia Sav. Bank v. Ballarino*, 891 F.2d 370 (1st Cir. 1989) (affirming denial of injunctive relief where no danger of recurrent violation was shown).[3] Under First Circuit law, a plaintiff seeking an injunction must demonstrate

> the likelihood of substantial and immediate irreparable injury, and the inadequacy of remedies at law. . . . It is not enough for a plaintiff to assert that she 'could be' subjected in the future to the effects of an unlawful policy or illegal conduct by a defendant-the prospect of harm must have an 'immediacy and reality.'

Steir v. Girl Scouts of the USA, 383 F.3d 7, 16 (1st Cir. 2004) (citations omitted). The Third Circuit has echoed this point, emphasizing that "more than a risk of irreparable harm must be demonstrated. The requisite for injunctive relief has been characterized as a 'clear showing of

---

[2] Nor do these allegations state a valid claim. The MBTA must allege an actual violation of the CFAA. It has no right of civil action for either an attempted violation, or for aiding an abetting another in violating the law. 18 U.S.C. § 1030(g). Of course, the MIT Students neither attempted to violate the CFAA nor attempted to aid and abet another to do so.

[3] *W.T. Grant Co.* and *Hibernia Sav. Bank* discuss the standard for injunctive relief generally. They do not apply the even higher standard for injunctive relief that constitutes a prior restraint on speech. As shown here, the MBTA has not even met the general standard for injunctive relief, much less the heightened showing needed to enjoin speech.

immediate irreparable injury.'" *Ammond v. McGahn*, 532 F.2d 325, 329 (3d Cir. 1976) (internal citations omitted). The MBTA must meet a high standard for demonstrating the likelihood of ***future*** harm to justify a continued injunction.[4] The MBTA must show "there exists some cognizable danger of recurrent violation, something more than a mere possibility which serves to keep the case alive." *W.T. Grant,* 345 U.S. at 633. "The purpose of an injunction is to prevent future violations." *Id.*

Thus, the MBTA's reliance on what "would have" or "might have" happened at the DEFCON conference is irrelevant to whether an injunction should issue. The conference is over, and the MIT Students have no plans or intentions to give a similar presentation in the future. Ryan Declaration in Support of Motion for Reconsideration of Discovery Order ¶ 8; Attached Anderson Decl. attached as Exhibit 1 ¶ 30.

Although the MBTA might claim that despite the assessment of its own official and the FBI it remains fearful about what might have happened or what could have happened at the DEFCON conference, such fear does not support the continuation of an injunction, particularly since the MIT Students have now repeatedly demonstrated their willingness to support the MBTA in improving its security system. (*Id*. ¶ 24.) As the Third Circuit has emphasized, "[i]njunctions will not be issued merely to allay the fears and apprehensions or to soothe the anxieties of the parties. Nor will an injunction be issued 'to restrain one from doing what he is not attempting and does not intend to do.'" *Continental Group, Inc. v. Amoco Chemicals Corp.*, 614 F.2d 351 (3rd Cir. 1980). [5] The standard is even higher when the injunction sought restricts

[4] There has been no ***past*** violation—the MIT Students gave no presentation at the DEFCON conference.

[5] The MBTA improperly turns the test for injunctive relief on its head. The MBTA suggests continued application of the Temporary Restraining Order will cause no harm to the students, because "the TRO language does not prohibit the Individual Defendants from engaging in any conduct they originally planned." (MBTA Opp. at 10-11.) The MBTA gets the law backwards. Because the MIT Students have no intention of disclosing key information, the MBTA does not even have a colorable basis for an injunction.

speech. *See Lawson v. Murray*, 515 U.S. 1110, 1114 (1995) ("Precedent shows that a speech-restricting 'injunction' that is not issued as a remedy for an ***adjudicated or impending violation of law*** is also a prior restraint in the condemnatory sense, that is, a prior restraint of the sort prohibited by the First Amendment") (emphasis added).

The situation here is analogous to *Continental Group.* In that case, a former employee of the plaintiff testified that he did *not* intend to disclose damaging information, but the district court nonetheless entered an injunction after attempting to "ascertain the possibility of irreparable harm … from the risk of inadvertent disclosure." *Continental Group*, 614 F.2d at 358. The appeals court reversed, holding that the "risk of harm if information is inadvertently disclosed is not sufficient to satisfy the standards for granting a preliminary injunction." *Id.*

In this case, the MIT Students have repeatedly stated that they did not intend to disclose at the DEFCON conference critical information necessary to compromise the MBTA Fare Cards, nor do they intend to do so in the future. Supp. Sullivan Decl. ¶ 5 (the MIT Students "would withhold key elements that would allow others to exploit the vulnerabilities"); Declaration of Scott Henderson (Docket #10) ¶ 11 ("We are absolutely are not disclosing everything we found in this report"); July 31 email from Zack Anderson to Nikita Caine (Anderson Decl. ¶ 19, Ex. 1) ("We left out a couple of key details from the slides"). Further, the MBTA asserts that the information provided publicly so far is not sensitive. (Docket #30 at 5-6.) Even were such disclosure unlawful, which it is not, there is no imminent risk that it will occur.

II. The CFAA Regulates Attacks on Protected Computers, Not Speech.

The MIT Students' Motion for Reconsideration provides a comprehensive discussion of the legislative history and case law interpreting the CFAA. (*See* Docket #23, Mot. at 9-12.) In response, the MBTA claims the MIT Students' interpretation of the CFAA is "illogical" but fails to cite even a single statutory provision, court opinion, or item from the legislative record that supports its interpretation. (*See* MBTA Opp. at 8-10.)

The MBTA relies only on Webster's New World Dictionary for the definition of "transmit," claiming that "transmission…to a protected computer" under the CFAA must include "verbal acts" as well as actual electronic transmission of code. In every opinion of which we are aware that involves a claim made, as here, under 18 U.S.C. § 1030 Section (a)(5)(A)(i), "transmission" involves the transfer of code from one computer to another computer, not the verbal act of talking about such transmission. Every case, including those that take the most liberal view of what is required to state a claim under section (a)(5)(A) of the CFAA, require that code be transmitted to a computer. *See, e.g., Arience Builders, Inc. v. Baltes*, 2008 WL 2580166 (N.D. Ill. June 17, 2008) (defendant deleted confidential and proprietary business data, information and trade secrets as well as data that would have revealed his improper conduct); *U.S. v. Pok Seong Kwong*, 237 Fed. Appx. 966 (5th Cir. 2007) (defendant installed harmful programs on the plaintiff's computer system); *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (plaintiff sufficiently alleged "transmission" by claiming defendant downloaded a program designed to permanently erase computer files); *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268 (S.D. Fla. 2003) (accessing VPN and spoofing computers constitutes transmission).

The issue raised by the MBTA of what constitutes a "transmission" was specifically addressed in *International Airport Centers* and *Arience Builders, Inc*. In *International Airport Centers*, the court determined that the statute was satisfied when a program was "transmitted to the computer *electronically*." 448 F.3d at 419 (emphasis added). The Seventh Circuit expressed a concern about stretching the understanding of "transmission" beyond the electronic context. Judge Posner, writing for the court, noted:

> Pressing a delete or erase key in fact transmits a command, but it might be stretching the statute too far (especially since it provides criminal as well as civil sanctions for its violation) to consider any typing on a computer keyboard to be a form of "transmission" just because it transmits a command to the computer.

Id. at 419. Under the MBTA's formulation of "transmission," however, just telling someone about the *existence* of the delete key would be a transmission subject to the CFAA.

In *Arience Builders*, the court addressed a motion to dismiss made in reliance on *International Airport Centers*. The court held the plaintiff had sufficiently alleged 'transmission' in violation the CFAA, by claiming that a former employee entered 'a code and/or command' which caused 'deletion and/or damage' to employer's computer system by secretly and maliciously copying and converting proprietary data for his own use and then deleting proprietary and other data, including data that would have revealed the improper conduct. *Arience Builders, Inc.*, 2008 WL 2580166 at *1-2. Again, "transmission" under the act required entering instructions into a computer.

Thus, it is clear that a violation of the CFAA requires an actual transmission of instructions to a protected computer. Merely talking about potential vulnerabilities in computers does not state a cause of action. The MBTA has cited no contra authority.[6]

III. The MBTA's View of "Responsible Disclosure" Is Irrelevant.

Here, the MBTA self-servingly defines "responsible disclosure" as preventing criticism of the computer security of public transit agency until that agency (a) is provided the factual basis for the criticism; and (b) can fix the problem. (*See* Complaint at ¶ 57, and Requested Relief ¶ 3(c), (g).) It then asserts that the letter signed by eleven preeminent computer scientists and security researchers and submitted on behalf of the MIT Students, *see* Docket #23-3, is "illogical" and "self contradictory." (MBTA Opp. at 13.) The letter speaks for itself and provides useful context for understanding this dispute. As outlined in the letter, the MIT Students have followed best practices in carrying out and disclosing their research.

[6] The MBTA's discussion of "chains" of actors is similarly unsupported by authority. In any event, even in the hypothetical it provides, *see* MBTA Opp. at 8-9, malicious code is still transmitted to a computer while the actual harm is delayed. Here, there was no transmission of code to any computer, nor was any such transmission threatened or imminent.

Moreover, MBTA's view of responsible disclosure should not be credited by this Court because the MBTA's argument posits that an entity with the poor security has *carte blanche* to decide when or if the security vulnerability ever becomes public. Where, as here, the insecure entity is going about in the public sphere casting doubt on the vulnerabilities,[7] the MBTA's view of "responsible disclosure" would prevent security researchers from *proving* their claims by giving sufficient information for third parties to replicate the claims. Instead, to the extent the MBTA would allow security researcher to participate in the debate at all,[8] the researcher could only do so while crippled.

In any event, the concept of "responsible disclosure" has no legal force. Even if the MIT Students had not acted responsibly, the MBTA has no cause of action. Neither the MBTA nor the courts may constitutionally impose a requirement of "responsible" speech. For example, in *Westfield High School L.I.F.E. Club v. City of Westfield*, 249 F. Supp. 2d 98 (D. Mass. 2003), another court in this district considered a "Responsible Speech" policy at a high school. Even in the more restrictive context of a high school, the court applied strict scrutiny and found the students "substantially likely to prevail on their claim that the school's speech policies are facially unconstitutional subject-matter-based restrictions." The court also found it to be an impermissible prior restraint to require students to obtain the permission of the administration before distributing literature on school grounds. If a government sponsored view of responsibility is not permissible for school administrators and high school students, it certainly is

---

[7] *See* Christopher Baxter and Hiawatha Bray, *MIT students' report makes security recommendations to T*, Boston Globe, August 12, 2008 ("'There have been claims in the past that have been made against our card or other cards, and, happily, they've all been able to be dismissed or dealt with,' said Daniel A. Grabauskas, general manager of the Massachusetts Bay Transportation Authority. 'I'm confident it will be the same thing here.'")

[8] *See* Complaint, Requested Relief ¶ 3(c) (requesting a preliminary injunction against "publicly stating or indicating that the security or integrity of the CharlieCard pass, the CharlieTicket pass, or the MBTA's Fare Media systems has been compromised…until the MBTA's vendors have had sufficient time to correct defects.")

not permissible for transit agencies and adults. Indeed, it the MBTA were to enforce the MBTA's views of "responsible disclosure" through discipline against own employees, it would run afoul of the Massachusetts Civil Rights Act, M.G.L.A. 12 § 11I.

IV. The MIT Students' Speech Is Core First Amendment Speech and the MBTA's Reliance on "Commercial Speech" Cases Is Inapposite.

The MBTA wrongly contends that the speech in question here is "commercial" and thus entitled to a lower level of protection. (*See* MBTA Opp. at 12.) To the contrary, the MIT Students had proposed to engage in core political speech: a matter of critical public and academic interest—the effectiveness of the security in Boston's mass transit fare payment system—with other security researchers.

It is black letter law that issues of public policy are "core" speech under the First Amendment and thus entitled to the highest level of protection. *See, e.g. Connick v. Myers*, 461 U.S. 138, 145 (1983) ("speech on public issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.") (internal quotations omitted); *see also First National Bank of Boston v. Bellotti*, 435 U.S. 765, 776 (speech on matters of public concern lies "at the heart of the First Amendment's protection.").

There can be no doubt the censored presentation and the "Security Analysis" currently at issue concern a matter of significant public interest—whether a major public subway system is using payment systems with sufficient security.[9] Indeed, the articles in Boston-area press and elsewhere, long before the DEFCON conference, illustrate the public interest in this subject. *E.g.*, Hiawatha Bray, *T Card Has Security Flaw, Says Researcher*, Boston Globe, Mar. 6, 2008; Szanislo, Marie, *Research: Charlie Card is Far From Hack Proof*, Boston Herald, Mar. 6, 2008; see also B. Schneier, *Why Being Open About Security Makes Us All Safer in the Long Run*, The

[9] The Boston Herald reports that the "T gave a no-bid contract for CharlieCard services to a former government employee." Marie Szaniszlo, *Board member demands MBTA audit*, Boston Herald, August 14, 2008. This significantly increases the public interest in whether the MBTA's choice to deploy the CharlieCard was a good one.

Guardian, Aug. 7, 2008.[10] Indeed, the intensity of public interest in these issues is amply demonstrated by the extensive coverage this litigation itself has received. *See e.g., MBTA Blocks MIT Students from Revealing Fare Tips*, Boston Globe, August 10, 2008; Christopher Baxter, and Hiawatha Bray, *MIT Students' Report Makes Security Recommendations to T*, Boston Globe, August 12, 2008; Marie Szaniszlo, *Board Member Demands MBTA Audit*, Boston Herald, August 14, 2008; Maddie Hanna, *Court Tells Students to Disclose Hacker Secrets in T Case*, Boston Globe, August 15, 2008. In addition to daily news coverage, this issue has sparked much public comment and opinion. *See e.g.* Boston Globe Editorial Board, *Hacking and Free Speech,* Boston Globe, August 14, 2008; Harvey Silverglate, *National Security and Free Speech*, August 16, 2008.

By the same token, both the original presentation and the "Security Analysis" now at issue would help inform public discussion of a matter of public policy: whether Boston's transportation authorities have taken appropriate steps to protect the security of the public subway system. "The central commitment of the First Amendment . . . is that 'debate on public issues should be uninhibited, robust, and wide-open." *Bond v. Floyd*, 385 U.S. 116, 136 (1966). That debate cannot be robust if important information about how government authorities are performing their duties is withheld from the public. *New York Times*, 376 U.S. at 275 (noting Founding Fathers viewed "The right of free public discussion of the stewardship of public officials [as] a fundamental principle of the American form of government."); *Thornhill v. Alabama*, 310 U.S. 88, 101-02 (1940) ("Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.").

Indeed, the issues raised by the MIT Students presentation have already led one MBTA board member to publicly question the effectiveness of MBTA management, noting that the

[10] Copies of all the articles cited here are attached to the Declaration of Corynne McSherry in Support of the MIT Students' Motion for Reconsideration.

apparent security vulnerabilities were just "the latest example of 'a systemwide failure' to properly implement and oversee the system." *See* Christopher Baxter, *T Board member says automated fare collection is a mess*, Boston Globe, Aug. 13, 2008. The students, as members of the public, have a right to participate in this debate.

Moreover, the students were planning to present to other security researchers the results of their academic, noncommercial research, conducted for a credited course on Computer and Network Security and acknowledged as superior work by a renowned MIT professor.[11] Their speech, both as originally considered and now contemplated, is plainly academic work, which has long been understood to be a special concern of the First Amendment. *See Keyishian v. Bd. of Regents of Univ. of State of N.Y.*, 365 U.S. 589, 603 (1967) ("Our Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment."); *Sweezy v. New Hampshire*, 354 U.S. 234, 250 (1957) (areas of academic freedom and political expression are "areas in which government should be extremely reticent to tread."). *See also Regents of the Univ. of Cal. v. Bakke*, 438 U.S. 265, 312 (1978) ("Academic freedom, though not a specifically enumerated constitutional right, long has been viewed as a special concern of the First Amendment"); *accord Asociacion de Educacion Privada de Puerto Rico, Inc. v. Garcia-Padilla*, 490 F.3d 1 (1st Cir. 2007) ("The right to academic freedom establish[es] a zone of First Amendment protection for the educational process itself") (internal citations omitted). Indeed, this Court's temporary restraining order has been viewed as a threat to the free exchange of scholarship, prompting eleven leading computer scientists to file a letter supporting the students. *See generally* Letter from Computer Science Professors and Computer Scientists (Docket #23-3).

[11] Dr. Ronald Rivest, the students' professor, is one of three inventors of the RSA algorithm, widely recognized as one of the first great advances in a particular type of cryptography that is now widely used. Prof. Rivest is also a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptologic Research, and the American Academy of Arts and Sciences.

Contrary to the MBTA's argument, discussion of the MBTA security vulnerabilities is not commercial speech. The MBTA has, in fact, offered ***no*** evidence that the MIT Students' speech possesses any attributes of commercial speech. *See Virginia State Bd. Of Pharm. v. Virginia Consumer Council*, 425 U.S. 748, 762 (1976) (commercial speech is speech that does "no more than propose a commercial transaction"). Nor do they explain how any future comments on the issue could arguably be "commercial" for the purposes of First Amendment doctrine.

The students did not and do not propose to offer any product or service for sale, nor are they affiliated with any commercial entity related to the research, nor is there a shred of evidence suggesting their presentation was economically motivated.[12] *Compare Bolger v. Young's Drug Products Corp.* 463 U.S. 60 (1983) (pamphlets to be mailed to general public by contraceptives manufacturer were commercial speech under the First Amendment where they were conceded to be advertisements, contained references to manufacturer's products, *and* manufacturer had economic motivation for mailing them.). They did not propose even to provide information *about* any product. *Compare Virginia Bd. of Pharmacy*, 425 U.S. at 760-61 (prescription drug advertising constituted commercial speech).

According to the MBTA's theory, any time a researcher attempted to promote her own research, even where, as here, the research concerns a matter of great public import, the speech would automatically lose its full First Amendment protection and be downgraded to the lower commercial speech standard that is afforded to material such as prescription drug advertising.

[12] While speakers at the DEFCON conference have the option to receive a small honorarium or free passes to the conference, this nominal compensation would not have even covered the MIT Students' expenses in traveling to the conference. (Anderson Decl. ¶ 25.) "It is well settled that a speaker's rights are not lost merely because compensation is received; a speaker is no less a speaker because he or she is paid to speak." *Riley v. National Federation of the Blind of North Carolina, Inc.*, 487 U.S. 781, 801 (1988); *see also United States v. National Treasury Employees Union*, 513 U.S. 454, 475 (1995) (invalidating a prohibition on the receipt of honoraria by government employees on First Amendment grounds). In any event, the students were not actually paid the honorarium. (Anderson Decl. ¶ 25.)

Were this true, academic research and publication would be chilled with potentially dire consequences for academic freedom and public discourse. The MBTA's position is not just wrong, it is dangerous.

CONCLUSION

For the above-stated reasons, the Court should **GRANT** the MIT Students' Motion and dissolve the Temporary Restraining Order. The Court should also **DENY** any motion by the MBTA to convert the Temporary Restraining Order into a preliminary injunction.[13]

August 16, 2008

Respectfully submitted,

/s/ Adam J. Kessel
Lawrence K. Kolodney (BBO # 556851)
Email: kolodney@fr.com
Adam J. Kessel (BBO # 661211)
Email: kessel@fr.com
Thomas A. Brown (BBO # 657715)
Email: tbrown@fr.com
FISH & RICHARDSON P.C.
225 Franklin Street
Boston, MA 02110-2804
(617) 542-5070 (Telephone)
(617) 542-8906 (Facsimile)

John Reinstein, BBO #416120
Email: reinstein@aclum.org
ACLU of Massachusetts
211 Congress Street, 3rd Floor
Boston, MA 02110

Jennifer Stisa Granick, CA Bar No. 168423
Email: Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
Email: kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
Email: marcia@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333

Counsel for Defendants Anderson, Ryan and Chiesa

[13] The MIT Students reserve their right to file a separate opposition to any motion for a preliminary injunction the MBTA might file.

CERTIFICATE OF SERVICE

I certify that this motion and the attached declaration are being filed through the Court's electronic filing system on August 18, 2008, which serves counsel for other parties who are registered participants as identified on the Notice of Electronic Filing (NEF). Any counsel for other parties who are not registered participants are being served by first class mail on the date of electronic filing.

/s/ Adam J. Kessel
Adam J. Kessel

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	Civil Action No. 08-11364-GAO

DECLARATION OF ZACK ANDERSON IN REPLY TO OPPOSITION TO MOTION FOR RECONSIDERATION OF TEMPORARY RESTRAINING ORDER

1. I am a student in computer science and electrical engineering at the Massachusetts Institute of Technology. I am a defendant in this matter. I have personal knowledge of the matter stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.
2. I am 21 years old. My fellow students RJ Ryan and Alessandro Chiesa are also defendants in this case. RJ is 22 years old and Alessandro is 20.
3. The computer science and electrical engineering program at MIT is academically demanding. I worked hard in high school to be accepted at MIT and I work hard now to maintain high academic standards now that I am a student. I have a 4.5/5 GPA.

4. I have received the following awards and honors: DARPA Grand Challenge Robotics Competition Finalist (2004), US FIRST Rookie All-Star Award (2005), George C. Newton Prize (2008), California Scholarship Foundation Award (2005), 1st Place at LA County Science Fair for autonomous robot (2003), National AP Scholar (2005), SFV Engineer's Council Robotics Engineering Excellence Award (2002).
5. I have also applied for two patents.
6. I have many extracurricular projects related to my academic areas of interest, including robotics projects.
7. RJ and Alessandro are also serious students with important extracurricular activities. My understanding is that both are also at the top of their class at MIT. Both RJ and Alessandro are on MIT's Division I rowing team, and RJ has been very involved with volunteer work. RJ has been nationally recognized for his work in computer graphics. For all three of us, our education at MIT is extremely important.
8. For the final project in one of our classes with Professor Ron Rivest, RJ, Alessandro, another student and I applied existing research on stored value cards commonly used for fare payment in transit systems to the Boston subway's CharlieCard and CharlieTicket. This experiment confirmed that an attacker could modify the CharlieTicket and presented an aspirational attack on the CharlieCard that showed that additional security measures employed by plaintiff Massachusetts Bay Transportation Authority ("MBTA") were inadequate to prevent card modifications. Our paper received an "A."
9. As part of the security research, RJ and I tested the CharlieTicket vulnerability. Allessandro did not participate in the security testing. To conduct this security

vulnerability testing, it was not necessary to (and we did not) ride the subway or otherwise use the MBTA's transportation services for free. In the course of our research we spent between $100 and $200 on MBTA stored value cards, plus hundreds more on research equipment. To put that in perspective, MIT students can obtain monthly T passes for $29.50 through MIT. *See* "Take the T to Work and Leave the Driving to Someone Else," http://web.mit.edu/facilities/transportation/tpass.html

10. The teaching assistants for Professor Rivest's class, Computer and Network Security, asked whether we would like our paper posted publicly on the class website. We said we did not want to post the paper because we wanted to have an opportunity to discuss our findings with the MBTA first.
11. On May 15, 2008, RJ, Alessandro and I submitted a talk proposal to present our research at the DEFCON computer security conference, held August 8 to August 10, 2008 in Las Vegas, Nevada. Our talk was accepted.
12. DEFCON is advertised as one of the oldest and largest hacker conferences in the world. It is the sister conference to Black Hat, which happens earlier in the week. Academics, corporate security officers, government officials and IT experts from companies like Microsoft and Google pay to attend Black Hat and get free admission to DEFCON. In addition, a lot of independent security researchers attend and speak at the conference. It is supposed to be fun.
13. In both the proposal and the abstract for our talk, we blatantly emphasized that our findings showed a security flaw that could be exploited by attackers because we wanted to sensationalize our talk and make it seem fun so that people would attend.
14. For the substance of the talk, we always planned to include existing and original

research, but to leave out information we had discovered about a checksum safeguard that the MBTA had implemented on the CharlieTicket because we believed that that information could give an attacker too much assistance in modifying the ticket or creating a false ticket. We also did not disclose details about the encryption algorithm (Crypto-1) behind the CharlieCard, some of which we do not know.

15. On Friday, July 25, 2008 we emailed Professor Rivest to ask for assistance setting up a meeting with the MBTA about our findings. We did not immediately receive a response from Professor Rivest, who was away at a conference, so we emailed again on July 30, 2008.

16. Professor Rivest called the MBTA on July 31, 2008 and then let us know that the agency was concerned about our upcoming talk and that they had contacted the FBI.

17. We set up a meeting with the MBTA for August 4, 2008. The MBTA sent Sergeant Detective Richard Sullivan of the Transit Police, and he brought a special agent from the Federal Bureau of Investigation, Jacob Shaver, with him. MBTA had not told us that an FBI agent was going to be at the meeting.

18. At the end of the meeting, Detective Sullivan did not request that that we give him a copy of our slides. Rather, we agreed to deliver a short confidential report to the MBTA summarizing our vulnerability findings and recommendations. Later that day, we received a friendly note from S.A. Shaver. We did not believe that there was any problem going forward with our talk as planned.

19. Attached as Exhibit 1 are true and correct copies of two emails I sent to Nikita Caine, an organizer for DEFCON. These emails have been provided to the MBTA in discovery.

20. To address the MBTA's concerns, we asked DEFCON to modify the abstract to make it clear that we had no intention of teaching people how to make counterfeit cards or tickets. Exhibit 1, Email from Zack Anderson to Nikita Caine, August 5, 2008, MBTA00011
21. On July 31, 2008, I informed Ms. Caine that RJ, Alessandro and I intentionally left out key details from the slides. Exhibit 1, Email from Zack Anderson to Nikita Caine, July 31, 2008, MBTA00012
22. Before DEFCON we provided a Confidential Vulnerability Report ("CVR") to the MBTA. That document contained the information about the checksum on the CharlieTicket, which we had always intended to withhold. MBTA has publicly filed the CVR in this case and it is now a public document. The three of us were surprised and concerned that the MBTA chose to do that.
23. The MBTA did not ask for copies of our slides until Friday, August 8, 2008, after we had already been told by MIT's counsel Jay Wilcoxson that he understood the MBTA was in the process of filing suit against us and seeking a temporary restraining order to keep us from giving our presentation. We decided not to send the slides to the MBTA until we had an opportunity to review the lawsuit.
24. In order to further assist the MBTA we created a longer, more detailed report about our research. We provided that report under seal in this case. This report also represents everything that we want to be able to talk about in the future regarding our research on MBTA security. Furthermore, it covers all of our significant and relevant findings about the vulnerabilities.

25. Speakers at the DEFCON conference have the option to receive a $200 honorarium or free passes to the conference. We elected to take the honorarium. This nominal compensation would not have even covered our expenses in traveling to the conference. Since we did not give the talk, we are not entitled to receive any compensation at all.
26. We did not and do not intend to publish the Class Paper.
27. We did not publish the software tools developed in the course of this research.
28. We never decided which research materials, including software code, if any, we would include or demonstrate in our final presentation at DEFCON. Our efforts to re-evaluate the materials after the MBTA expressed its concerns delayed the decision-making process. In light of the MBTA's concerns and the subsequent filing of this lawsuit, we ultimately did not finalize any software or demonstration plans for the DEFCON presentation.
29. Our research materials were never presented to the public.
30. We do not currently intend to demonstrate any research materials.

Signed under penalty of perjury this 18th day of August 2008.

\s\ Zack Anderson
Zack Anderson

Subject: Re: Revised abstract
Date: Tue, 05 Aug 2008 22:29:35 -0400
From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>
References: <48988CC7.5060901@mit.edu>
<5dba3ce20808051926m7555b2c5o4cb74c1ddda11117@mail.gmail.com>

Thanks so much!

Zack

Nikita Caine wrote:
This should be updated on the website soon if not already, however do note the webmaster is in las vegas at the moment, and your previous abstract will be what is printed on the program.

On Tue, Aug 5, 2008 at 10:24 AM, Zack Anderson <zacka@mit.edu> wrote:

Hi Nikita,

We met with a Sargent Detective of the Intelligence unit at the MBTA and a Special Agent of the cybercrimes division of the FBI yesterday. The meeting went well, and our legal counsel has advised us that we can definitely proceed with the talk. If you don't mind, can you change our abstract on the website to this:

"In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems."

Thanks,
Zack

-------- Original Message --------
Subject: Revised abstract
Date: Tue, 05 Aug 2008 13:24:23 -0400

From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>

Hi Nikita,

We met with a Sargent Detective of the Intelligence unit at the MBTA and a Special Agent of the cybercrimes division of the FBI yesterday. The meeting went well, and our legal counsel has advised us that we can definitely proceed with the talk. If you don't mind, can you change our abstract on the website to this:

"In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey 'human factors' that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems."

Thanks,
Zack

-------- Original Message --------
Subject: Re: Defcon CD
Date: Thu, 31 Jul 2008 22:33:37 -0400
From: Zack Anderson <zacka@mit.edu>
To: Nikita Caine <barkingkitten@gmail.com>
References: <5dba3ce20807010045o46a72b5bi6700c97871711870@mail.gmail.com>
<489231BD.6030209@mit.edu>
<5dba3ce20807311734n416e4aa6pd03a9c6b6728a838@mail.gmail.com>

We still plan on giving the talk. We left out a couple of key details from the slides, so for now I think we will be alright. We are meeting with the MBTA and legal counsel on Monday. I will keep you posted if anything changes, but expect us to give the talk.

Zack

Nikita Caine wrote:
Zack,

The CD's have been printed and are on their way to Vegas, There is no way to change it at this point. Please let me know if you will be

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY, Plaintiff, v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendants.	Civil Action No. 08-11364-GAO

DECLARATION OF CORYNNE MCSHERRY IN SUPPORT OF MOTION FOR RECONSIDERATION OF TEMPORARY RESTRAINING ORDER

I am an attorney with the Electronic Frontier Foundation, co-counsel for the Defendants Zack Anderson, RJ Ryan, and Allesandro Chiesa in the above-captioned matter. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

1. Attached hereto as Exhibit 1 is Hiawatha Bray, *T Card Has Security Flaw, Says Researcher*, Boston Globe, Mar. 6, 2008, downloaded August 17, 2008 from http://www.boston.com/business/articles/2008/03/06/t_card_has_security_flaw_says_researcher.

2. Attached hereto as Exhibit 2 is Marie Szaniszlo, *Research: Charlie Card is Far From Hack Proof*, Boston Herald, Mar. 6, 2008, downloaded August 17, 2008, from http://news.bostonherald.com/news/regional/general/view.bg?articleid=1078138.

3. Attached hereto as Exhibit 3 is Bruce Schneier, *Why Being Open About Security Makes Us All Safer in the Long Run,* The Guardian, Aug. 7, 2008, downloaded

August 17, 2008, from http://www.guardian.co.uk/technology/2008/aug/07/hacking.security.

4. Attached hereto as Exhibit 4 is *MIT Blocks Students from Revealing Fare Tips*, Boston Globe, Aug. 10, 2008, downloaded August 17, 2008 from http://www.boston.com/news/local/massachusetts/articles/2008/08/10/mbta_blocks_mit_students_from_revealing_fare_tips/.

5. Attached hereto at Exhibit 5 is Christopher Baxter, *MIT Students' Report Makes Security Recommendations,* Boston Globe, Aug. 12, 2008, downloaded August 17, 2008 from http://www.boston.com/news/education/higher/articles/2008/08/12/mit_students_report_makes_security_recommendations_to_t/.

6. Attached hereto as Exhibit 6 is George Hulme, *MBTA: Legally Shackling Security Researchers Rarely Works*, InformationWeek Security Weblog, Aug. 14, 2008, downloaded August 17, 2008, from http://www.informationweek.com/blog/main/archives/2008/08/mbta_legally_sh.html.

7. Attached hereto as Exhibit 7 is Marie Szaniszlo, *Board Member Demands MBTA Audit*, Boston Herald, Aug. 13, 2008, downloaded August 17, 2008 from http://news.bostonherald.com/news/regional/politics/view/2008_08_14_Board_member_demands_MBTA_audit/srvc=home&position=also.

8. Attached hereto as Exhibit 8 is Maddie Hanna, *Court Tells Students to Disclose Hacker Secrets in T Case*, Boston Globe, Aug. 14, 2008, downloaded August 17, 2008 from http://www.boston.com/news/local/articles/2008/08/15/court_tells_students_to_disclose_hacker_secrets_in_t_case/.

9. Attached hereto as Exhibit 9 is Boston Globe Editorial Board, *Hacking and Free Speech*, Boston Globe, Aug. 14, 2008, downloaded August 17, 2008 from

http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2008/08/14/hacking_and_free_speech/?page=full.

10. Attached hereto as Exhibit 10 is KiMae Heussner, *Leading Computer Scientists Defend Student Hackers*, ABCnews.com, Aug. 14, 2008, downloaded on August 17, 2008 from http://www.abcnews.go.com/Technology/story?id=5581876&page=1

11. Attached hereto as Exhibit 11 is Marie Szanislow, *MIT Students Must Turn In Charlie Card Data Today*, Boston Herald, Aug. 15, 2008, downloaded on August 17, 2008 from http://news.bostonherald.com/news/regional/general/view/2008_08_15_MIT_students_must_turn_in_CharlieCard_data_today/.

12. Attached hereto as Exhibit 12 is Robert Caron, *Missed Opportunity On MBTA Security*, Letters to the Editor, Boston Globe, Aug. 16, 2008, downloaded Aug. 17, 2008 from http://www.boston.com/bostonglobe/editorial_opinion/letters/articles/2008/08/16/missed_opportunity_on_mbta_security/.

13. Attached hereto as Exhibit 13 is Harvey Silverglate, *National Security and Free Speech*, Boston Globe, August 16, 2008, downloaded August 17, 2008 from http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2008/08/16/national_security_and_free_speech/.

14. Attached hereto as Exhibit 14 is Ben Arnoldy and Uri Friedman, *Not So Smart Cards Easily Hacked*, Christian Science Monitor, August 18, 2008, downloaded August 18, 2008 from http://www.csmonitor.com/2008/0819/p01s01-usgn.html.

Signed under penalty of perjury this 18th day of August 2008 in San Francisco, California.

__/s/_____
Corynne McSherry, Esq.

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING



T card has security flaw, says researcher

The Boston Globe

Cracked code could lead to counterfeits, study team warns

By Hiawatha Bray, Globe Staff | March 6, 2008

A computer science student at the University of Virginia asserts that he has found a security flaw in the technology behind the Massachusetts Bay Transportation Authority's CharlieCard system.

German-born graduate student Karsten Nohl specializes in computer security. Nohl and two fellow security researchers in Germany say they've cracked the encryption scheme that protects the data on the card. The team warns that their breakthrough could be used to make counterfeit copies of the cards, which are used by commuters to pay for MBTA bus and subway rides.

"You could have thousands of cards and sell them in the underworld," said David Evans, an associate professor of computer science at the university, and Nohl's adviser. Nohl himself is on spring break and could not be reached.

The CharlieCard uses a Radio Frequency Identification, or RFID, chip. The card is pressed against a detector, which reads data from the chip and deducts the price of a subway or bus ride from the owner's account.

The T spent $192 million to introduce the CharlieCard in 2006. The system replaced cash and tokens.

A press release issued by the University of Virginia said Nohl's research team obtained the same kind of chip, then used abrasives to scrape away the chip layer by layer. By examining the chip circuitry, they were able to figure out the encryption algorithm it uses and found weaknesses that made it easy to break. Next, the team was able to use commercially available RFID readers to capture data from any RFID-equipped cards that came within range. They could then decrypt the data on those cards and copy them. Nohl said that his team needed only about $1,000 worth of equipment to dismantle the chip and crack the code.

Nohl said that the RFID chip they compromised, the MiFare Classic by NXP Semiconductors of the Netherlands, is the one used in London's subway system and in the MBTA CharlieCard. But MBTA spokesman Joe Pesaturo refused to confirm or deny this. "It's MBTA policy not to discuss security measures around its smart card technology," he said.

A 2004 policy analysis of the CharlieCard system produced by the Massachusetts Institute of Technology said that it would be based on MiFare technology.

NXP Semiconductors issued a statement saying that Nohl's team breached only one of several security features built into the MiFare Classic chip. "This does not breach the security of the overall system," the company said. "Even if one layer were to be compromised, other layers will stop the misuse."

Evans said it might be hard to solve the issue. "There are chips that have a much higher security level available," he said. "They cost more and it is not a trivial matter to upgrade the system."

Ari Juels, chief scientist and director of computer security company RSA Laboratories in Bedford, said that Nohl's research illustrates that there are serious security flaws in many smartcard applications. "The vulnerability is most certainly for real," Juels said.

Hiawatha Bray can be reached at bray@globe.com. ■

© Copyright 2008 The New York Times Company

Research: CharlieCard is far from hack-proof

By Marie Szaniszlo | Thursday, March 6, 2008 | http://www.bostonherald.com | Local Coverage

New research by a University of Virginia graduate student shows that “smart cards” like the CharlieCard may be vulnerable to cyber thieves, who potentially could steal fares or sell counterfeits.

The incentive for theft could increase if state officials proceed with plans to allow commuters to use a CharlieCard not only to ride the T, but also to pay Mass Pike tolls and access government-run parking facilities, with funds being automatically withdrawn from their bank account.

The article you requested has been archived

All coverage within BostonHerald.com from the last 7 days remains **free of charge**. Articles do not always include original photos, charts or graphics.

» **Click for access to article within the archive**

Article URL: http://www.bostonherald.com/news/regional/general/view.bg?articleid=1078138

Related Articles:

MIT students must turn in CharlieCard data today
/news/regional/general/view.bg?articleid=1113095

Contact us | Print advertising | Online advertising | Herald history | News tips | Electronic edition | Browser upgrade | Home delivery | Herald wireless

$ave on Boston Herald Home Delivery

Jobs with Herald Media

For back copy information and more information on other collectible copies please call 617-426-3000 Ext. 7714. Click here for Celtics, Patriots and Red Sox back copies

© Copyright by the Boston Herald and Herald Media.
No portion of BostonHerald.com or its content may be reproduced without the owner's written permission. Privacy Commitment



guardian.co.uk

Why being open about security makes us all safer in the long run

Bruce Schneier
The Guardian, Thursday August 7 2008

London's Oyster card has been cracked, and the final details will become public in October. NXP Semiconductors, the Philips spin-off that makes the system, lost a court battle to prevent the researchers from publishing. People might be able to use this information to ride for free, but the sky won't be falling. And the publication of this serious vulnerability actually makes us all safer in the long run.

Here's the story. Every Oyster card has a radio-frequency identification chip that communicates with readers mounted on the ticket barrier. That chip, the "Mifare Classic" chip, is used in hundreds of other transport systems as well — Boston, Los Angeles, Brisbane, Oslo, Amsterdam, Taipei, Shanghai, Rio de Janeiro — and as an access pass in thousands of companies, schools, hospitals, and government buildings around Britain and the rest of the world.

The security of Mifare Classic is terrible. This is not an exaggeration; it's kindergarten cryptography. Anyone with any security experience would be embarrassed to put his name to the design. NXP attempted to deal with this embarrassment by keeping the design secret.

The group that broke Mifare Classic is from Radboud University Nijmegen in the Netherlands. They demonstrated the attack by riding the Underground for free, and by breaking into a building. Their two papers (one is already online) will be published at two conferences this autumn.

The second paper is the one that NXP sued over. They called disclosure of the attack "irresponsible," warned that it will cause "immense damages," and claimed that it "will jeopardize the security of assets protected with systems incorporating the Mifare IC." The Dutch court would have none of it: "Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings."

Exactly right. More generally, the notion that secrecy supports security is inherently flawed. Whenever you see an organization claiming that design secrecy is necessary for security — in ID cards, in voting machines, in airport security — it invariably means that its security is lousy and it has no choice but to hide it. Any competent cryptographer would have designed Mifare's security with an open and public design.

Secrecy is fragile. Mifare's security was based on the belief that no one would discover how it worked; that's why NXP had to muzzle the Dutch

researchers. But that's just wrong. Reverse-engineering isn't hard. Other researchers had already exposed Mifare's lousy security. A Chinese company even sells a compatible chip. Is there any doubt that the bad guys already know about this, or will soon enough?

Publication of this attack might be expensive for NXP and its customers, but it's good for security overall. Companies will only design security as good as their customers know to ask for. NXP's security was so bad because customers didn't know how to evaluate security: either they don't know what questions to ask, or didn't know enough to distrust the marketing answers they were given. This court ruling encourages companies to build security properly rather than relying on shoddy design and secrecy, and discourages them from promising security based on their ability to threaten researchers.

It's unclear how this break will affect Transport for London. Cloning takes only a few seconds, and the thief only has to brush up against someone carrying a legitimate Oyster card. But it requires an RFID reader and a small piece of software which, while feasible for a techie, are too complicated for the average fare dodger. The police are likely to quickly arrest anyone who tries to sell cloned cards on any scale. TfL promises to turn off any cloned cards within 24 hours, but that will hurt the innocent victim who had his card cloned more than the thief.

The vulnerability is far more serious to the companies that use Mifare Classic as an access pass. It would be very interesting to know how NXP presented the system's security to them.

And while these attacks only pertain to the Mifare Classic chip, it makes me suspicious of the entire product line. NXP sells a more secure chip and has another on the way, but given the number of basic cryptography mistakes NXP made with Mifare Classic, one has to wonder whether the "more secure" versions will be sufficiently so.

• *Bruce Schneier is a security technologist and author: schneier.com/blog*

guardian.co.uk © Guardian News and Media Limited 2008

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

MBTA blocks MIT students from revealing fare tips

Associated Press

August 10, 2008

BOSTON --The Massachusetts Bay Transportation Authority is suing three MIT students who say they've found security flaws in the T's automated fare system.

The three planned to make their findings public at a Las Vegas computer hacker conference, but the MBTA was granted a court injunction barring them from revealing what they found about the CharlieCard and CharlieTicket system.

The MBTA alleges in court documents that the three claimed to have circumvented the security protocols of the ticketing system, according to the Boston Sunday Globe. The suit claims the three offered free subway rides for life to people over the Internet.

The suit also named MIT as a defendant.

Lawyers for the three did not return phone calls to the Globe.

Information from: The Boston Globe, http://www.boston.com/globe ■

© Copyright 2008 The New York Times Company

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

MIT students' report makes security recommendations to T

The Boston Globe

MBTA chief faults school on response

By Christopher Baxter, Globe Correspondent and Hiawatha Bray, Globe Staff | August 12, 2008

A report provided to the MBTA by three MIT students recommends that the agency implement an auditing system to detect tickets with forged encryption codes, create a central repository to store the current value of cards, and improve physical security measures in stations across Boston.

The vulnerability assessment, a confidential document that researchers said was not part of any public presentation, was included in filings after the Massachusetts Bay Transportation Authority sued Friday in federal court. A judge granted a temporary order blocking the students from publicly discussing how to hack the CharlieCard and CharlieTicket system to ride the T for free.

"There have been claims in the past that have been made against our card or other cards, and, happily, they've all been able to be dismissed or dealt with," said Daniel A. Grabauskas, general manager of the Massachusetts Bay Transportation Authority. "I'm confident it will be the same thing here."

Grabauskas lauded the judge's decision and said he was disappointed by the actions of the students and what he described as a less-than-zealous response from the Massachusetts Institute of Technology. MIT declined to comment on the pending litigation.

The MBTA sued after learning that MIT students Zack Anderson, R.J. Ryan, and Alessandro Chiesa planned to present their findings Sunday at the DEFCON hacker convention in Las Vegas. The temporary order is valid for 10 days. Then the T must prove that the students' research poses such a risk that an extended injunction is necessary. The T is also seeking unspecified financial damages, according to court papers.

"It's not a light step for a judge to grant this action, and it speaks to the strength of our arguments and the merits of our position," Grabauskas said.

But Marcia Hofmann - staff lawyer for the Electronic Frontier Foundation, a nonprofit representing the students - called the decision a "dangerous precedent for security researchers," which could potentially discourage the investigation and improvement of technology across the country.

"That certainly would discourage security researchers from discussing their work and sharing information that might ultimately make systems more secure," Hofmann said.

Anderson, a Los Angeles native and senior electrical engineering and computer science major, said the research started as a project in a network security class. He said the group was upfront with the MBTA, provided all the information it requested, and intended to help fix problems, rather than create more.

"We planned all along not to reveal the full details about what we had found," Anderson said. "We basically gave some information, but nothing that would enable someone to defraud the MBTA at all."

But Grabauskas said that the students did not disclose all their research and that he was concerned about what information not included in the written presentation might have been discussed at the conference.

Despite the agency's efforts to keep the information under wraps, much of the technology and vulnerabilities of the CharlieCard and CharlieTicket were detailed in court filings.

Regular MBTA riders usually obtain a CharlieCard, a hard plastic card that contains a Radio Frequency Identification chip. The card is pressed against a detector, which reads data from the chip and deducts the price of a subway or bus ride from the owner's account. Passengers can also use a paper CharlieTicket, which has a magnetic strip that stores the data. The report states that both cards can be cloned or forged.

The students' report says the CharlieTicket has four main problems: Value is stored on the card, not in a central MBTA database; anyone that has a card can read and write it with low-cost technology; a cryptographic signature algorithm is not used on the data to prevent forgeries; and MBTA networks do not have any centralized card verification system.

The CharlieCard has some level of security through encryption, according to the report, but it can be duplicated.

"They've made claims that they've been able to in some way understand part of the code," Grabauskas said. "What we're doing is simply trying to figure out whether or not there is anything to their claims."

Karsten Nohl, a German researcher who was one of the first to crack the CharlieCard's security, said he has been comparing notes with the MIT team and hopes to come to Boston to meet them.

He may also give a public demonstration of the CharlieCard security flaw by purchasing a card and showing how to clone it, he said. ■

© Copyright 2008 The New York Times Company

InformationWeek's Security Weblog

Topics: Security

- E-mail this page
- | Print this page
- | BOOKMARK

MBTA: Legally Shackling Security Researchers Rarely Works

Posted by **George Hulme**, **Aug 14, 2008 05:18 PM**



As many security and technology followers know, three MIT students had planned on presenting their findings on a number of vulnerabilities they found in the Massachusetts Bay Transportation Authority's CharlieTicket and CharlieCard payment cards at last week's Defcon conference. That was, until a gag order was put in place to keep them quiet. Today, a federal judge in Boston let the temporary restraining order stand. And so this Saga of Stupidity continues.

The hearing held in Boston today was to decide if it was OK for the MIT students to talk about the bevy of vulnerabilities they found in the Boston T. And let me tell you, if Russell Ryan, Zack Anderson, and Alessandro Chesa's presentation slides are an accurate indication of the state of security in the city's transportation system, one of the important questions remaining is why hasn't the Boston T been pwned long, long ago. We're talking about a system rife with all kinds of vulnerabilities. In fact, it may very well already have been compromised.

Part of their scheduled talk, Anatomy of a Subway Hack, would have provided details in how it's possible to generate stored-value fare cards, reverse engineer magstripes, and tap into the fare vendor network. And I think it's reasonable to assume others already have figured some of this out.

Because U.S. District Judge George O'Toole has decided not to decide until next Tuesday, this story may not move forward until Aug. 19.

The problem of trying to solve security vulnerabilities like this through the legal stifling of speech are manifold. Like the fact that it does nothing to solve the underlying security problems, and steals energy away from actually mitigating the problem. Chris Wysopal summed it up very well in his Zero In A Bit blog at VeraCode:

> "Security problems go away by mandating independent security testing before a product is accepted, not by trying to get security researchers to be quiet. This is a good example of how the reactive approach doesn't work. The flaws are still in the system and suing researchers has just shined a bright light on them."

Wysopal is right, and if the energy used to stifle the MIT students from publishing their research had been used to test the payment systems before it was deployed, you'd be reading about something else right now. So if you're upset at these researchers for finding these flaws, your anger is misplaced: it should be directed at the authorities for buying such a sheep of a system.

The idiocy of this all, especially now, is that the student's PowerPoint presentation was given to the thousands of Defcon attendees, and a 5-page vulnerability analysis already has become public. Not to forget, as ZDNet's Richard Koman noted earlier, that the MBTA, in its legal compliant, put a 30-page confidential report written by the students into the public record.

« Detecting Counterfeit Cisco Equipment | Main | Energy-Efficient Ethernet In The Data Center »

Tomorrow's CIO: Do you have what it takes?
Find out at the 2008 InformationWeek 500 Conference
Sept. 14-16, St. Regis Resort, Monarch Beach, Calif.

Sign up now for the weekly *InformationWeek* Blog Newsletter.

Discuss This

2 message(s). Last at: Aug 15, 2008 10:45:45 AM

p.s. I forwarded this like to my eastcoast inlaws. Some of them live in Boston.

So what you are saying is that if I track down which U.S. District Court has Judge O'Toole I can then run down the case and read the entire 30 page explaination of how to ride the subway for free? If I lived in Boston or any other city that used products from the same vendor I would be a travellin' man. Awsome!

Add Your Comment:

Post as user

Please login or register here for a free Techweb account to post

Post as guest

Name

This is a public forum. United Business Media and its affiliates are not responsible for and do not control what is posted herein. United Business Media makes no warranties or guarantees concerning any advice dispensed by its staff members or readers.

Community standards in this comment area do not permit hate language, excessive profanity, or other patently offensive language. Please be aware that all information posted to this comment area becomes the property of United Business Media LLC and may be edited and republished in print or electronic format as outlined in United Business Media's Terms of Service.

Important Note: This comment area is NOT intended for commercial messages or solicitations of business.

Please enter the word you see below



Submit Comment

Board member demands MBTA audit

By Marie Szaniszlo | Thursday, August 14, 2008 | http://www.bostonherald.com | Local Politics



Photo by Herald (file)

A member of the MBTA's board of directors yesterday waged an all-out assault on the agency's general manager, demanding an audit and saying she had lost confidence in him and in the safety and security of the T.

At a board meeting, Janice Loux cited a series of incidents that had occurred on Daniel A. Grabauskas' watch, from a fatal Green Line accident in May to three MIT students' claims that the CharlieCard, the T's automated fare collection system, is vulnerable to hackers.

"I have grave concerns today," Loux said, "and I have lost confidence in the general manager."

Bernard Cohen, the board's chairman and the state's transportation secretary, said he had asked Grabauskas to review the T's safety record and procedures after the Green Line trainwreck that left 24-year-old operator Terrese Edmonds dead.

"I have confidence in the safety of the MBTA system," Cohen said. "We can all do better in this area. No accident is acceptable . . . But the general public should feel safe riding the MBTA."

But Loux called for an outside audit, noting that safety was not the only issue.

The T gave a no-bid contract for CharlieCard services to a former government employee, she said. And, in addition to finding security problems with the CharlieCard, MIT undergrads Zack Anderson, R.J. Ryan and Alessandro Chiesa also claim to have found unlocked turnstile control boxes, control and surveillance rooms left unattended and keys left in unlocked boxes in public areas, Loux noted.

"This reaffirms my concerns about safety and security," she said.

The board will decide the scope of any audit in the coming weeks before deciding whether to proceed with one.

In the meantime, lawyers for the MBTA are due in court this morning to try to block the MIT students from releasing any information that could jeopardize the T's fare collection system.

"We just want to make very clear that we're not interested in quashing anyone's First Amendment rights," Grabauskas said, declining to respond to Loux's criticisms. "All we're really asking is that the court bar the release of any nonpublic information that might adversely affect the CharlieCard's security."

Article URL: http://www.bostonherald.com/news/regional/politics/view.bg?articleid=1112940

Related Articles:

MBTA worker nabbed in 'drop-box' scheme
/news/regional/general/view.bg?articleid=1113522

Critics rail over MBTA raises
/news/regional/politics/view.bg?articleid=1113247

MIT students must turn in CharlieCard data today
/news/regional/general/view.bg?articleid=1113095

Contact us | Print advertising | Online advertising | Herald history | News tips | Electronic edition | Browser upgrade | Home delivery | Herald wireless

$ave on Boston Herald Home Delivery

Jobs with Herald Media

For back copy information and more information on other collectible copies please call 617-426-3000 Ext. 7714. Click here for Celtics, Patriots and Red Sox back copies



© Copyright by the Boston Herald and Herald Media.
No portion of BostonHerald.com or its content may be reproduced without the owner's written permission. Privacy Commitment

0.04444 : cached : hawk.heraldinteractive.com
ma20041112940_2008-08-13 22:31:03_text_1_0_0

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

Court tells students to disclose hacker secrets in T case

The Boston Globe

Refuses to lift order prohibiting public discussion

By Maddie Hanna, Globe Correspondent | August 15, 2008

A federal judge yesterday refused to lift an order prohibiting three MIT students from publicly talking about how they allegedly hacked into the MBTA's automated ticketing system. However, he did order the trio to privately provide more information to the court about the security flaws they say they have uncovered.

US District Judge George A. O'Toole Jr., granting a request by the MBTA, ordered Zack Anderson, Alessandro Chiesa, and R.J. Ryan to provide him with a paper they wrote for a class at MIT and correspondence they had with the organizers of Defcon, a Las Vegas hacker convention where the students were slated to speak last Sunday on alleged security flaws in the MBTA's system.

The judge said he needed to know more to "enable me to make a sounder decision about the facts of the case." He ordered the students, who were not present, to provide the information by 4 p.m. today. He said he'll weigh all the facts, then hold another hearing Tuesday on whether to dismiss or extend the 10-day restraining order that was issued Saturday and prevented the students from giving their presentation at the convention.

The MBTA filed suit last week, alleging trespass and computer fraud by the students and negligence by the Massachusetts Institute of Technology after a vendor spotted promises of "free subway rides for life" on a website advertising the students' presentation.

After yesterday's hearing, Jennifer Granick, a San Francisco attorney who represents the students, dismissed those promises as "puffery" and said the students had used "florid language" to drum up interest in their presentation.

In court, Granick, who is civil liberties director of the Electronic Frontier Foundation in San Francisco, said the students have already provided "the entire universe of information," including material they never intended to release about security flaws, in a 30-page sealed document provided to the court earlier this week.

Granick argued that the restraining order is an unconstitutional gag order that has done "irreparable harm" to the students and the First Amendment. Granick said the students have acted responsibly and "never intended to release important information that would allow or teach a bad guy" to hack into the system.

MBTA spokesman Joe Pesaturo said the students have not provided the MBTA with enough information for officials to know whether the system's security is endangered. "We simply want them to provide the information that's been requested by the court or the MBTA," he said.

Ieuan G. Mahony, a Boston lawyer who is representing the MBTA, said after the hearing that some form of a restraining order is necessary until the agency has fixed any flaws that may exist.

The MBTA contends that the students had a responsibility to share their findings with agency officials before making them public so the agency would have time to fix the problems before they could be exploited, Mahony said.

After the hearing, Granick said the restraining order is "preventing them from talking about what they found, even though there's a public debate. If these students figured it out, other people could figure it out, too."

She said today's deadline would be difficult to meet because Anderson is not in the country and Ryan and

Chiesa are not in Boston. ■

© Copyright 2008 The New York Times Company

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

GLOBE EDITORIAL

The Boston Globe

Hacking and free speech

August 14, 2008

THREE MIT students claim to have identified ways of hacking the MBTA's automated fare-collection system, and they could have spared themselves some trouble had they notified the transit agency of any security flaws right away. The T found out about their work only after they made plans to describe their discoveries last Sunday at DEFCON, a conference for hackers. On Saturday, the agency persuaded US District Judge Douglas Wood-lock to issue a temporary restraining order against the undergrads.

But what the students should have done out of moral obligation and what they have the right to do under the First Amendment are two different questions. For good reason, US courts have long been highly skeptical of prior restraints on what may be said in a public forum. Woodlock strayed into dangerous territory by restricting what the students could disclose at the conference. At a hearing today, Judge George O'Toole will hear motions to modify or lift the order. He ought to lift it.

The order had its intended effect, for the students did not give their talk. But it would be a mistake to regard them merely as mischief-makers bent on helping scofflaws ride for free. Finding security breaches in electronic systems is a legitimate, even vital, line of inquiry. The students began looking into the T's CharlieCards and CharlieTickets in conjunction with an MIT class.

The T says it wants to enforce the principle of "responsible disclosure" - the notion that a security researcher who finds a flaw in an electronic system should notify the owner and give sufficient time to fix the breach before going public.

The students and T officials met for the first time about a week before DEFCON. The transit agency argues that the students did not offer enough information to judge whether they would behave responsibly at the conference. But should the T be the arbiter of what constitutes responsible disclosure? The students' lawyer says they met the standard, because they planned to withhold from their talk key information necessary to cheat the fare collection system.

In any case, responsible disclosure, while a valuable ethical standard, is not enshrined in federal statutes, and should not trump First Amendment rights. Such rights aren't absolute; if the students were to incite others to commit crimes, they could face civil and criminal penalties. But if expression can lead to penalties after the fact, that is one more reason not to block it in advance.

The MIT undergrads and others in this field surely need to learn that, even if they have a First Amendment right to disclose their work at their discretion, it doesn't mean they always should. But the MBTA should recognize that security flaws are a design problem, not a legal one. ■

© Copyright 2008 The New York Times Company

ABC NEWS

Leading Computer Scientists Defend Student Hackers

11 of the Country's Top Researchers Call Judge's Order 'Dangerous'

By KI MAE HEUSSNER

Aug. 14, 2008—

Eleven of the country's top computer scientists have come out in support of the three MIT students who were silenced by a gag order before they were able to tell a hackers conference in Las Vegas how they were able to break into Boston's subway fare collection system.

In an eight-page letter, the researchers argued that the injunction and others like it could have a "dangerous impact" on computer security research.

The temporary restraining order was meant to block discussion of how the students at the Massachusetts Institute of Technology figured out how to evade the computer system's security to change a $1.25 fare card to a $100 fare card.

In the letter filed Tuesday, the researchers, from leading institutions such as the University of California at Berkeley and Columbia University, urged the court to remove the restraining order issued against the students Sunday.

"We are concerned that the pall cast by the temporary restraining order will stifle research efforts and weaken academic computing research programs," the letter said. The students received an A on the project from their MIT professor.

"In this case, the law gives the public a false sense of security, achieved through law, not technical effectiveness," the letter also noted.

Despite the researchers' support, U.S. District Judge George O'Toole Jr. today left the injunction intact.

According to a spokeswoman for the Electronic Frontier Foundation, the civil liberties group defending the students, the judge did not uphold or remove the temporary restraining order. Instead, he postponed the decision to another hearing that will take place Tuesday.

The judge also asked the students to turn over more documentation on their research. By Friday afternoon, the students must hand over the class report that they submitted to their professor, part of the code that was intended to be part of their presentation and e-mail correspondence with organizers of the hacking conference.

The students and their lawyers said they are moving toward the judge's deadline but also plan to appeal the ruling to the U.S. 1st Circuit Court of Appeals.

"These restraints on the students' speech is flatly unconstitutional," said Rebecca Jeschke, a foundation spokeswoman.

Computer security experts say the attempt to gag the alleged hackers has boomeranged -- again.

"Every single time, harassing the researcher ends up spreading the research," said Dan Kaminsky, a computer security consultant for Seattle-based IOActive, Inc.

MIT students Zack Anderson, R.J. Ryan and Alessandro Chiesa were scheduled to present their "Anatomy of a Subway Hack" Sunday at Defcon, the popular Las Vegas hackers convention. Their trip to the podium, however, was blocked when they were served with an injunction obtained by the Massachusetts Bay Transportation Authority ordering them not to talk about the flaws in the MBTA security system.

But not only had the presentation already been distributed at the Defcon convention, it had been entered into public record when the MBTA filed its complaint. In the blink of a mouse click, the slides were posted on the Internet and hackers were shaking their heads at the MBTA's attempt to block discussion of the information.

"The bottom line is independent security research is how we get more secure networks," Kaminsky said. "But because anyone can just say anything, the way we differentiate what's true from what's not is to actually show the details that can be independently verified."

The students emphasize that their objectives were not to defraud the transit authority.

"Our intention & was to find out what vulnerabilities might be present and then determine how those might be fixed," Anderson told ABCNews.com.

Most importantly, he said, the students never planned to reveal the information that would actually permit others to hack the system. The slideshow and presentation did not include the key enabling information.

Anderson said they contacted transit authority officials in late July. The purpose of the meeting was to educate them about the system's flaws and present them with possible solutions.

Early last week, Anderson said, the students met with the transportation officials. After walking representatives through their presentation, the students thought they had allayed the transit authority's fears.

But Aug. 8, they were notified that a federal lawsuit had been filed against them.

"It was a huge shocker," said Anderson.

In a complaint filed Aug. 8 with a U.S. district court in Massachusetts, the transportation authority said the students did not provide it with ample time to address the system's weaknesses. As a result, public disclosure of the flaws could cause significant damage to the transit system.

In an e-mail, a spokesman for the MBTA told ABCNews.com that, at the meeting, the students agreed to provide the transit authority with a copy of the presentation. After several days passed without receiving the information, the MBTA said it had "no choice but to seek assistance from a federal court judge."

The MBTA said it is now "reviewing the information to determine if there is any degree of substance to the claims being made by the students."

Corynne McSherry, a staff attorney with the Electronic Frontier Foundation, said injunctions such as the one requested by the MBTA chill the conversations that protect consumers from computer security threats.

The Electronic Frontier Foundation, a nonprofit group that advocates for civil liberties in the digital world, is defending the three students. The group's lawyers contend that the court violated the students' First Amendment rights to discuss their research.

"The court stopped researchers from speaking about their research traditional academic research," she said. "[It] essentially decided that talking about security vulnerabilities was somehow forbidden."

Some legal experts have a different view.

"It's one thing, for academic purposes, to do research. It's something entirely different to actually carry it out," said Peter S. Vogel, an attorney with the Dallas office of Gardere Wynne Sewell who specializes in Internet security and e-commerce. He is also an adjunct professor at the Southern Methodist University Dedman Law School.

If transit authority lawyers presented compelling evidence that the students violated state or federal laws while conducting their research, the judge would have been obligated to grant the injunction, Vogel added.

"The First Amendment doesn't protect people from breaking the law. It's a fine line to draw between violating a law and freedom of speech," Vogel said.

Copyright © 2008 ABC News Internet Ventures

MIT students must turn in CharlieCard data today

By Marie Szaniszlo | Friday, August 15, 2008 | http://www.bostonherald.com | Local Coverage

The lawyer for three MIT students, who say the CharlieCard - the MBTA's automated fare collection system - is vulnerable to hackers, has until this afternoon to hand over documents detailing their claim.

U.S. District Court Judge George O'Toole Jr. gave lawyer Jennifer Stisa Granick until 4 p.m. to turn over a paper the students wrote on the topic for a class, as well as any materials they had been planning to distribute last Sunday at a hackers conference and any communication they had with conference organizers.

Stisa Granick said she had already submitted a sealed document - open only to the students, the MBTA, MIT, their lawyers and O'Toole - containing everything the students know about the CharlieCard.

Last Saturday, MBTA lawyers obtained a 10-day restraining order barring undergraduates Zack Anderson, R.J. Ryan and Allessandro Chiesa from speaking at the Las Vegas conference.

The MBTA argued their presentation could jeopardize the CharlieCard's security.



Photo by Herald (file)

But Stisa Granick said, "The question of whether the system works is a critical part of the public debate."

Article URL: http://www.bostonherald.com/news/regional/general/view.bg?articleid=1113095

Related Articles:

MBTA worker nabbed in 'drop-box' scheme
/news/regional/general/view.bg?articleid=1113522

Critics rail over MBTA raises
/news/regional/politics/view.bg?articleid=1113247

Building program's schools for scandal
/news/opinion/editorials/view.bg?articleid=1113064

Contact us | Print advertising | Online advertising | Herald history | News tips | Electronic edition | Browser upgrade | Home delivery | Herald wireless

$ave on Boston Herald Home Delivery

Jobs with Herald Media

For back copy information and more information on other collectible copies please call 617-426-3000 Ext. 7714. Click here for Celtics, Patriots and Red Sox back copies

© Copyright by the Boston Herald and Herald Media.
No portion of BostonHerald.com or its content may be reproduced without the owner's written permission. Privacy Commitment

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

Missed opportunity on MBTA security

The Boston Globe

August 16, 2008

IT'S SURPRISING to see the MBTA's actions concerning the MIT student project concerning Charlie Card security ("T sues 3 students before hacker show," City & Region, Aug. 10). This is very unlike Dan Grabauskas; I can only guess he was browbeaten by his legal staff into wielding a sledgehammer here.

Grabauskas has long been a competent, out-of-the-box state official. He has a shining track record for fixing what's broken in state agencies, often with the most innovative of solutions.

What I would have expected is Grabauskas to form some kind of team or partnership with the students, praising MIT for its students' contributions to the betterment of the Commonwealth, and reaping their undoubted expertise. Instead, it seems like both an operational and promotional opportunity missed.

ROBERT CARON
Northborough ■

© Copyright 2008 The New York Times Company

boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

HARVEY SILVERGLATE

The Boston Globe

National security and free speech

By Harvey Silverglate | August 16, 2008

WHY DID the federal district court gag three MIT undergraduates who apparently discovered a flaw in the MBTA's electronic fare-collection system? The reason one judge imposed the unconstitutional gag order prohibiting the students from presenting their paper Aug. 10 at the DEFCON computer "hackers" conference, and another judge refused on Aug. 14 to vacate that order even after the conference ended, is the current excuse du jour for an epidemic of censorship: national security.

The students, as a project for their class in computer security, discussed how the CharlieCard could be decoded and used to obtain free T rides. When the MBTA learned that they were going to present their paper at DEFCON, it sought a temporary restraining order. Judge Douglas Woodlock, sitting as emergency "duty judge," granted the T's request and prohibited the presentation -- a clearly unconstitutional decision -- citing a violation of the federal Computer Fraud and Abuse Act. Even after a follow-up Aug. 14 hearing before Judge George O'Toole, the order stands.

The Computer Fraud and Abuse Act almost certainly does not apply to mere speech; rather, it covers someone who "knowingly causes the transmission of a program, information, code, or command to a computer or computer system." In other words, the statute outlaws hacking, not a scholarly (or even unscholarly) presentation. And even if the statute could be twisted to cover the DEFCON presentation, the First Amendment's free speech guarantee would render this use unconstitutional. Yet Woodlock issued a patently unconstitutional order. Why?

This bizarre court intervention is rooted, as are many other recent civil liberties violations, in the aftermath of the Sept. 11, 2001, terrorist attacks. The MBTA's court complaint highlights "the role of the MBTA in Homeland Security efforts" and claims that the hacking threat "affects a computer system used by a government entity for national security purposes." A supporting affidavit of MBTA personnel adds that "in 2007 the MBTA received $4 million from the Department of Homeland Security . . . for use in emergency communications initiatives." Thus the T, in reality just another local transit system struggling under crushing debt and long-term mismanagement, transmogrified a temporary threat to its fare collection system into something so urgent as to override the First Amendment.

The MBTA's motion for a gag order was heard by Woodlock. Four years ago, the judge penned an opinion when civil libertarians and political activists challenged Draconian security measures aimed at severely limiting demonstrations at the 2004 Democratic National Convention in Boston. While characterizing the chicken-coop-like "free speech zone" into which protesters were to be herded outside the Fleet Center as akin to "an internment camp," Woodlock said that it was "irretrievably sad" that post-Sept. 11 security threats made such tight restrictions on otherwise protected activity necessary. "One cannot conceive of other elements [that could be] put in place to create a space that's more of an affront to the idea of free expression than the designated demonstration zone," Woodlock moaned as he facilitated the affront.

The convention security issues were, admittedly real, even if the solution was unnecessarily harsh on free speech. But the possibility of real or merely feared -- but in any event temporary -- revenue losses for the T should not qualify as the kind of extraordinary and irreparable threat that can justify a restraining order. The Supreme Court has not had occasion -- yet -- to change that high legal barrier, but some lower federal courts have nonetheless since 9/11 been setting a lower bar for the censors.

Ironically, this constitutional violation is for naught, since the order will not stop other bright minds from making the same discovery. Knowledge and its spread, for both constitutional and practical reasons, are not subject to court injunctions. The MBTA would have been better off hiring, rather than suing, the MIT trio to solve the electronic flaw. The students (and their professor) could doubtless do a better job of patching the security hole than the T's security officials, consultants, and vendors who designed the vulnerable system. But with the

ghosts of 9/11 and "national security" hovering, the students and the First Amendment didn't stand a chance.

Harvey Silverglate is a criminal defense and civil liberties litigator and writer. ■

© Copyright 2008 The New York Times Company

THE CHRISTIAN SCIENCE MONITOR

PRINTTHIS

Not so smart cards easily hacked

MIT students hack into Boston's transit system, highlighting security flaws in mass-transit cards.

By Ben Arnoldy – | *Staff writer of The Christian Science Monitor*
and Uri Friedman – | *Contributor to The Christian Science Monitor*
from the August 18, 2008 edition

Oakland, Calif.; and Boston - The recent hacking into Boston's mass transit system by three local university students underscores a much broader problem: More than a billion mass-transit fare cards and door-swipe badges worldwide have a security weakness.

That's due to a flaw revealed in a smart chip's design earlier this year. Other agencies that use the chip – from the London Tube to the Dutch government – have scrambled to adopt temporary countermeasures, says Karsten Nohl, the researcher who first uncovered the trouble. All their smart cards, he says, need to be shored up or replaced.

Three Massachusetts Institute of Technology students drove home this and other weaknesses in Boston's transit system when they claimed to have found a way to add money onto fare cards free of charge.

For now, a restraining order taken out by the Massachusetts Bay Transportation Authority (MBTA) stops the students from publicizing their work. But details are already leaking out. And their exploits come less than a year after Mr. Nohl's research had already pointed down one path to hacking such systems.

That's leaving some security experts to question the MBTA's efforts to maintain security through secrecy. "I'll predict for you that within a couple of months someone will reproduce the attack, whether or not the details were released," says Mike Davis, a senior security consultant with IOActive in San Francisco. "What these new hard-core attacks are starting to show us is that the obscurity we relied on to protect these systems are just assumptions people have made."

The MBTA spent $192 million upgrading its fare collection system in 2006, and picked a smart card system with the "Mifare Classic" chip. Mr. Nohl, now finishing his PhD at the University of Virginia,

showed in December that this chip relied on a quickly crackable cipher whose only real strength turned out to be its secrecy.

"Now [MBTA officials] are trying to decide whether they should again replace everything with a third technology, or seek alternative means to combat fraud – one of which is to sue researchers," says Nohl.

Others have responded differently, he adds. London Tube officials developed a stopgap that could protect them until an upgrade becomes available. The Dutch government has dispatched security guards at key doorways once guarded only by smart cards using that technology.

However, only Boston's system has actually suffered a public hack.

Doing MBTA a good turn?

The MBTA cannot be sure that its security system is vulnerable until it has more detailed information from the MIT students, such as the report they submitted to their professor and the computer code they planned to reveal earlier this month at the DefCon hacker conference in Las Vegas, according to MBTA spokeswoman Lydia Rivera.

"If we get additional information, then we can actually make an informed and responsible decision on whether in fact their findings have merit," she says. "These students, along with the MIT staff and teachers overseeing them, have a responsibility to the public to share the information [with us] prior to making the information public or trying to make it public."

The students found flaws not included in Nohl's research and developed ways to add hundreds of dollars onto both the MBTA's new smart cards and its older-style paper tickets with magnetic strips.

As security researchers, they feel they are contributing to the public welfare by exposing critical vulnerabilities in the transit system. Transit authorities assessing their computerized systems need to sweat the details, says Zack Anderson, one of the students involved in the project.

"There are a lot of small intricacies that, if not done correctly, could result in systemwide failure," he says. "Some of the issues sometimes come down to fundamental mathematical errors like cryptography algorithms. That wouldn't be the MBTA's fault or the system integrator's fault. That would be the [fault of the] vender who sells the technology."

Mr. Anderson says the students did approach the MBTA about their findings before the conference.

Another court hearing takes place Tuesday, and researchers are warning that if the lawsuit succeeds it will poison future cooperation. "I think hackers will keep hacking, but they won't do responsible disclosure anymore," says Nohl.

Despite the legal wrangling, the cat is almost out of the bag anyway. A slide show presentation the students planned on giving at DefCon has already hit the Internet, even though they canceled the speech.

Back in March, newspapers including The Boston Globe and the Boston Herald widely publicized Nohl's findings.

MBTA's Ms. Rivera says she does not recollect those reports.

Nohl says the MBTA was aware of the vulnerabilities he outlined and that they considered implementing additional security measures. He adds that his Dutch colleagues will be publishing more explicit research on the chip's weakness in October.

"Once that paper is published, everybody can easily copy cards," he says.

John von Goeler at Scheidt & Bachmann, the system integrator for many US public transit systems including Boston's T, declined to comment.

Older system was weaker

Still, transit fare systems that don't use smart cards are often even weaker. Older-style subway tickets with magnetic stripes usually have no encryption, but they also tend to store value in a central computer rather than on the cards themselves. New York City's MetroCard doesn't even have that security.

"The monetary value of the card itself [is] stored on the magnetic stripe," says Joseph Battaglia, an electrical engineer who mapped most of the data fields on the MetroCard. "If a criminal wanted to proceed to continue the reverse-engineering effort in order to create their own cards, there would be absolutely nothing preventing them."

Nor is encryption used for highway toll collection, according to Nate Lawson, founder of the Oakland-based security consultancy Root Labs. He discovered that the Bay Area's FasTrak transponders could be tampered with remotely, even by people in nearby cars.

Adding encryption increases the costs. The MBTA could have chosen smart cards with strong cryptography, says Mr. Lawson, but since the fare cards are given out free of charge, the MBTA saved money upfront by choosing the much cheaper Mifare Classic chips.

The danger for weak systems like the MBTA's is that "somebody will take the attack and package it nicely," says Lawson.

Such systems can be sold to criminals who can then use it to churn out bogus cards to sell on the street. "Once it hits that level, that's when it costs the transit company a lot of money."

Find this article at:
http://www.csmonitor.com/2008/0819/p01s01-usgn.html

Check the box to include the list of links referenced in the article.

www.csmonitor.com | Copyright © 2008 The Christian Science Monitor. All rights reserved.