Hacking in the Name of Science

Tadayoshi (Yoshi) Kohno (University of Washington)
Jon Callas (PGP Corporation)
Alexei Czeskis (University of Washington)
Daniel Halperin (University of Washington)
Karl Koscher (University of Washington)
Michael Piatek (University of Washington)

DEFCON 16 - August 8, 2008

Who We Are

- Researchers at the University of Washington
  - Tadayoshi Kohno, http://www.cs.washington.edu/homes/yoshi/
  - Alexei Czeskis,http://www.cs.washington.edu/homes/aczeskis/
  - Daniel Halperin, http://www.cs.washington.edu/homes/dhalperi/
  - Karl Koscher, http://www.cs.washington.edu/homes/supersat/
  - Mike Piatek, http://www.cs.washington.edu/homes/piatek/
- Co-founder of PGP Corporation
  - Jon Callas, jon@callas.org

Focus for Today

Explore "**hacking**" in the **academic community**

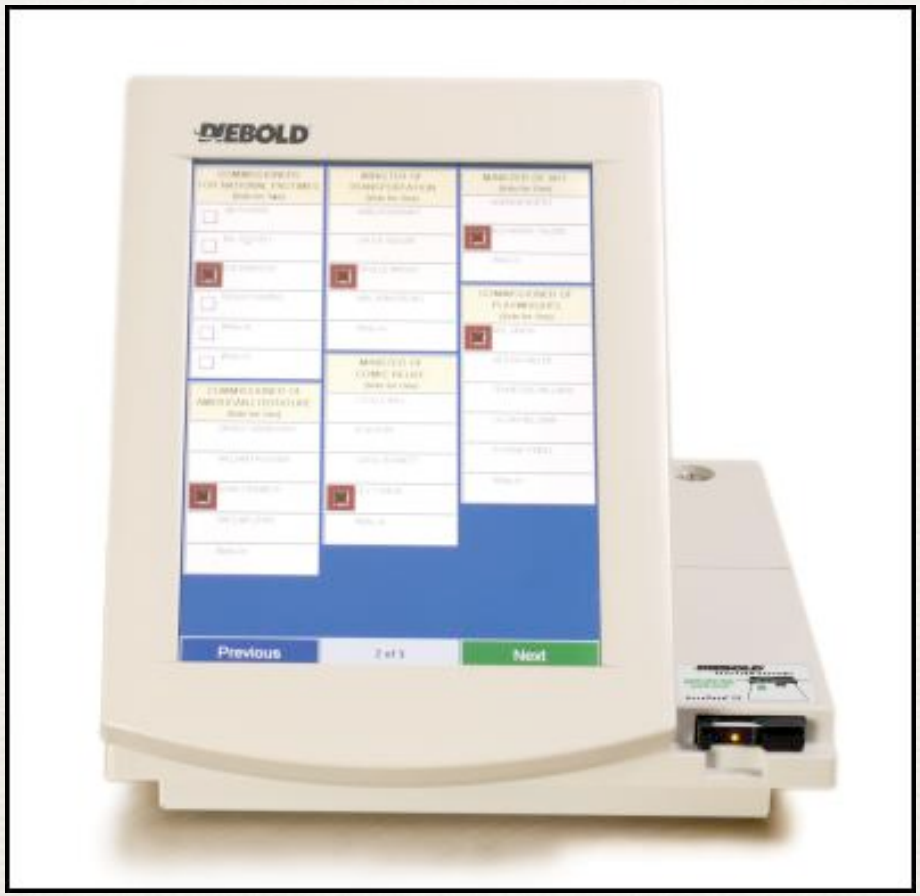
We call this line of work many things, like "**attacks research**" or "**measurements**," but **never** "**hacking**"

For concreteness, we base this talk on our own research (often in collaboration with others)

About Yoshi

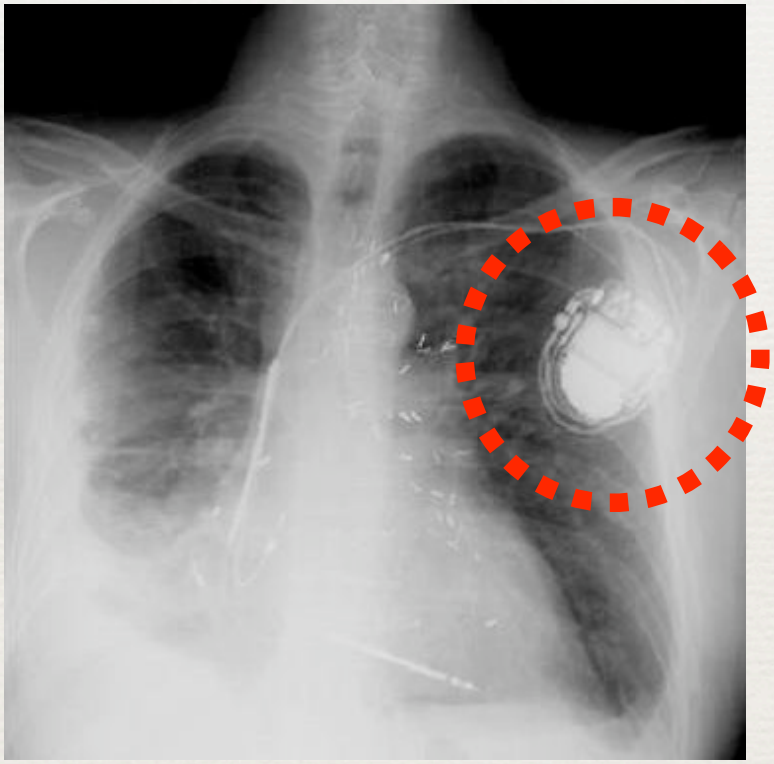
- Others will introduce themselves when they first start
- Ph.D. from University of California San Diego
  - Lots of crypto / mathy stuff
  - But also lots of work on analyzing real systems -- and that's the focus of today's talk
- Past industry work: Bruce Schneier's old company, and Cigital
- Now: Faculty at the University of Washington

Previews for Today



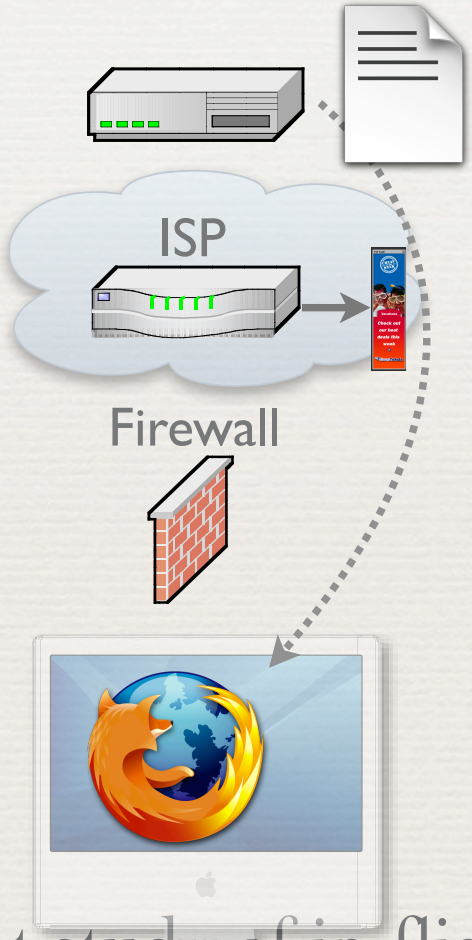
First public analysis of **Diebold**'s AccuVote-TS **e-voting** source code (2003, Kohno, Stubblefield, Rubin, Wallach)

Previews for Today



First public analysis of a common **wireless** implantable **medical device** (2008, Halperin, Heydt-Benjamin, Ransford, Clark, Defend, Morgan, Fu, Kohno, Maisel)

Previews for Today





Measurement study of in-flight **changes to web pages by ISPs** and others (2008, Reis, Gribble, Kohno, Weaver)

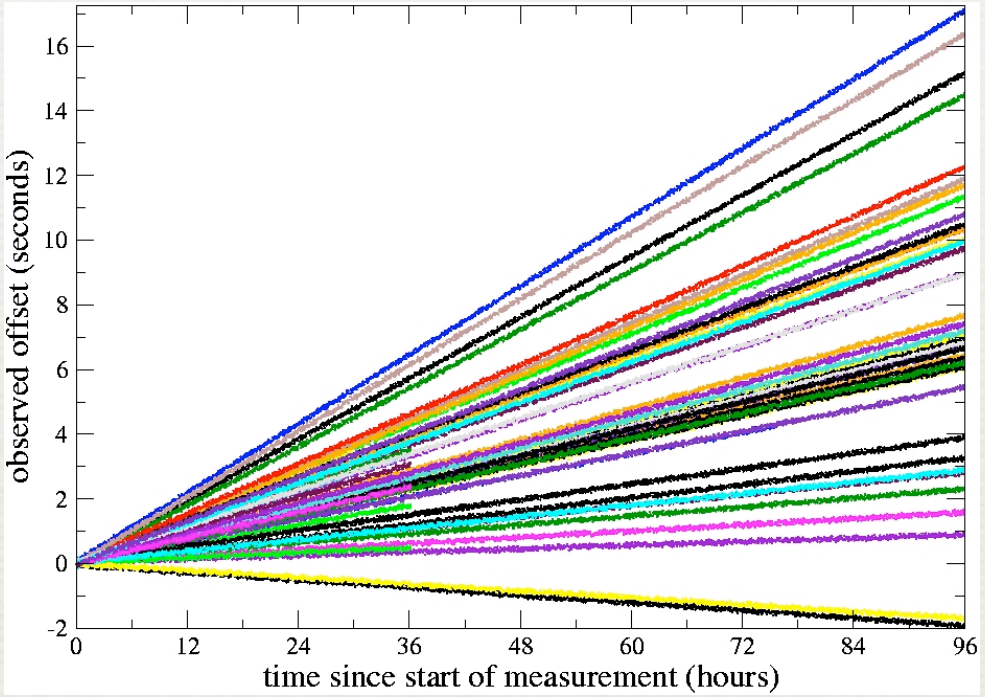
Previews for Today



Measurement study of **DMCA notices** in BitTorrent (2008, Piatek, Krishnamurthy, Kohno)

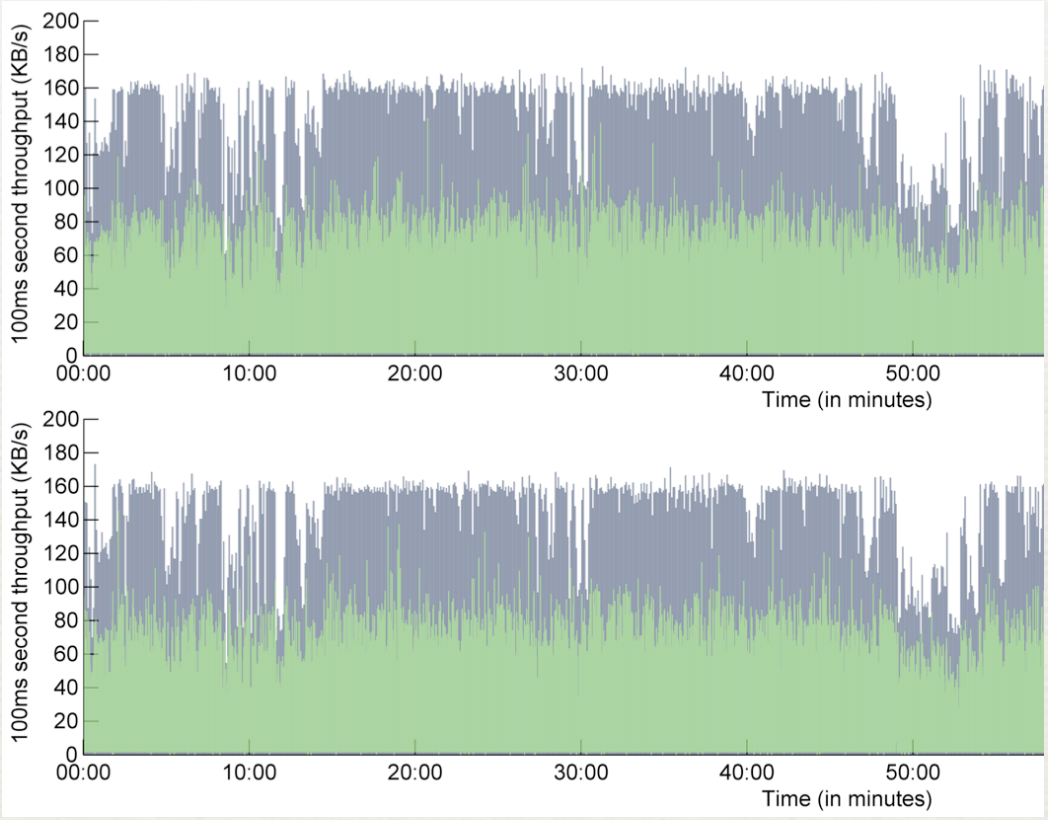
Previews for Today





Fingerprinting physical machines based on information leakage and **clock skew** (2005,Kohno, Broido, and Claffy)

Previews for Today



Information leakage and **encrypted** streaming multimedia: the case of the Slingbox Pro (2007, Saponas, Lester, Hartung, Agarwal, and Kohno)

Previews for Today

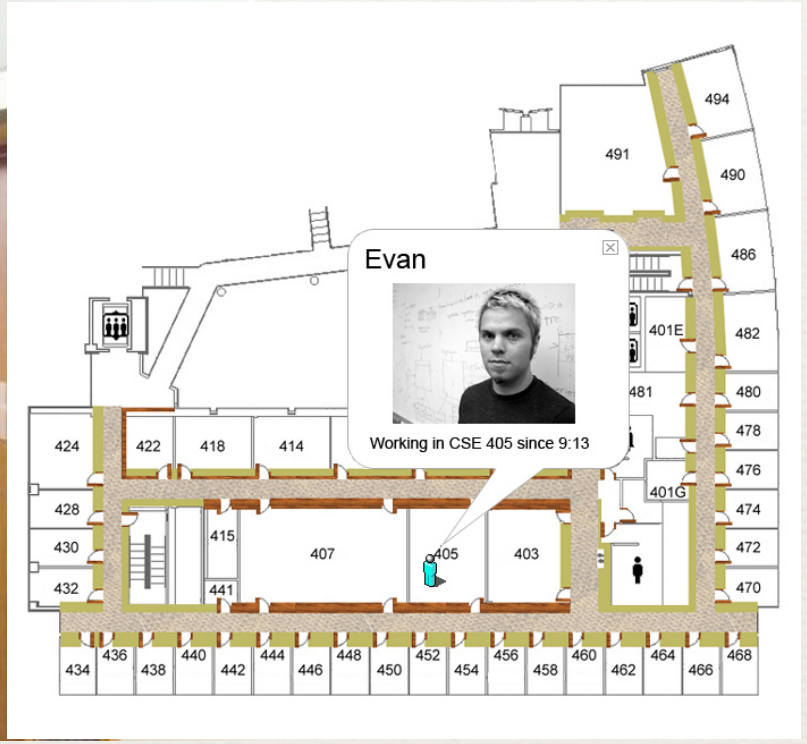


Contents of a "hidden" file

Information leakage and **deniable filesystems** like TrueCrypt (2008, Czeskis, St. Hilaire, Koscher, Gribble, Kohno, and Schneier)

Previews for Today





Exploring privacy in a **future world** with ubiquitous surveillance (the UW RFID Ecosystem team)

Previews for Today

Inside the Twisted Mind of the Security Professional

WIRED

Bruce Schneier ✉ 03.20.08

Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and t
ants. My friend expressed surprise th
in the mail.

I replied: "What's really interesting is
tube of live ants to anyone you tell th

Security requires a particular mindse
least the good ones -- see the world d

Which is why CSE 484, an undergraduate computer-security course taught this quarter at the University of Washington, is so interesting to watch. Professor Tadayoshi Kohno is trying to teach a security mindset.

You can see the results in the blog the students are keeping. They're encouraged to post security reviews about random things: smart pill boxes, Quiet Care Elder Care monitors, Apple's Time Capsule, GM's OnStar, traffic lights, safe deposit boxes, and dorm -room security.

The most recent one is about an automobile dealership. The poster

Developing the "**Security Mindset**" in a **University of Washington undergraduate** computer security **course**

Previews for Today

Why is this **science** and not just **hacking**?

Previews for Today

The Industry Perspective

Previews for Today

Your Turn! Let's discuss!

What can academics learn from you?
What do you think we could do better?
What would you like us to look at next?
What **shouldn't** we be doing?
Who/What/When/Where/Why/How <you fill in>?

We Build Too!

We **build** secure systems too!

But the focus of **this talk** is on "**academic security analyses**," so **we omit many projects**

Visit our websites if you are interested!

Part 1: “Our Hacks”

Background

- **The academic model**
  - We experiment with technologies
    - Analyze existing ones
    - Build new ones
  - But we also need to **publish our results in peer-reviewed venues** (conferences, journals)
- **As scientists, we seek to learn new things about and improve our world**, and our approaches must be rigorous

Background

- We provide links to our papers in subsequent slides
- If you'd like more detailed examples of what an academic paper looks like, please follow these links
- We will highlight some critical properties of academic security research

Type A: Analyzing Critical Systems

Properties of these projects

- Focus on **critical systems** that are **important** to people and **society**
- Often **previously understudied** technologies / applications of technologies
  - At least not studied by the public
- Papers must have **lessons** and/or **bigger picture implications -- not just attacks**
  - Academic community generally frowns on papers that *only* break a system

Properties of these projects

- Results can have broad-reaching affects, to public policy, legislation, and so on
- Papers also often include discussions of **possible defenses**

Analysis of an electronic voting machine

Tadayoshi (Yoshi) Kohno (University of Washington)
Adam Stubblefield (Johns Hopkins University and ISE)
Aviel D. Rubin (Johns Hopkins University and ISE)
Dan S. Wallach (Rice University)

IEEE Symposium on Security and Privacy, 2004
(Previously JHU ISI Technical Report, 2003)

http://www.cs.washington.edu/homes/yoshi/papers/eVoting/vote.pdf

Cornerstone of Democracy

- Voting is cornerstone of our democracy
- Allows us to influence
  - Crime prevention
  - Healthcare
  - Education
  - Foreign policy…
- U.S. citizens have fought hard for their right to vote

Presidential Election, 2000







Palm Beach County, FL



The FUTURE!

Case of the Diebold FTP Site

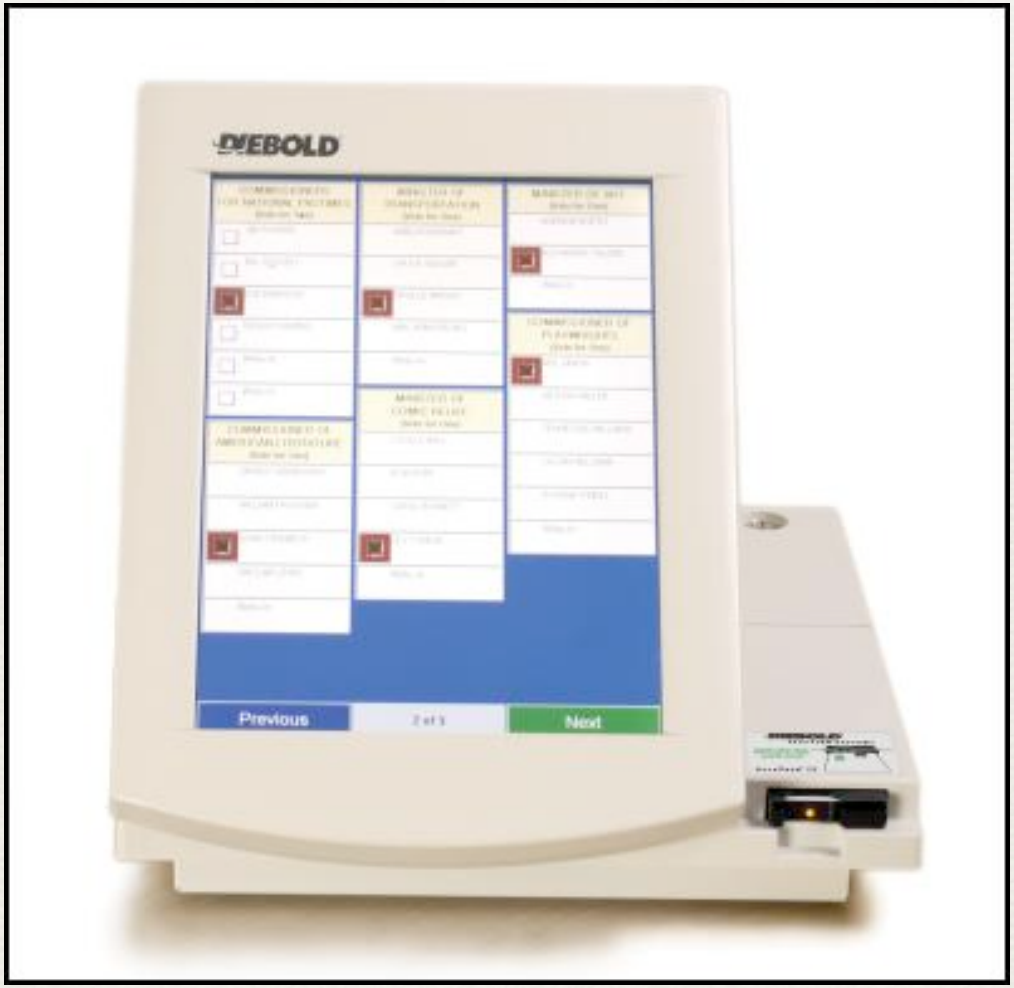
- Pre-2003
  - Some computer scientists concerned about e-voting security
  - But impossible for public to analyze
- 2003
  - Diebold source code posted on anonymous ftp site
  - Bev Harris found in January 2003
  - CVS repository from 10/2000 to 4/2002
  - First opportunity to publicly analyze source code of real e-voting machine

New Opportunity

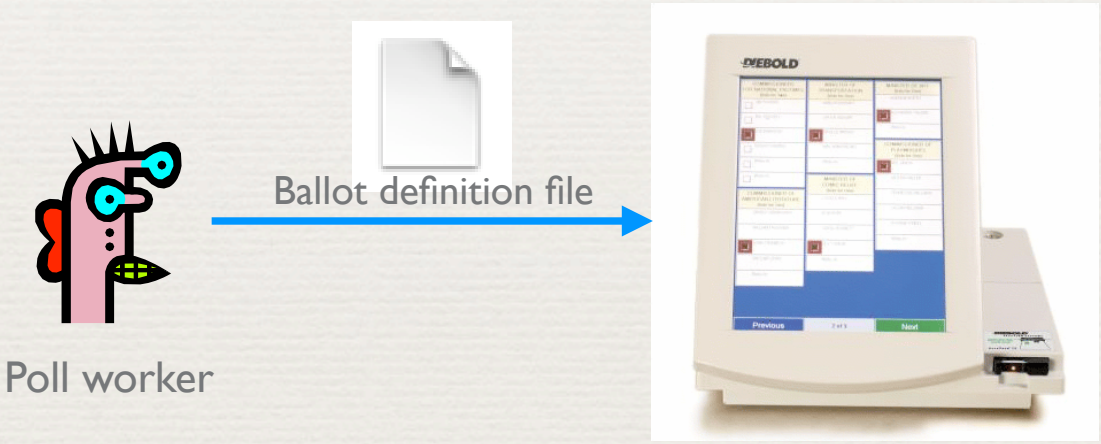
- New opportunity to analyze critical software
- We analyzed Diebold's AccuVote-TS version 4.3.1 source code.
- In many ways, computer scientists "worst nightmares" were true

Step 1: Determine How System Works

System Overview

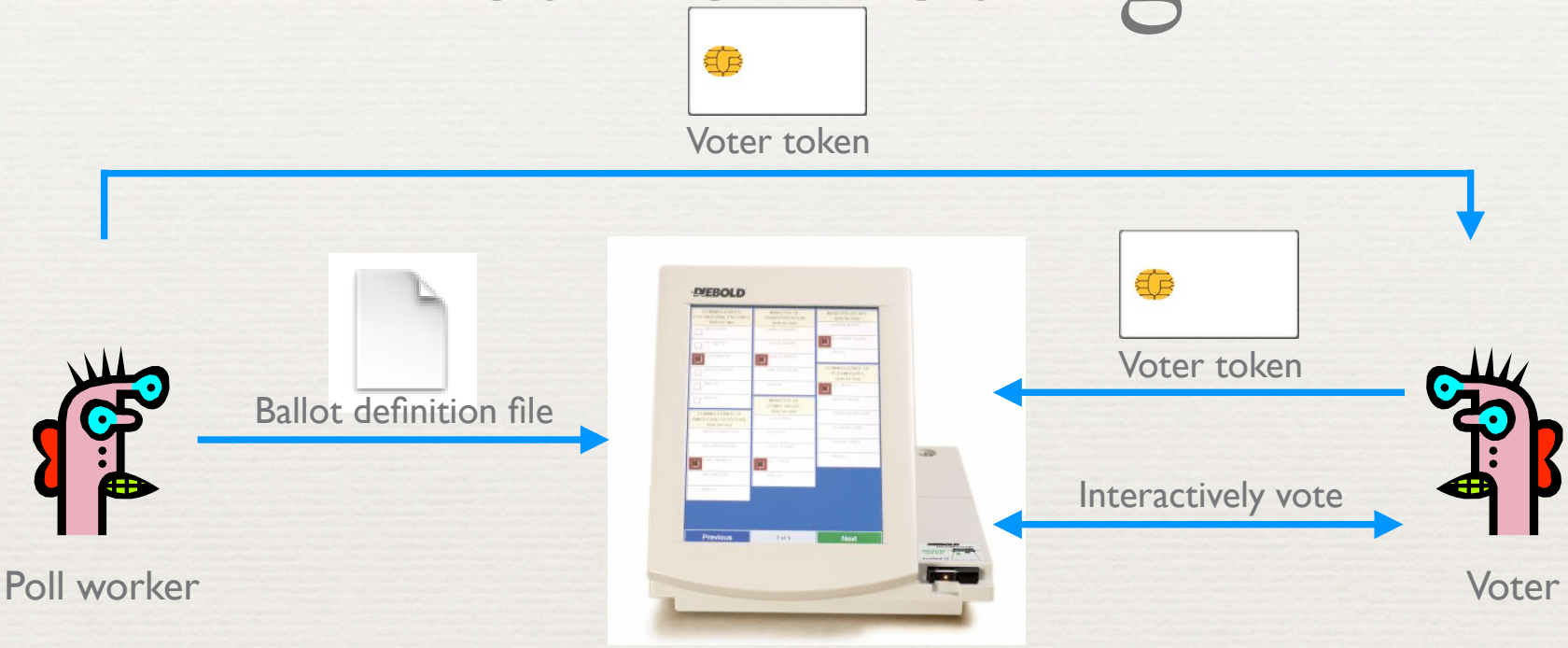


Pre-Election



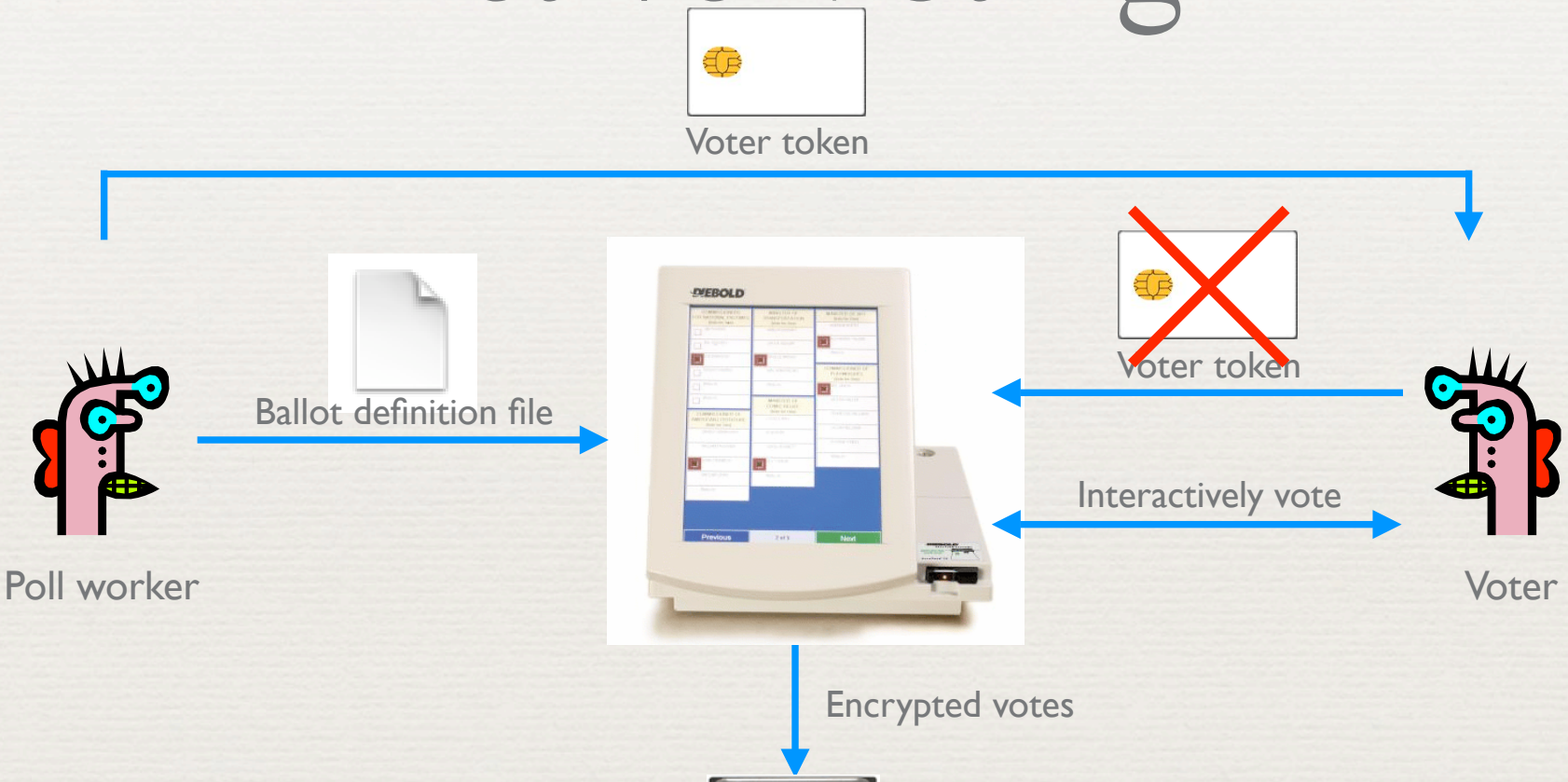
Pre-election: Poll workers load "ballot definition files" on voting machine.

Active Voting



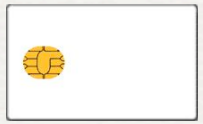
Active voting: Voters obtain single-use tokens from poll workers. Voters use tokens to active machines and vote.

Active Voting



Active voting: Votes encrypted and stored. Voter token canceled.

Post-Election



Voter token



Voter token

Ballot definition file



Interactively vote

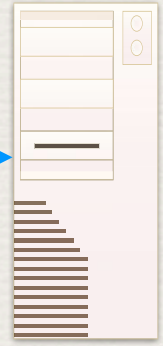
Poll worker

Voter

Encrypted votes



Recorded votes

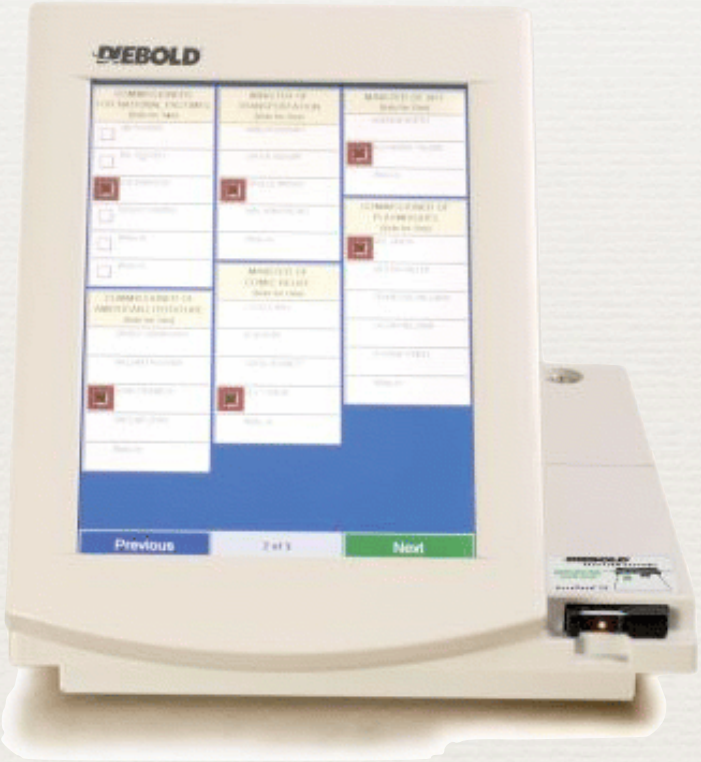


Tabulator

Post-election: Stored votes transported to tabulation center.

Step 2: Analyze Security and Privacy Under Different Threat Models

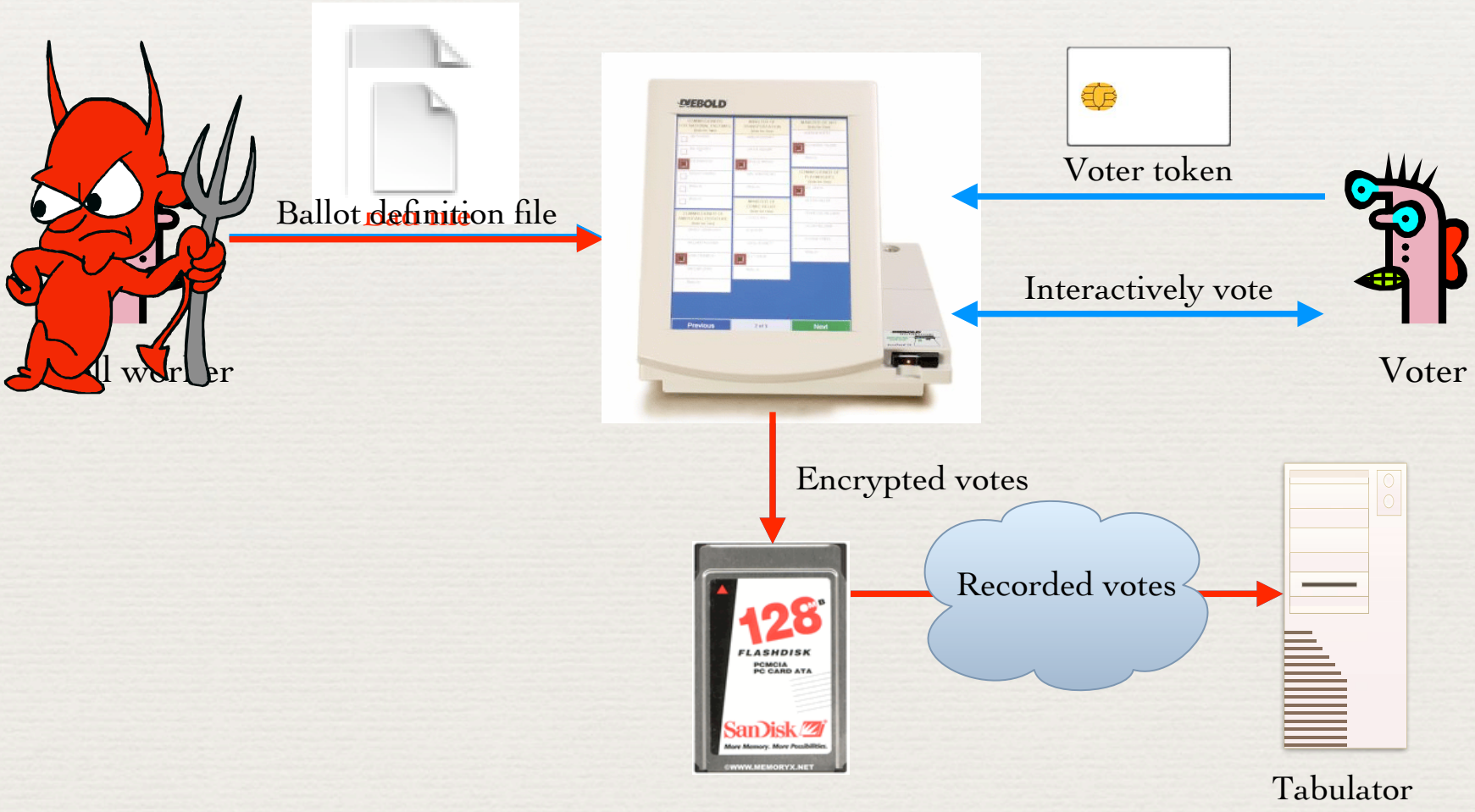
What Software is Running?



Problem: An adversary (e.g., a poll worker, software developer, or company representative) able to control the software or the underlying hardware could do whatever he or she wanted.

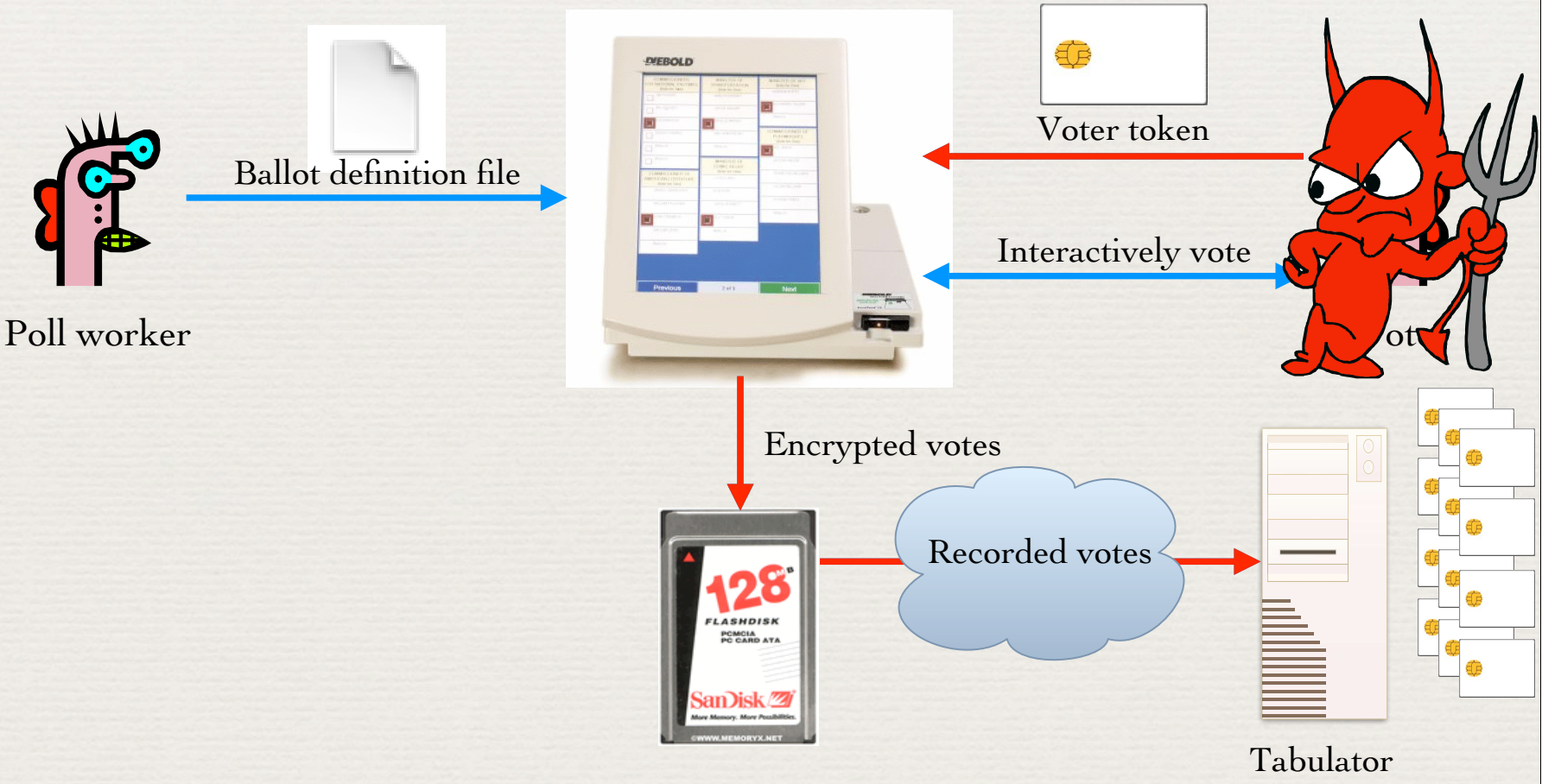
Problem: Ballot definition files are not authenticated.

Example attack: A malicious poll worker could modify ballot definition files so that votes cast for "Mickey Mouse" are recorded for "Donald Duck."



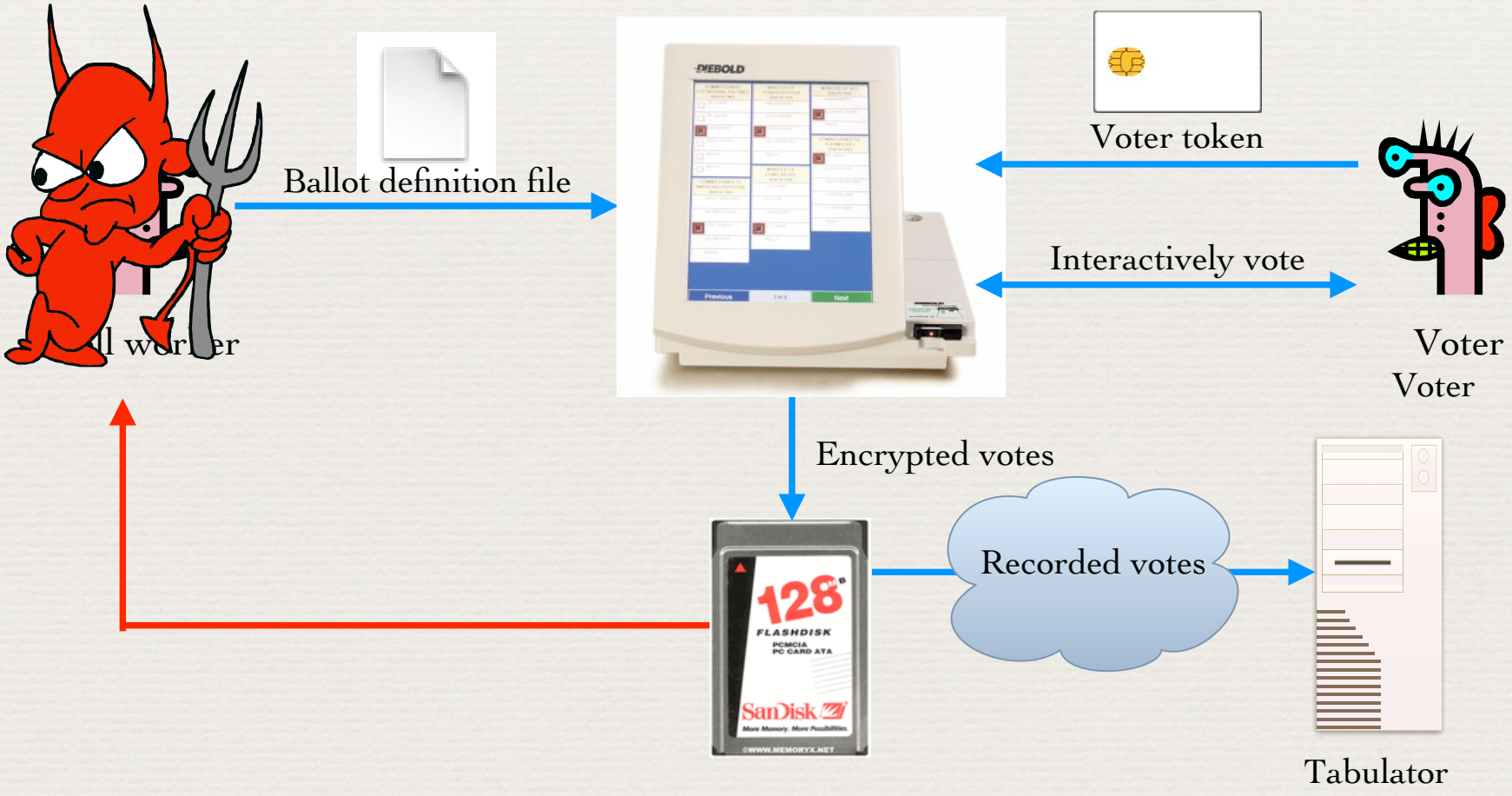
Problem: Smartcards can perform cryptographic operations. But there is no authentication from voter token to terminal.

Example attack: A regular voter could make his or her own voter token and vote multiple times.



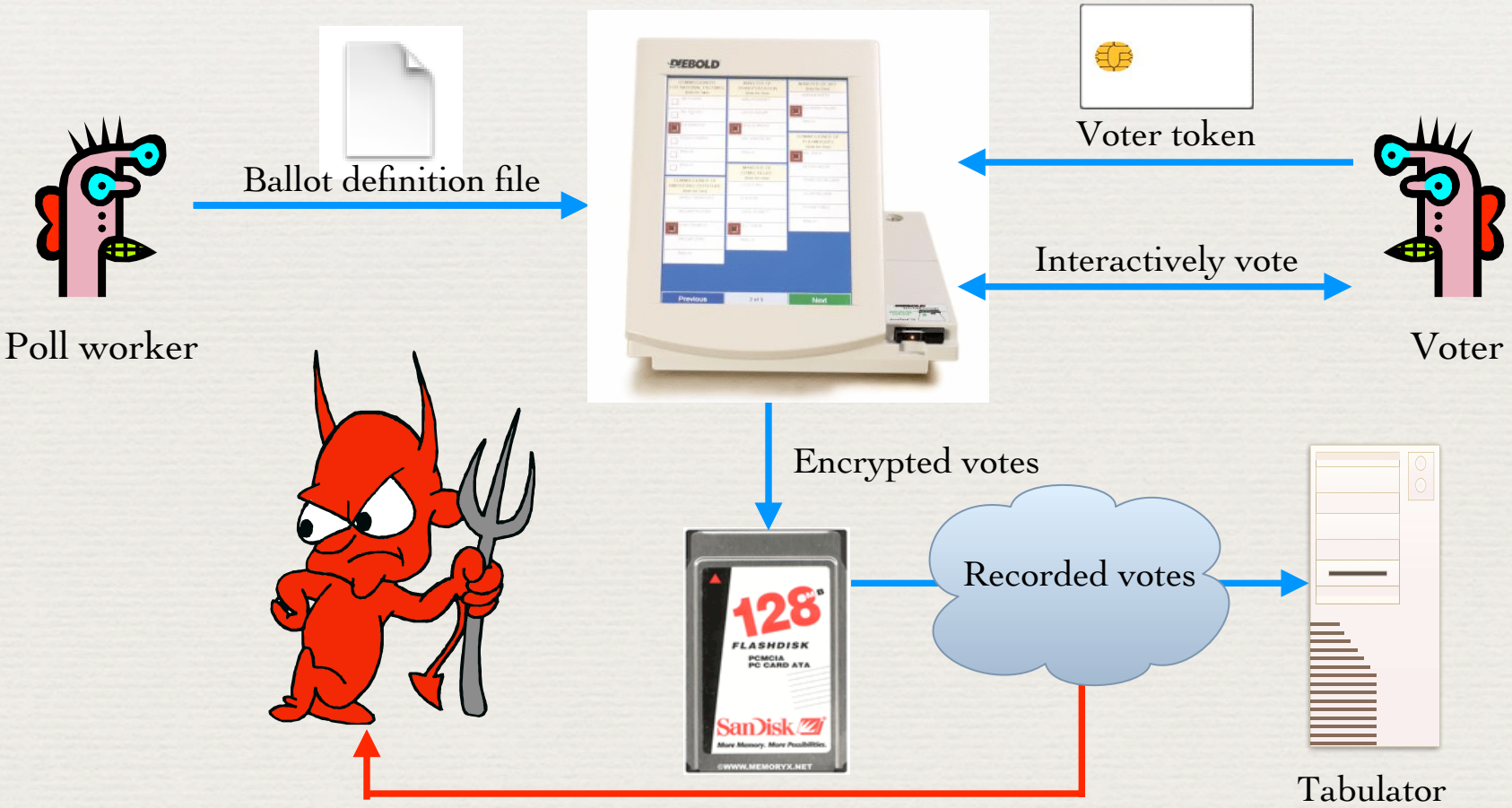
Problem: Encryption key ("F2654hD4") hard-coded into the software since (at least) 1998. Votes stored in the order cast.

Example attack: A poll worker could determine how voters vote.



Problem: When votes transmitted to tabulator over the Internet or a dialup connection, they are decrypted first; the cleartext results are sent the the tabulator.

Example attack: A sophisticated outsider could determine how votes vote.



Software Development

/* This is a bit of a hack for now. */

AudioPlayer.cpp

/* the BOOL beeped flag is a hack so we don't beep twice. This is really a result of the key handling being gorped. */

WriteIn.cpp

/* the way we deal with audio here is a gross hack. */

BallotSelDlg.cpp

/* need to work on exception *caused by audio*. I think they will currently result in double-fault.*/

BallotDlg.cpp

Example Reactions

"The correctness of the software has been proven through an extensive testing process."

"These machines have never been attacked in the past, so we know that they won't be attacked in the future."

"Not having security mechanisms built into the software is OK since election procedures would detect any malicious activity."

"The code we analyzed was old and that our results no longer apply."

News Clips (Other Machines)

"School Board member Rita S. Thompson (R), who lost a close race to retain her at-large seat, said yesterday that the new computers might have taken votes from her. … County officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for Thompson in about 'one out of a hundred tries.'" – David Cho, *The Washington Post*, November 6, 2003. [WINvote]

"Six electronic voting machines used in two North Carolina counties lost 436 ballots cast in early voting for the 2002 general election because of a software problem." – Kim Zetter, *Wired News*, February 9, 2003. [iVotronic]

News Clips (Other Machines)

"[A]n e-voting glitch in Boone County [Indiana] showed that 144,000 votes had been cast – an impossibility since the county had only 19,000 total registered voters, according to The Indianapolis Star. A corrected count by the clerk showed just 5,352 ballots were cast. 'I about had a heart attack,' County Clerk Lisa Garofolo told the newspaper about the problem, which she attributed to a 'glitch' in the software provided by MicroVote." – Cynthia L. Webb, *The Washington Post*, November 13, 2003.

Step 3: Follow Through

Toward Better E-Voting

- **Identify, study, and address challenges** to designing better e-voting machines
  - Usability
  - Cost
  - What does "secure" mean?
- **Active research area**
  - $5M NSF center for voting research
  - New EVT workshop
  - Lots of papers
- **Working with other communities** (not just computer scientists)

Example Subsequent Analyses

- Our report (July 2003)
- SAIC report (September 2003)
  - "The system, as implemented in policy, procedure, and technology, is at high risk of compromise."
- RABA report (January 2004)
  - "The State of Maryland election system (comprising technical, operation, and procedural components), as configured at the time of this report, contains considerable security risks that can cause moderate to severe disruption in an election."
- RABA had access to Diebold machines and implemented some of our attacks.
- More since then

New Paper Requirements

State	Law/Regulation	Summary	Date Enacted
Alaska	Alaska Statutes § 15.15.032	The director shall provide for a paper record of each electronically generated ballot that can be reviewed and corrected by the voter at the time the vote is cast and used for a recount of the votes cast at an election in which electronically generated ballots were used.	7/4/04
Arizona	SB1557	An electronic voting system shall provide a durable paper document or ballot that visually indicates the voter's selections, that the voter may use to verify the voter's choices, that may be spoiled by the voter if it fails to reflect the voter's choices and that permits the voter to cast a new ballot. This paper document shall be used in manual audits and recounts.	6/28/06
Arkansas	Act 654	If the machine is a direct read electronic voting machine, it shall include a voter verified paper audit trail.	3/9/05
California	California Elections Code § 19250a	On and after January 1, 2005, the Secretary of State shall not approve a direct electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail.	9/27/04
California	Secretary of State press release	Secretary of State Kevin Shelley approves Sequoia voting machines with VeriVote printers.	1/21/04
Colorado	Colorado Revised Statutes § 1-5-801(1)	On and after June 6, 2005, a political subdivision shall not acquire a voting system unless the voting system is capable of producing a voter-verified paper record of each elector's vote.	6/6/05

http://www.electionline.org/Default.aspx?tabid=290

Pacemaker and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defense

Daniel Halperin (University of Washington)
Thomas S. Heydt-Benjamin (UMass Amherst)
Benjamin Ransford (UMass Amherst)
Shane S. Clark (UMass Amherst)
Benessa Defend (UMass Amherst)
Will Morgan (UMass Amherst)
Kevin Fu (UMass Amherst)
Tadayoshi (Yoshi) Kohno (University of Washington)
William H. Maisel (BIDMC and Harvard Medical School)

IEEE Symposium on Security and Privacy, 2008

http://www.secure-medicine.org/icd-study/icd-study.pdf

About Dan

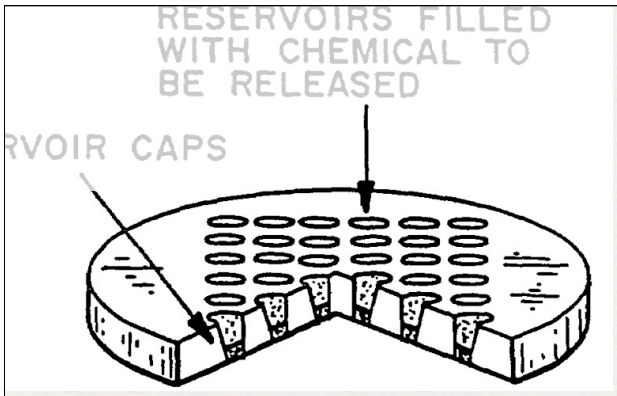
- Ph.D. student at University of Washington
  - Systems, networks, and security
- Graduated from Harvey Mudd College
  - Math and Comp Sci background
  - Free time: Lock picking, Urban spelunking
- Interested in {designing,building,analyzing,breaking} practical systems in all of these domains

Implantable Medical Devices (aka IMDs)

- Common - ***2.6 million*** pacemakers implanted 1990-2002
- Computers with sophisticated functionality
- Perform vital, lifesaving functions **in people**

adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

Photos: Medtronic, Hearing Loss Assoc. of WA, St. Jude Medical, Otto Bock



Pharmacy
on a chip



Neurostimulator



Cardiac device



Drug pump



Prosthetic
limb

adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

Why would academics study IMD security?

- Find yet another vulnerable product....
- So what?
- If you just add encryption, we can all go home...



Securing IMDs is *hard*!

adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

Cannot fail closed

- Closed: No credentials, no admission!
- ***But,*** medical personnel need emergency access.
- Basic tension between **patient safety + medical efficacy** and **security and privacy**.
- A challenge in this space is ***fail open*** *design*.

adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

So what did we do?

- Studied a real implantable device
- Found attacks with software radio
- Built prototypes looking towards potential defenses

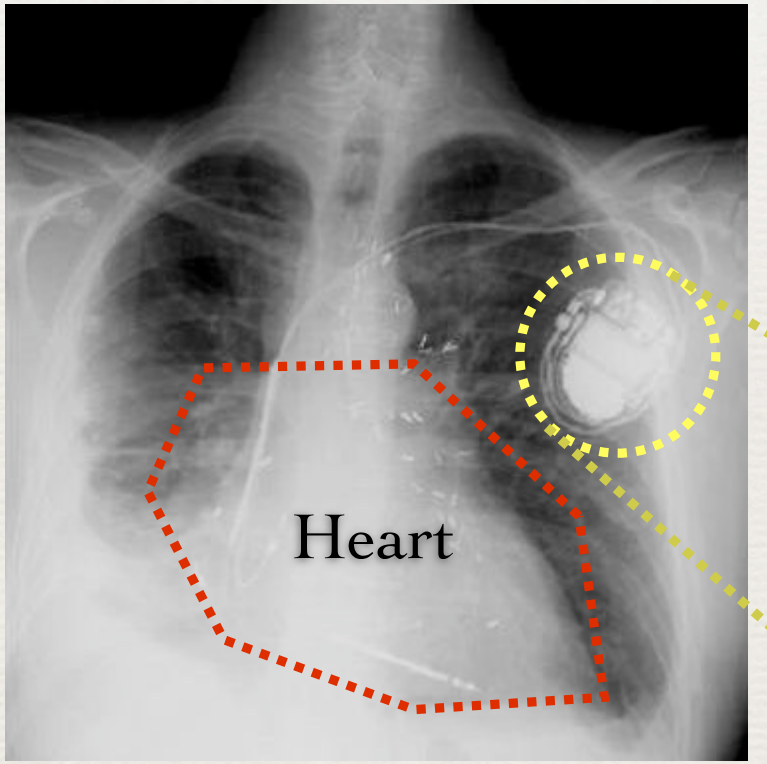


Implantable cardiac defibrillator

adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

Analysis of a Real Device

Implantable Cardiac Defibrillators



- Monitors heart waveforms
- Like a pacemaker, sets heart rhythm
- Also: delivers a large shock to resync heart



adapted from Ben Ransford, UMass Amherst http://www.cs.umass.edu/~ransford/

Defensive Directions

Medical Devices Need Continued Attention!

Type B: Measuring What's Happening in Today's World

Properties of these projects

- Many aspects of today's world are unknown
  - How do networks *really* work? What do ISPs *really* do?
- Academic researchers try to shed light on the answers to these questions
- Many follow-on possibilities, including
  - Improve artifacts of network or systems (e.g., make them faster or more secure)
  - Protect against these networks or systems

Properties of these projects

- Results can also have broad affects, to public policy, legislation, and so on
- Measurement papers generally also include discussions
  - Lessons learned from the measurements
  - Predictions for how systems will evolve
  - Possible improvements to the systems
  - Possible defenses against the systems

Detecting In-Flight Page Changes with Web Tripwires

Charlie Reis (University of Washington)
Steven D. Gribble (University of Washington)
Tadayoshi (Yoshi) Kohno (University of Washington)
Nicholas C. Weaver (International Computer Science Institute)

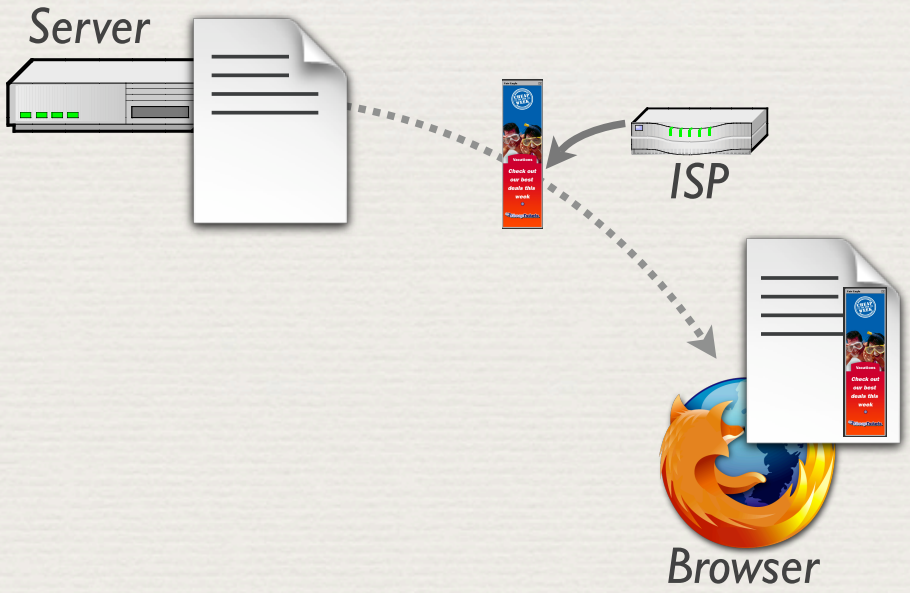
USENIX Symposium on Networked Systems Design and Implementation, 2008

http://www.cs.washington.edu/research/security/web-tripwire/nsdi-2008.pdf

ISP-Injected Ads

ISPs Inserting Ads Into Your Pages

Posted by CmdrTaco on Sat Jun 23, '07 09:19 AM
from the **now-thats-just-slimey** dept.



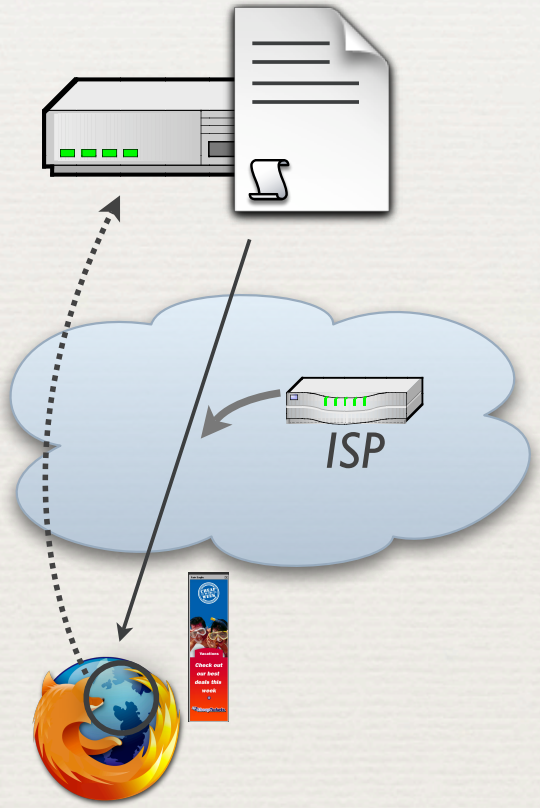
- Reports of web page modifications
  - ISPs injecting ads into web pages
- Is this really happening? How often?

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Scientifically study and measure the phenomenon

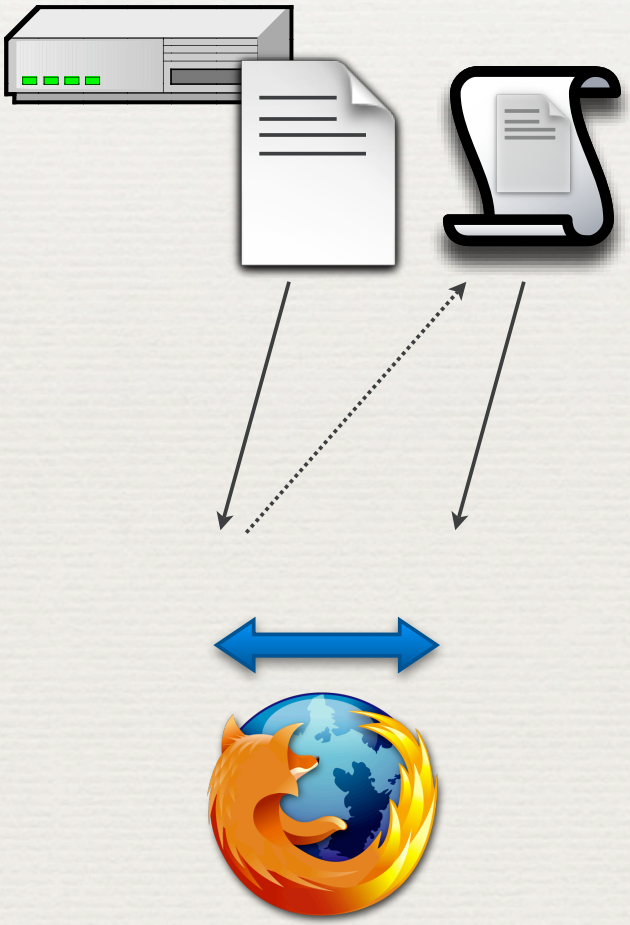
Detecting Page Changes

- Can detect with JavaScript
- Built a **Web Tripwire**:
  - Runs in client's browser
  - Finds most changes to HTML
  - Reports to user & server



Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

How it Works

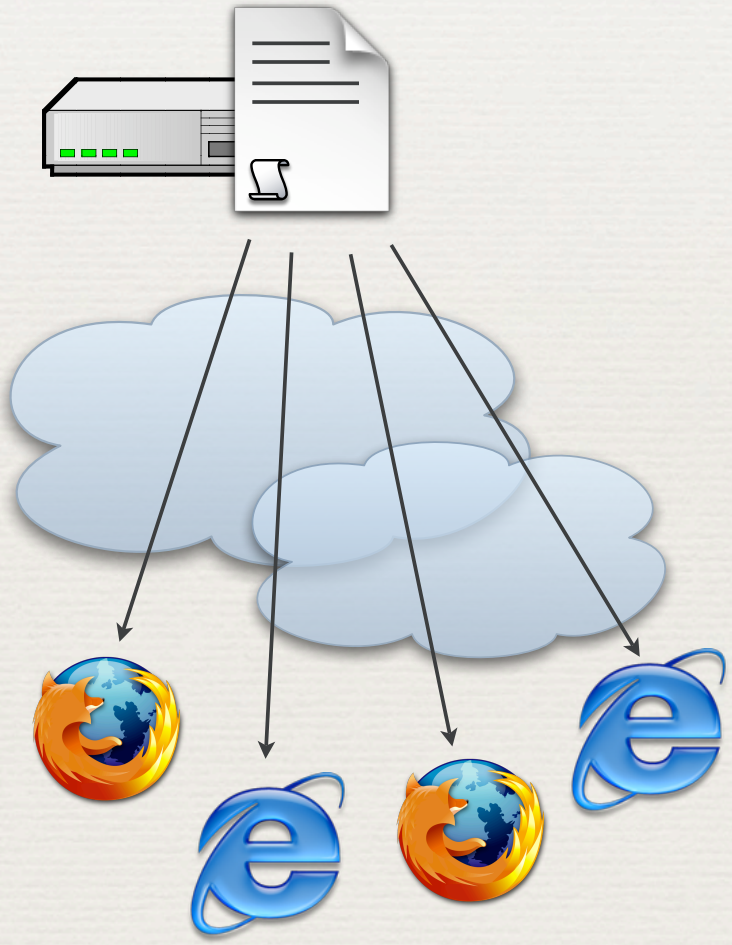


- Fetch and render original page
- Fetch JavaScript code in background
  - Second, encoded copy of page
- Compare against page's source code

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Attracting Visitors

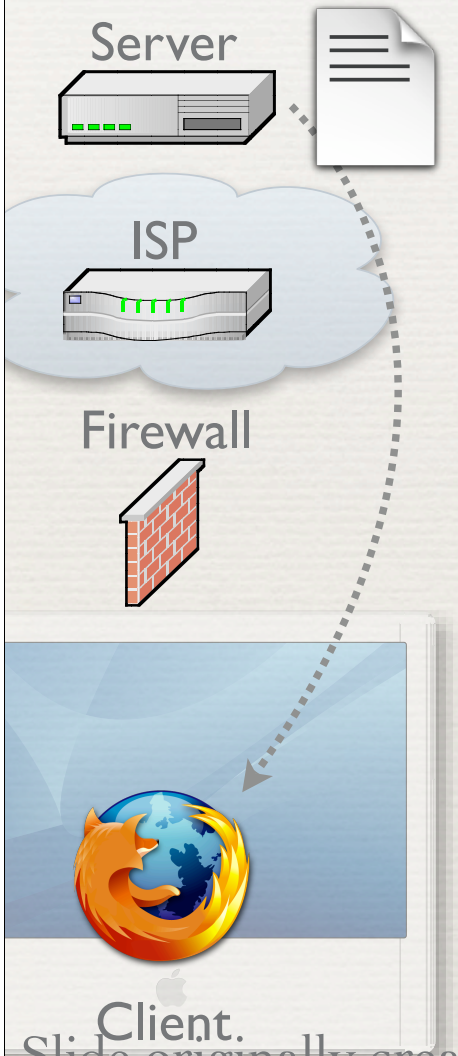
- Wanted view of many clients on many networks
- Posted to **Slashdot**, **Digg**, etc.
  - Visits from over 50,000 unique IP addresses



Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Analyze the Results

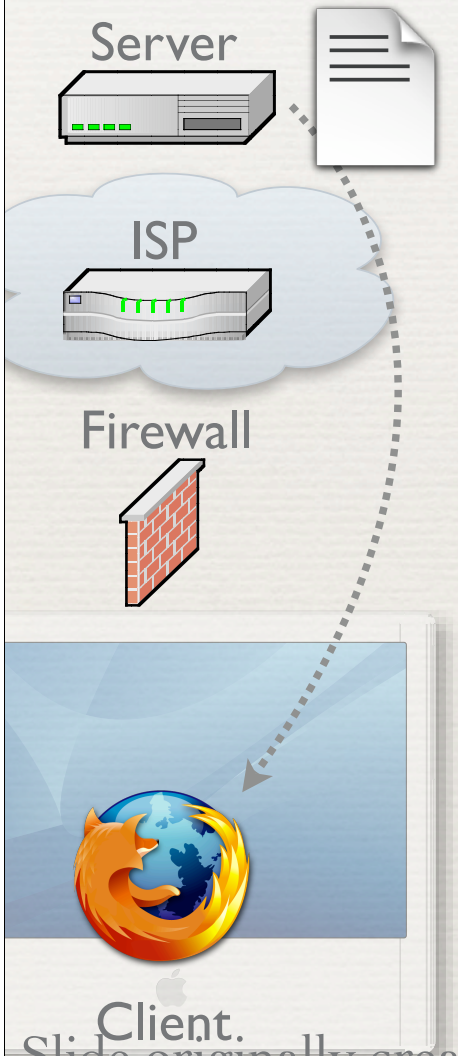
Many Users Affected



- 657 clients saw changes (1.3%)
  - Many made by client software
  - Some made by agents in network
- Diverse incentives
- Often concerning for publishers

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

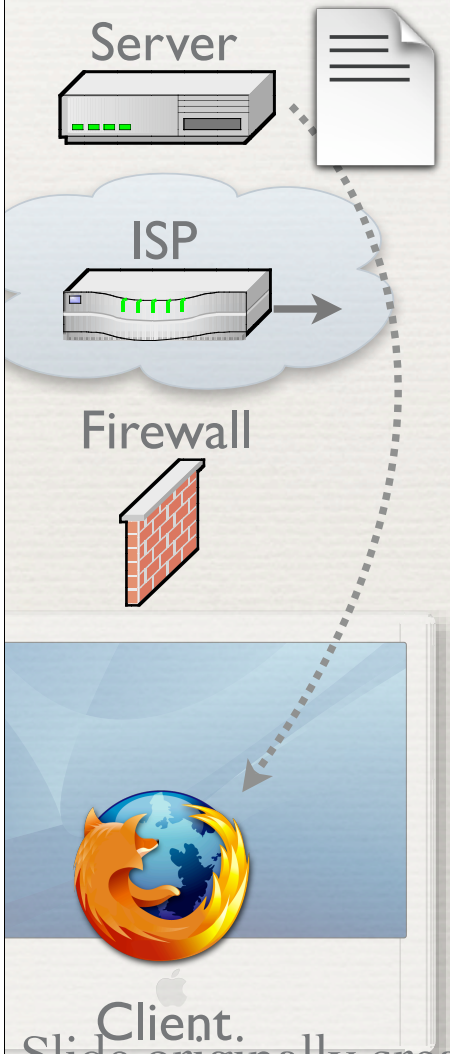
Many Types of Changes



- Internet Service Providers
- Enterprise Firewalls
- Client Proxies
- Malware

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Changes by ISPs



- **Injected Advertisements** (2.4%)
  - NebuAd, MetroFi, LokBox, ...



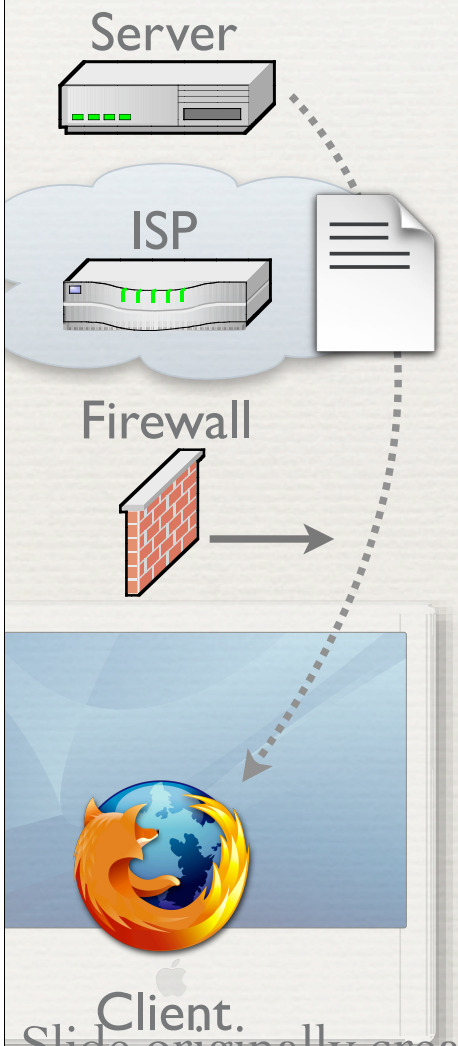
Revenue for ISP; annoy users

Growing Trend?
PerfTech, Front Porch, Adzilla, Phorm

- **Compression** (4.6%)

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Changes by Enterprises

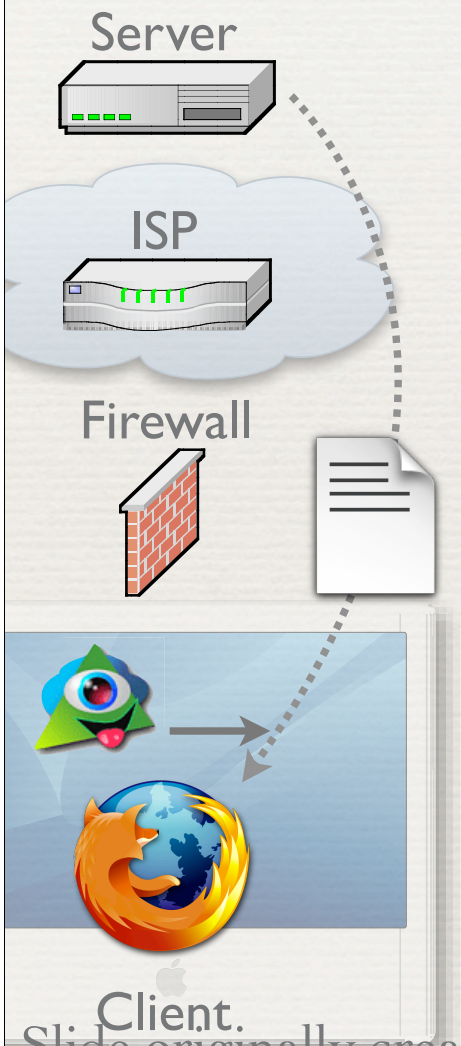


- **Security Checking Scripts** (2.3%)
  - BlueCoat Web Filter

Safer for clients; reduce risk

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Changes by Client Proxies

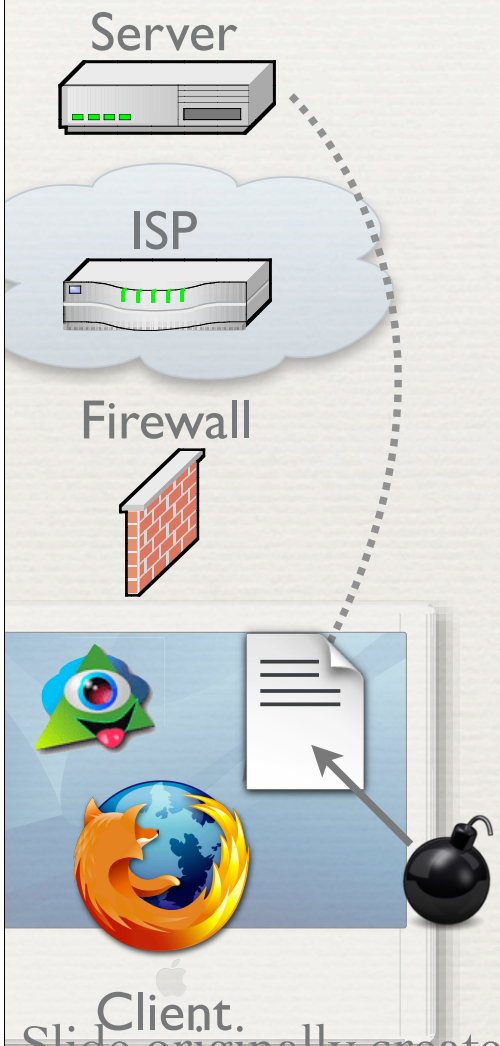


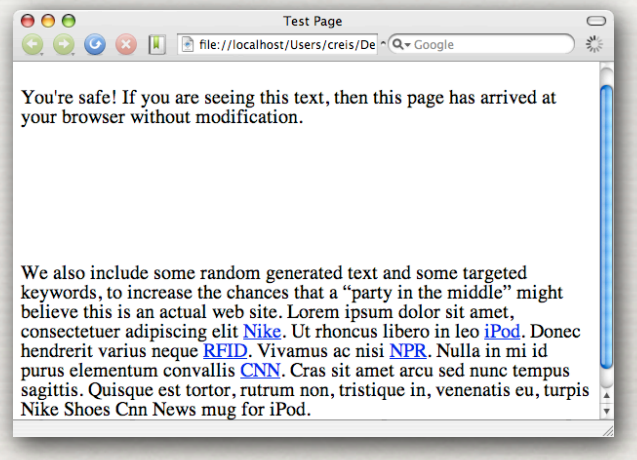
- **Popup & Ad Blockers** (71%)
  - Zone Alarm, Ad Muncher, …

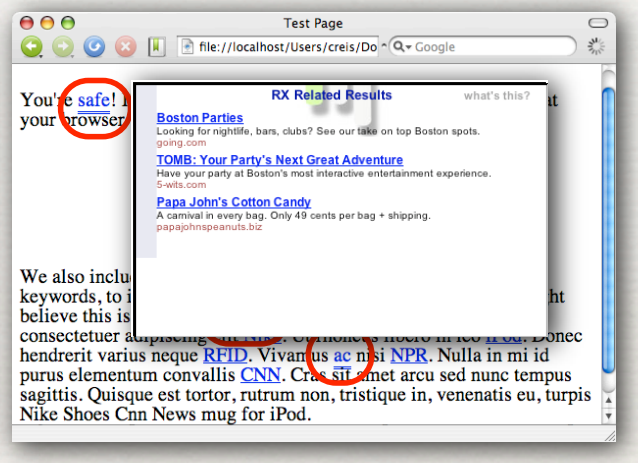
Less annoying; impact revenue

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Changes by Malware



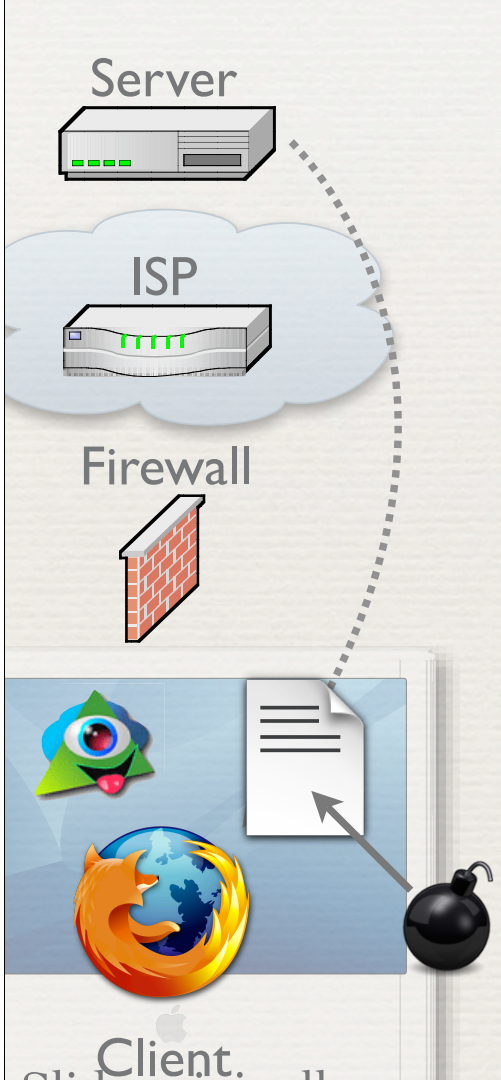




- **Adware** (1 client)

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Changes by Malware





ARP Poisoning

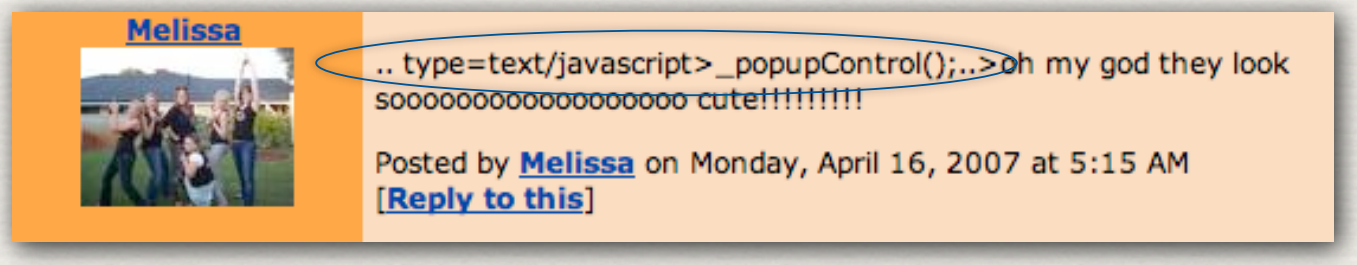
- **Adware** (1 client)
- **Worms** (2 clients)

Helps malware author; risk to user

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Unanticipated Impact

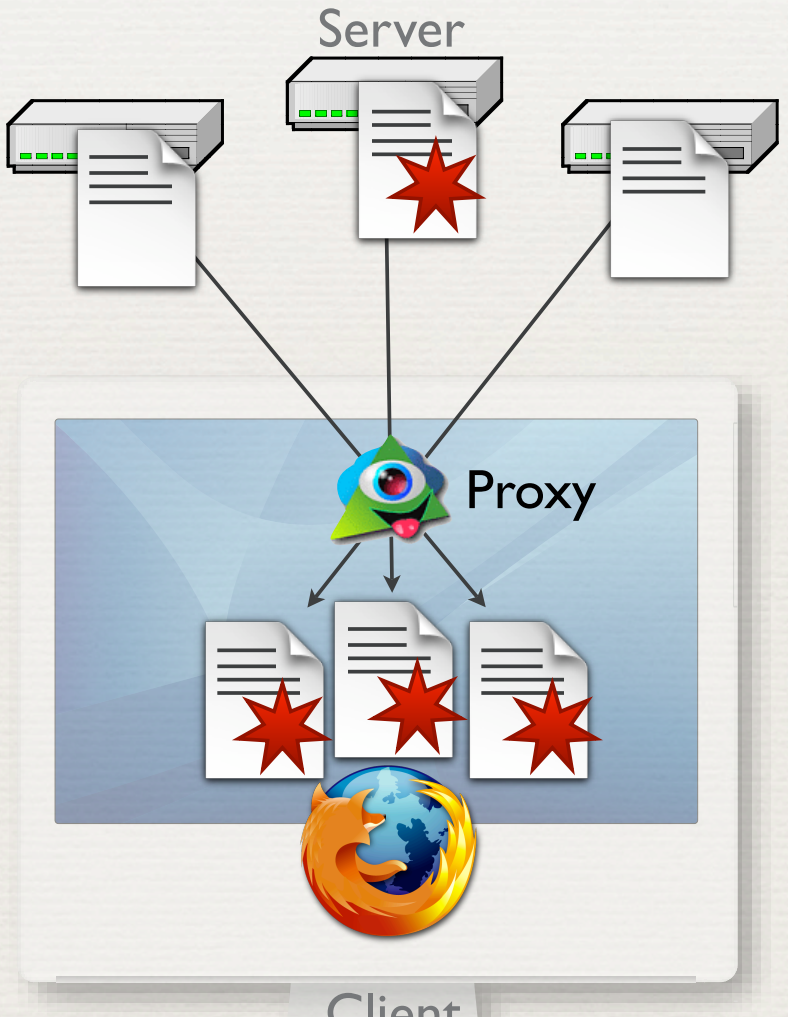
- Some changes **inadvertently** broke pages
  - JavaScript errors
  - Interfered with MySpace / forum posts



Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Introduced Vulnerabilities

- **XSS** allows script injection
  - Usually fixed at server
- Some proxies made otherwise safe pages vulnerable
  - Ad Muncher, Proxomitron
- Affected most HTTP pages
  - Like a **root exploit**



Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

XSS via Proxy

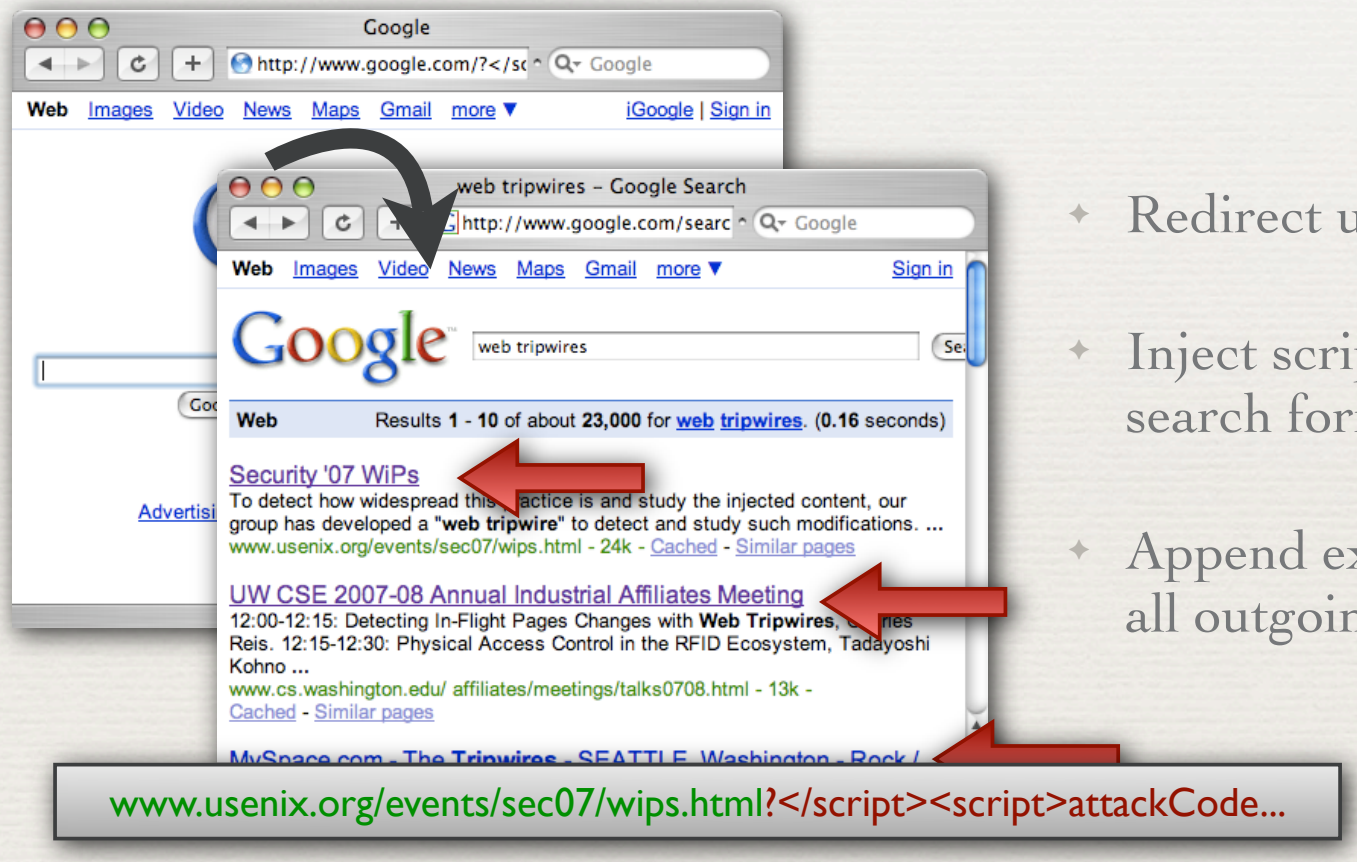
http://usbank.com/?</script><script>attackCode...



- Proxy injected script code
- **Page URL** was included in code
- Attacker could place script code in a valid URL
- Users who follow the URL run injected code

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Example Exploit



- Redirect user to Google
- Inject script code into search form
- Append exploit code to all outgoing links

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Vulnerability Aftermath

- Reported vulnerabilities; now fixed
- Web tripwires can help find vulnerabilities
  - Search for URL in page changes

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Develop and Study Defenses

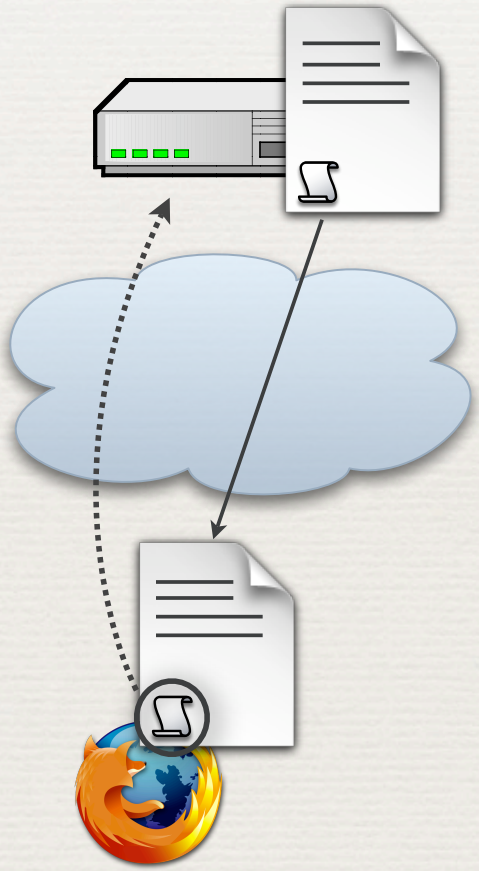
How to React?

- Option 1: **Use HTTPS**
  - Encryption prevents in-flight changes
- But… costly and rigid
  - Can't allow security checks, caching, etc.

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Web Tripwires

- JavaScript code to detect changes
- Easy for publishers to deploy
  - **Configurable toolkit**
  - **Web tripwire service**
- But… not cryptographically secure
- Can be robust in practice
- Available here: http://www.cs.washington.edu/research/security/webtripwires.html



Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

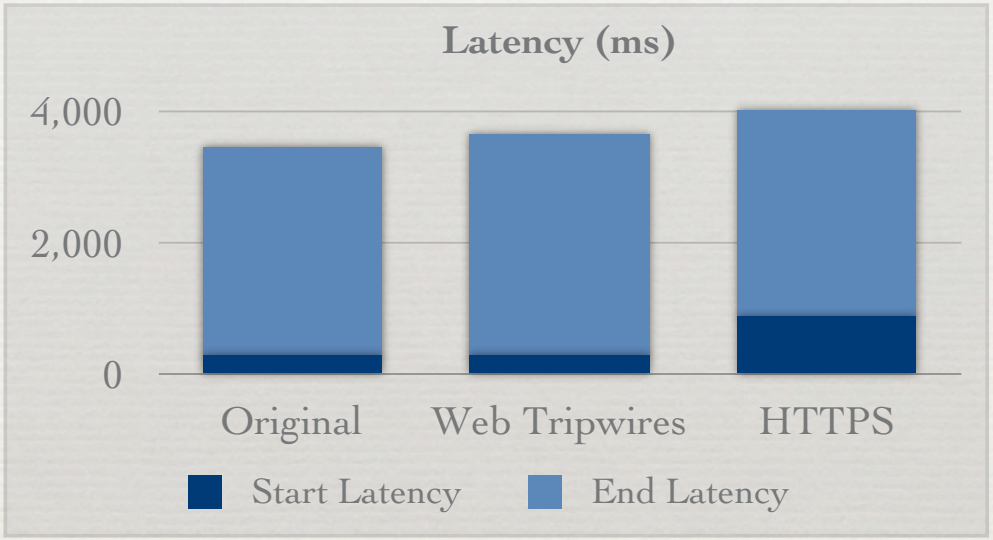
Tradeoffs

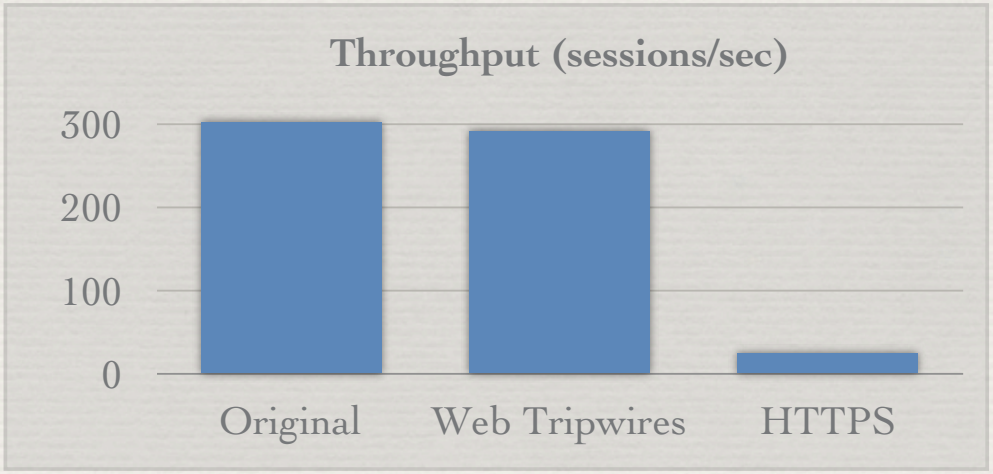
HTTPS	Web Tripwires
✦ Prevents most changes, as well as some useful services	✦ Detects most in-flight changes
✦ Cryptographically robust	✦ Could face an arms race ✦ Obfuscation can challenge adversaries
✦ Expensive: certificates, computation, extra RTTs	✦ Inexpensive to deploy

Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Performance Impact

- Relative to HTTPS, web tripwires have:
  - Low latency
  - High throughput





Slide originally created by Charlie Reis, http://www.cs.washington.edu/homes/creis/

Challenges and Directions for Monitoring P2P File Sharing Networks

Michael Piatek (University of Washington)
Tadayoshi (Yoshi) Kohno (University of Washington)
Arvind Krishnamurthy (University of Washington)

http://dmca.cs.washington.edu

Why monitor P2P?

Added	Name		Size	Seeds	Leechers
17 Jun 08	The Happening CAM XViD-[CoNsPIRACY]	17	700.21 MB	1700	7147
17 Jun 08	The Happening CAM XViD-[ViCiOsO] (Portuguese SUB)	13	700.21 MB	3167	5436
25 May 08	Star Wars I-VI Collection DvDrip-aXXo	237	4.38 GB	967	5174
07 May 08	Iron Man PROPER TS XviD iLG[contego ws]	8	1.4 GB	0	4644
26 Jun 08	Iron Man 2008 PROPER TS (With Sample) XViD ENG - INTERNAL	61	901.47 MB	655	4522
27 May 08	Jumper[2008]DvDrip AC3-aXXo	354	699.84 MB	4798	4269
19 Jun 08	The Incredible Hulk 2008 TS XVID - STG	40	856.61 MB	2403	3655
28 May 08	Vantage Point[2008]DvDrip AC3-aXXo	365	699.84 MB	3285	3486
21 Jun 08	Rocky-The Complete Saga[2007]DvDrip-aXXo	105	4.11 GB	414	3426
24 Jun 08	Journey to the Center of the Earth DVDRip XviD-BeStDivX	33	706.88 MB	2361	3274
30 May 08	Indiana Jones Kingdom of the Crystal Skull ViCiOsO[Portugese-SUB-]	13	700.5 MB	880	3255
16 Jun 08	Lethal Weapon-The Complete Collection DvDrip-aXXo	131	3.03 GB	522	3110
19 Apr 08	Hero Wanted 2008 DvDRip Eng-FxM	164	702.08 MB	2899	3108
06 Jun 08	My Mom's New Boyfriend[2008]DvDrip-aXXo	100	701.28 MB	2168	2937
05 May 08	Iron Man 2008 Eng TELESYNC DivX-LTT	94	707.43 MB	3688	2877

Copyright infringement:
movies, music, software, books, etc.

P2P Monitoring Today

1. Crawl P2P networks

2. Identify infringing users

3. Report infringement to ISP

Sample complaint

XXX has reasonable good faith belief that use of the material in the manner complained of in the attached report is not authorized by YYY, its agents, or the law. The information provided herein is accurate to the best of our knowledge. Therefore, this letter is an official notification to effect removal of the detected infringement listed in the attached report. The attached documentation specifies the exact location of the infringement.

What does this mean?

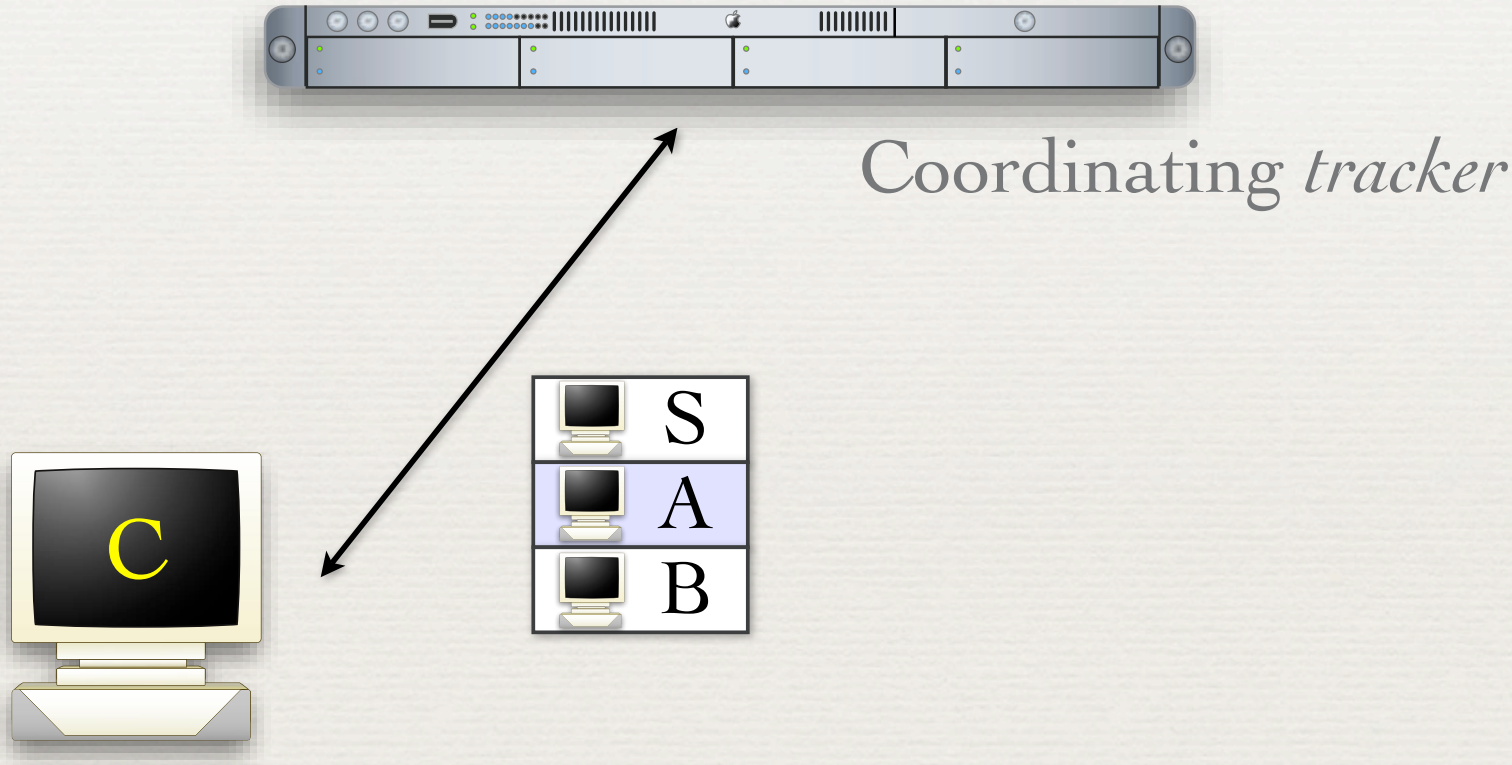
Our work

- **Goal:** Reverse engineer P2P monitoring and copyright enforcement in BitTorrent

- **Findings:**

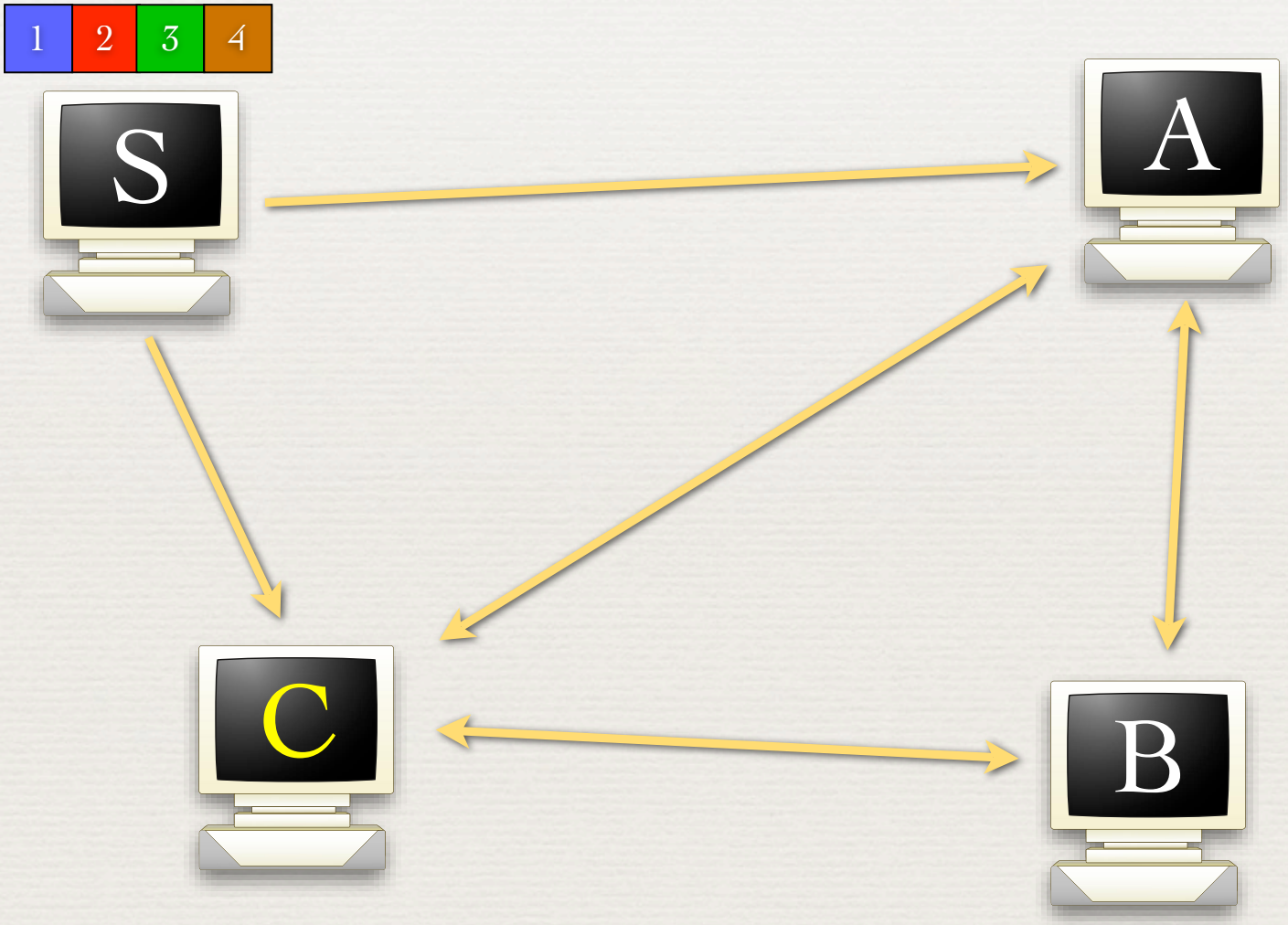
  1. Monitoring is sometimes inconclusive (and can be manipulated)
  2. Some monitoring agents are highly distinguishable

BitTorrent overview

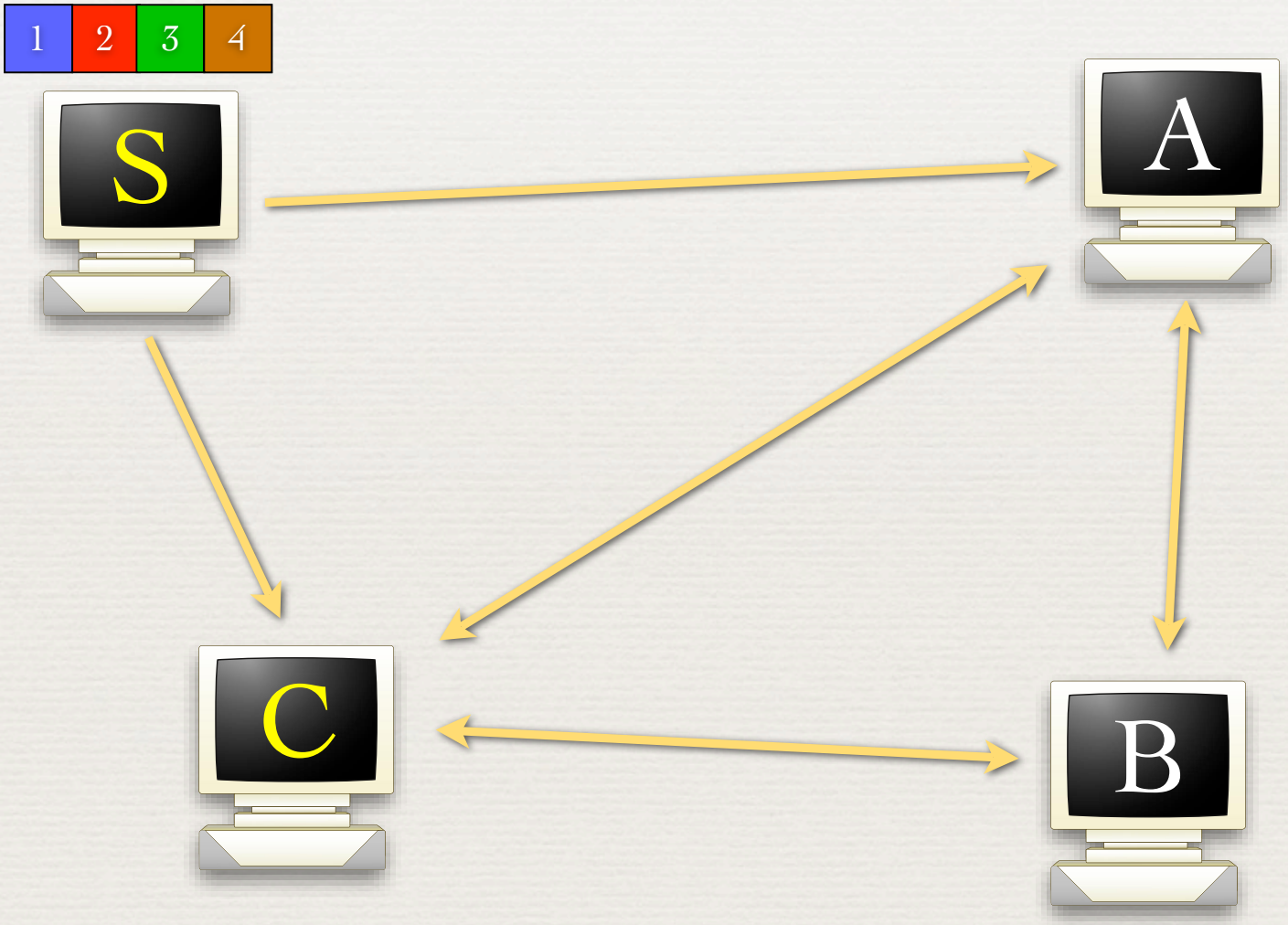


C joins the system by obtaining a random subset of current peers from a centralized coordinator

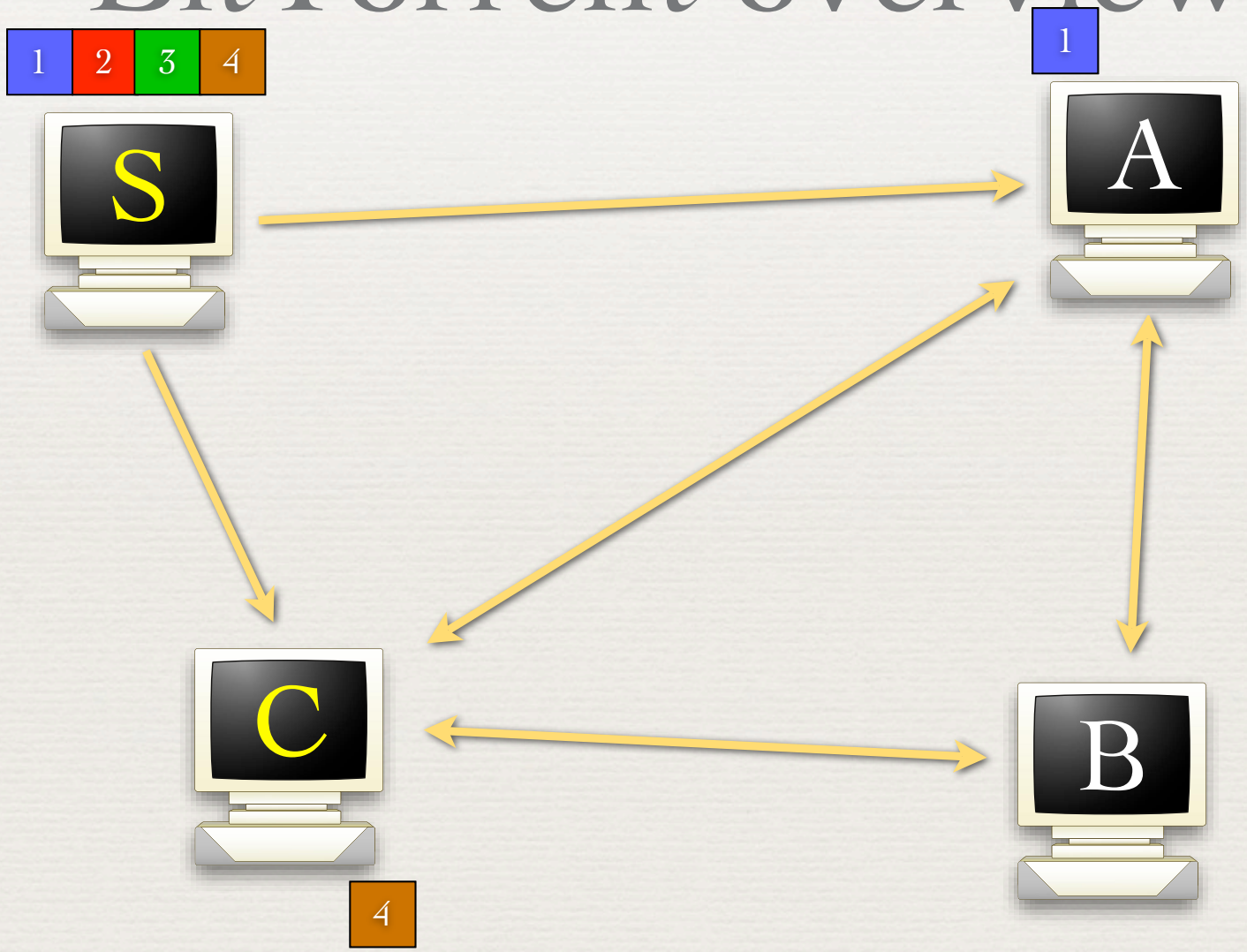
BitTorrent overview



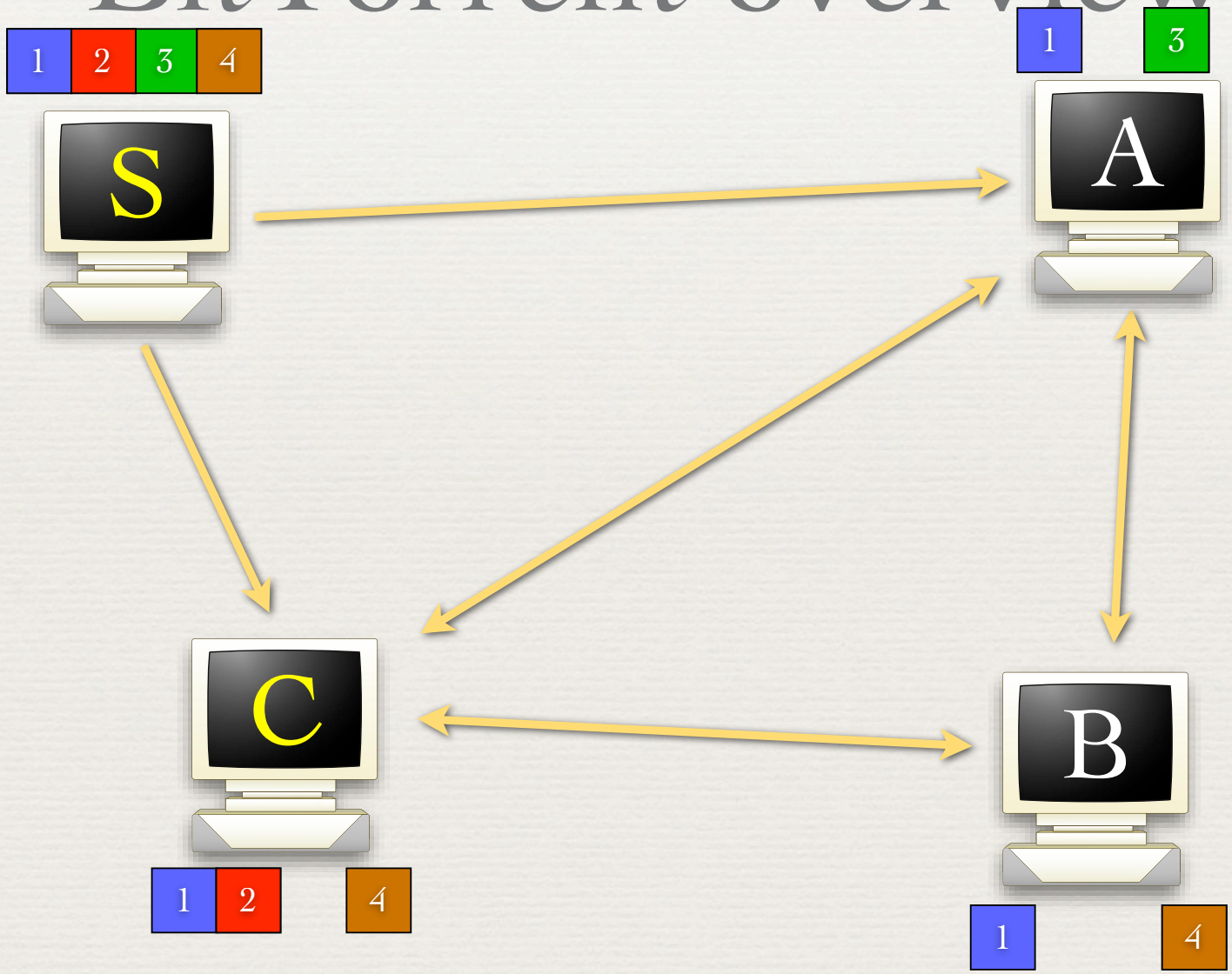
BitTorrent overview



BitTorrent overview



BitTorrent overview



Spoofing requests

- Indirect detection treats reports of membership from the tracker as authoritative
- Protocol support for proxy servers allows us to frame arbitrary IPs

```
wget 'http://torrentstorage.com/announce.php
?info_hash=%0E%B0c%A4B%24%28%86%9F%3B%D2%CC%
BD%0A%D1%A7%BE%83%10v&peer_id=-AZ2504-tUaIhr
rpbVcq&port=55746&uploaded=0&downloaded=0&le
ft=366039040&event=started&numwant=50&no_pee
r_id=1&compact=1&ip=A.B.C.D&key=NfBFoSCo'
```

Spoofing results

Host type	Complaints
Desktop machine (1)	5
IP Printers (3)	9
Wireless AP (1)	4

Framed complaints generated during May, 2008

Avoiding Monitoring

- **IP blacklists** prevent communication with suspected monitoring agents

- But, blacklists do not cover some some hosts:
  - ...that refuse incoming connections
  - ...that are listed in 10s of swarms per day
  - ...that are hosted at colocation facilities

Lessons & Challenges

For monitoring agencies:

- Direct monitoring would reduce false positives, but it would also significantly increase overhead.

For ISPs:

- ISPs should sanity-check complaints, but increasing complaint volume increases costs.

For users:

- Blacklisting techniques are likely to improve, but direct involvement of ISPs in monitoring is increasing.

Type C: Discovering and Exploring New Attack Classes

Properties of these projects

- Sometimes we discover a new way -- or class of ways -- to attack and existing system
- When we do so, we try to deeply study these new attacks. For example
  - Intensive experiments to help us fully understand the attacks
  - Explorations of multiple instantiations or generalizations of the attacks
  - Explore extensions to the attacks
  - Explore potential defenses

Remote Physical Device Fingerprinting

Tadayoshi (Yoshi) Kohno (University of Washington)
Andre Broido (CAIDA , now Google)
kc claffy (CAIDA)

IEEE Symposium on Security and Privacy, 2005

http://www.cs.washington.edu/homes/yoshi/papers/PDF/KoBrCl05PDF-lowres.pdf

Typical goals

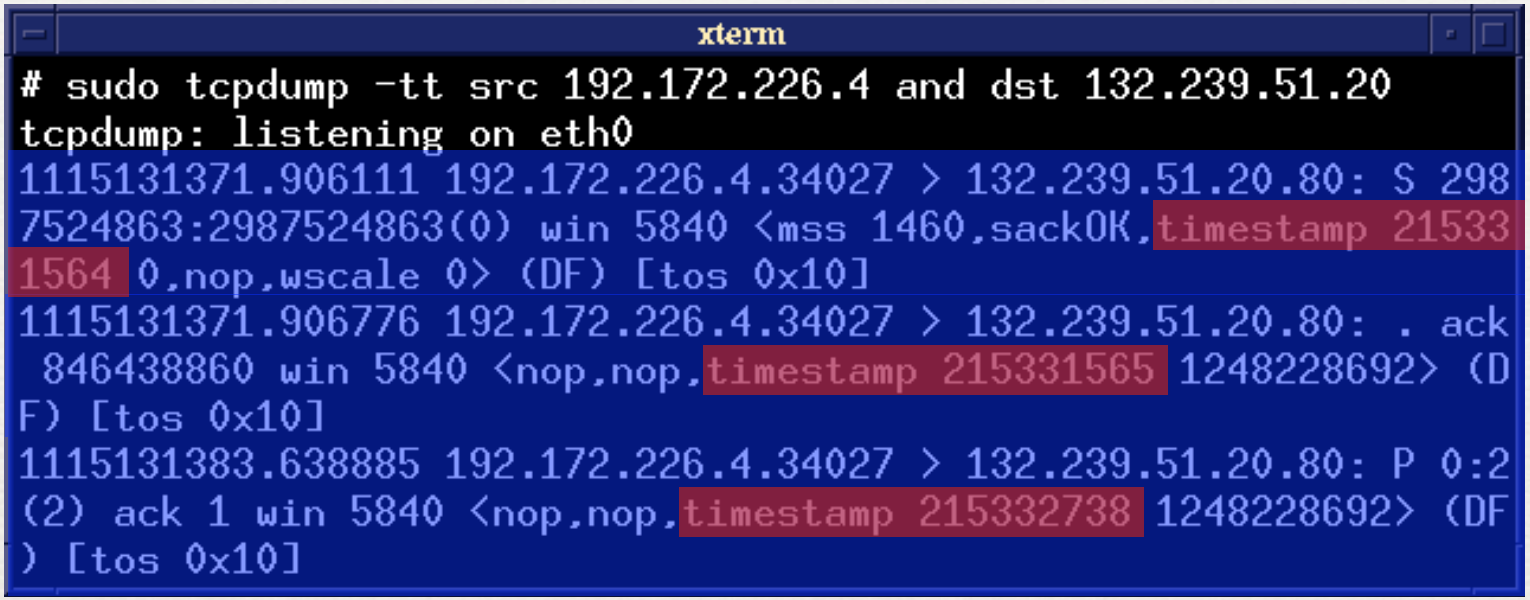
- Remotely distinguish between two devices that have the same hardware and software configuration.
- Remotely determine whether an IP address corresponds to a virtual host.
- Count the number of devices behind a NAT.
- Deanonymize anonymized network traces.

Possible tools

- Remote operating system fingerprinting.
- Usage characteristics.
- Compromise the device.
- Malware and cookies.
- Remote device fingerprinting via information leakage in the TCP and ICMP protocols.

Discover New Information Leakage Vector (TCP)

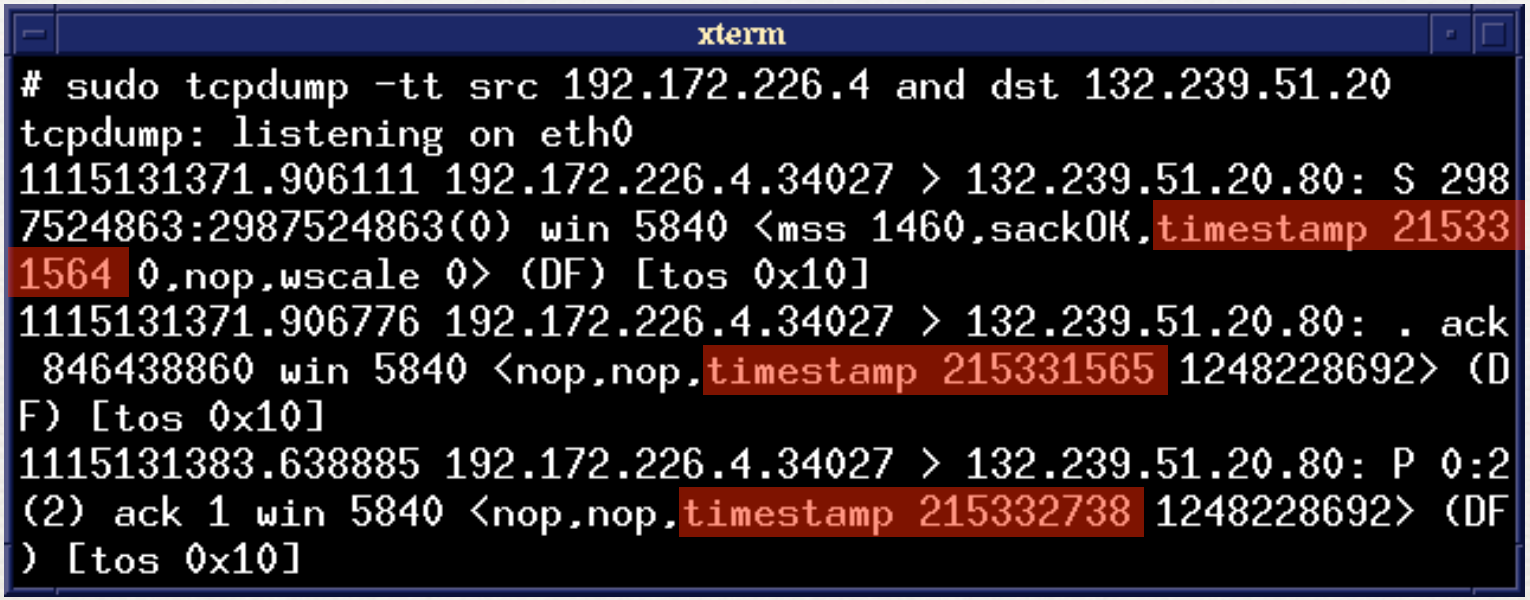
Information leakage in TCP



RFC 1323 defines the TCP Timestamps Option:

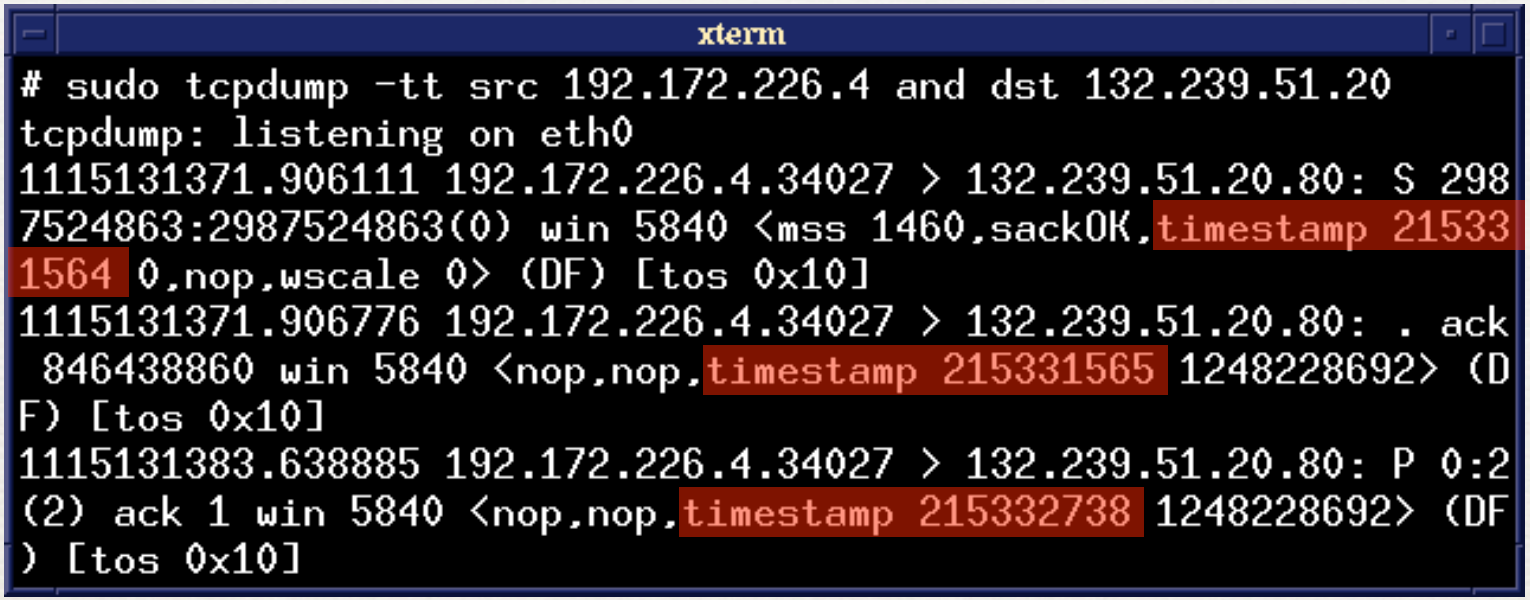
"The timestamp value to be sent in [each outgoing packet] is to be obtained from a (virtual) clock that we call the timestamp [TSopt] clock. Its values must be at least approximately proportional to real time. "

Information leakage in TCP



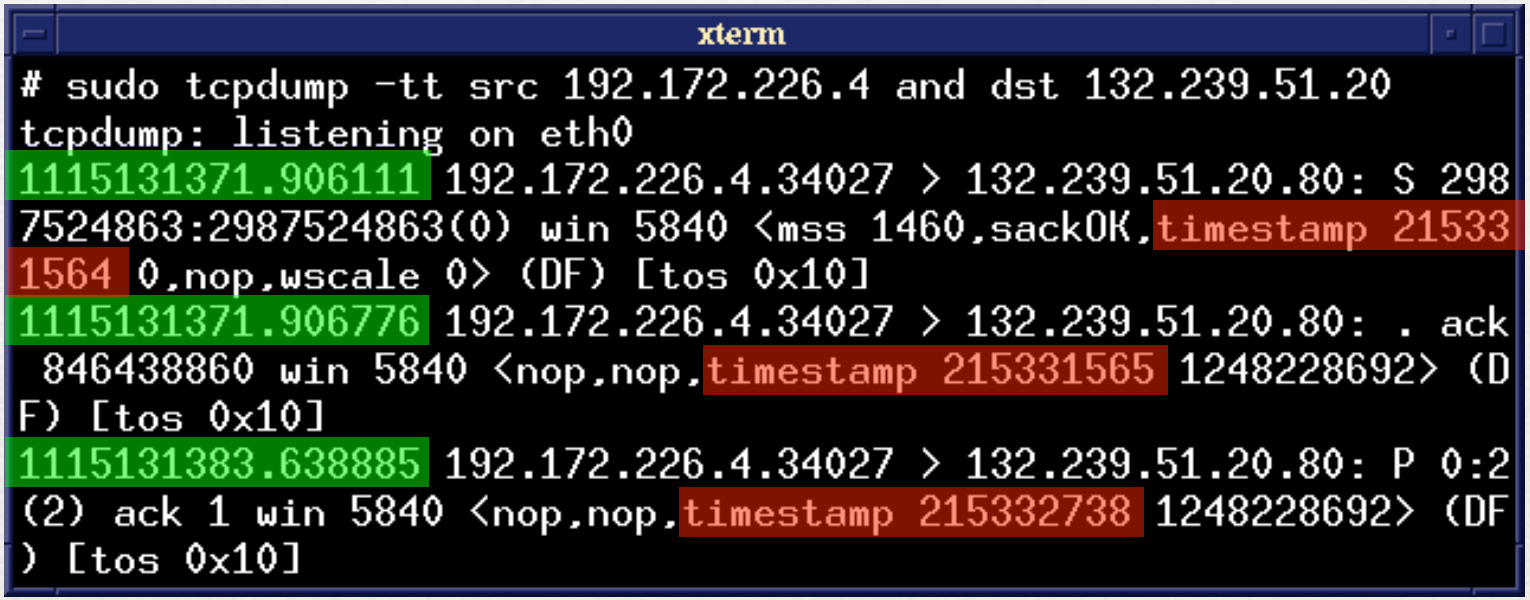
This is information leakage because different devices may have TSopt clocks that advance at different rates (based on the devices' TSopt clock skews).

Information leakage in TCP



A device's TSopt clock may be different from its system clock. NTP adjustments to a devices system clock may not affect the device's TSopt clock.

Extracting information



Let t_i denote the value of the measurer's system clock when it recorded the i-th packet.

Let C_i denote the value of the sender's TSopt clock when it generated the i-th packet.

Extracting information

Assume (for now) that

- the t_i values reflect the true time at which the i-th packet was recorded;
- the C_i values have infinite precision;
- there is no network delay;
- the sender's TSopt clock has constant clock skew s; common values for s are between -100 and 100 ppm;
- $t_1 = C_1 = 0$.

Then, by the definition of clock skew,

$$C_i = t_i + s t_i$$

for all i.

Extracting information

Under these assumptions, we learn the sender's clock skew as follows:

For each packet, plot

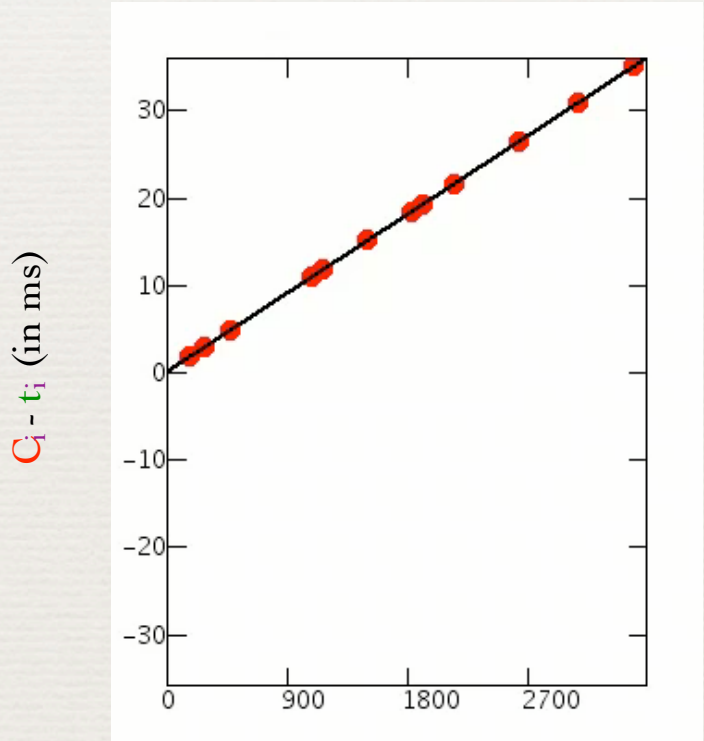
$$(t_i, C_i - t_i) .$$

Since, by definition

$$C_i - t_i = s t_i,$$

the skew s is the slope between any two points.

Artificial data



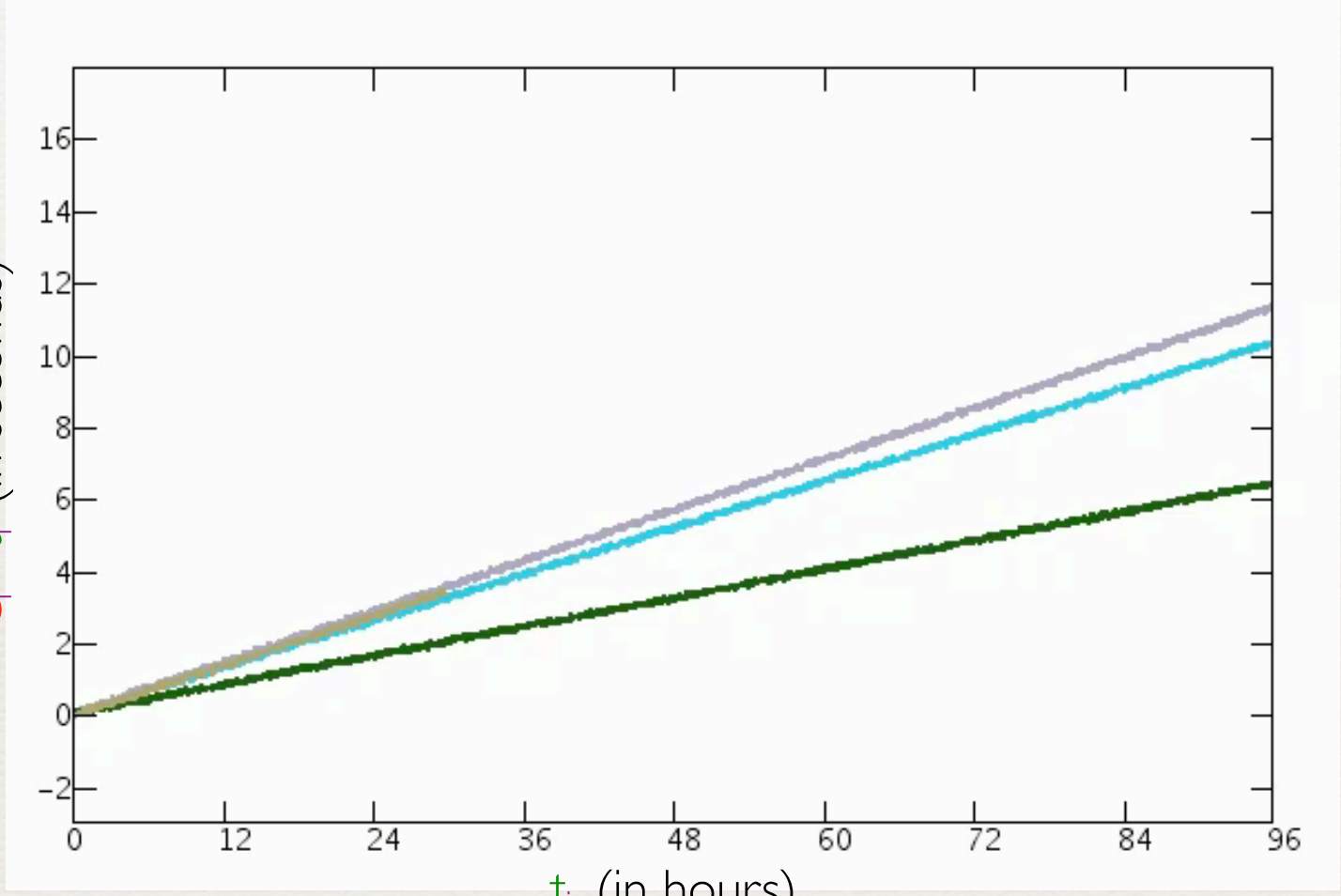
Example

- One of UCSD's undergraduate computing laboratories has 69 Micron 448 MHz PII machines, all running Windows XP SP1.
- measurer1 runs Debian 3.0 and synchronizes its system time with NTP.

  measurer1 is 3 hops away from the undergraduate laboratory.

Example

1. From measurer1 and at random intervals between 0 and 5 minutes, open connections to each machine in the lab.
2. Record a trace on measurer1.
3. Create a plot of (t_i, C_i - t_i) for each machine in the lab.



Plot for third machine in the lab (4624

Plot for the remaining 66 machines in the lab

Determine Vulnerable Population

Obtaining data

The TCP Timestamps Option is an option.

- Not all packets will have the option enabled.
- There are cases when a measurer cannot apply our technique.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

Windows-initiated flows

- When a Windows machine initiates a TCP connection, the initial SYN packet will not have the TCP Timestamps Option enabled.
- According to RFC 1323, none of the subsequent packets in the flow will contain the TCP Timestamps Option.

Resources for measurer	Windows 2000 and XP	Linux 2.2, 2.4, 2.6	OS X
Initiate flows with fingerprintees	Yes	Yes	Yes
Only capture packets	No	Yes	Yes
Cannot initiate flows, but can modify flows, e.g., an ISP or website	Yes	Yes	Yes

A "Yes" means that a measurer can force the system to use the TCP Timestamps Option.

A “trick” for the measurer

- An active measurer could re-write packets in a Windows-initiated flow so that the Windows machine receives packets containing the TCP Timestamps Option.
- The Windows machine will subsequently include the TCP Timestamps Option in its outgoing packets for this flow.

A “trick” for the measurer

Examples:

- An ISP could re-write all outgoing SYN packets so that the re-written packets contain the TCP Timestamps Option.
- A website could reply to all SYN packets with SYN/ACK packets containing the TCP Timestamps Option.

Advantage to active measurers

An active measurer can force a device to send a large number of packets, or send packets over a long duration of time.

Explore Generalizations (e.g, ICMP)

Information leakage in ICMP

- RFC 792 defines ICMP Timestamp Request and Timestamp Reply messages.
- If a measurer sends a fingerprintee a Timestamp Request message, some fingerprintees will reply with a Timestamp Reply message containing the fingerprintee's system time.
- A measurer receiving these Timestamp Reply messages could estimate the fingerprintee's system time clock skew.

Resources for measurer	Windows 2000 and XP SP1	Red Hat 9.0 and Debian 3.0	OS X
Initiate flows with fingerprintees	Yes	Yes	No
Only capture packets	No	No	No
Cannot initiate flows, but can modify flows, e.g., an ISP or website	No	No	No

A "Yes" means that a measurer can use our ICMP-based method to fingerprint a device.

Resources for measurer	Windows 2000 and XP SP1	Red Hat 9.0 and Debian 3.0	OS X
Initiate flows with fingerprintees	Yes	Yes	No
Only capture packets	No	No	No
Cannot initiate flows, but can modify flows, e.g., an ISP or website	No	No	No

A "Yes" means that a measurer can use our ICMP-based method to fingerprint a device.

For the remainder of this talk we shall focus on our TCP-based method because:

- If a measurer can use our ICMP-based method, then the measurer could also use our TCP-based method.
- The results of most of our experiments on our TCP-based method should generalize to our ICMP-based method.

Experimentally Study the New Attack Class

Machines

- laptop is a Dell Latitude laptop with a1.133 GHz PIII processor.

  We generally experiment with laptop running Red Hat 9.0.

- measurer2 is a Dell Precision desktop with a 2GHz P4 processor.

  measurer2 runs Debian 3.0 and is located within the UCSD CSE Department.
  measurer2 synchronizes its system time with NTP.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

Connect laptop to the Internet from multiple locations. Capture packets at measurer2.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

All skew estimates within a fraction of a ppm from each other.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

Regardless of laptop's location.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

Over the course of three months.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

When laptop was connected to the Internet via different access technologies.

Laptop location	Date	Access technology	NAT	Skew estimate
SDSC (CA)	2004-07-10	Wireless	No	-58.00 ppm
Residential cable (CA)	2004-07-12	Wireless	Yes	-58.21 ppm
Residential cable (CT)	2004-07-26	Wired	Yes	-58.19 ppm
Residential cable (CA)	2004-09-14	Wireless	Yes	-58.22 ppm
Dialup (CA)	2004-10-18	Dialup	No	-57.57 ppm
Library (CA)	2004-10-18	Wireless	Yes	-57.63 ppm

And when laptop was both behind and not behind a NAT.

Laptop location	Date			Skew estimate
SDSC (CA)	2004-07-10			-58.00 ppm
Residential cable (CA)	2004-07-12			-58.21 ppm
Residential cable (CT)	2004-07-26			-58.19 ppm
Residential cable (CA)	2004-09-14			-58.22 ppm
Dialup (CA)	2004-10-18			-57.57 ppm
Library (CA)	2004-10-18			-57.63 ppm

Laptop location	Date	Trace duration	Packets	Skew estimate
SDSC (CA)	2004-07-10	3 hours	182	-58.00 ppm
Residential cable (CA)	2004-07-12	3 hours	180	-58.21 ppm
Residential cable (CT)	2004-07-26	3 hours	182	-58.19 ppm
Residential cable (CA)	2004-09-14	30 minutes	1795	-58.22 ppm
Dialup (CA)	2004-10-18	30 minutes	1749	-57.57 ppm
Library (CA)	2004-10-18	30 minutes	946	-57.63 ppm

Laptop location	Date	Trace duration	Packets	Skew estimate
SDSC (CA)	2004-07-10	3 hours	182	-58.00 ppm
Residential cable (CA)	2004-07-12	3 hours	180	-58.21 ppm
Residential cable (CT)	2004-07-26	3 hours	182	-58.19 ppm
Residential cable (CA)	2004-09-14	30 minutes	1795	-58.22 ppm
Dialup (CA)	2004-10-18	30 minutes	1749	-57.57 ppm
Library (CA)	2004-10-18	30 minutes	946	-57.63 ppm

"Low" trace duration and data requirements.

Measurer location	Distance (hops)	Distance (ms)	Skew estimate of laptop
measurer2	8	1.16	-58.03 ppm
San Diego, CA	8	1.15	-58.03 ppm
Berkeley, CA	12	5.06	-58.02 ppm
Seattle, WA	9	15.12	-58.01 ppm
Princeton, NJ	14	36.97	-57.91 ppm
Boston, MA	13	41.09	-58.10 ppm
U. Kingdom	21	86.45	-58.18 ppm
Switzerland	21	84.07	-58.40 ppm
India	16	199.27	-59.60 ppm
Singapore	15	93.55	-58.05 ppm
CAIDA lab	5	0.24	-57.98 ppm

Simultaneously measure laptop from multiple locations around the world.

Measurer location	Distance (hops)	Distance (ms)	Skew estimate of laptop
measurer2	8	1.16	-58.03 ppm
San Diego, CA	8	1.15	-58.03 ppm
Berkeley, CA	12	5.06	-58.02 ppm
Seattle, WA	9	15.12	-58.01 ppm
Princeton, NJ	14	36.97	-57.91 ppm
Boston, MA	13	41.09	-58.10 ppm
U. Kingdom	21	86.45	-58.18 ppm
Switzerland	21	84.07	-58.40 ppm
India	16	199.27	-59.60 ppm
Singapore	15	93.55	-58.05 ppm
CAIDA lab	5	0.24	-57.98 ppm

PlanetLab machines are in red.

Measurer location	Distance (hops)	Distance (ms)	Skew estimate of laptop
measurer2	8	1.16	-58.03 ppm
San Diego, CA	8	1.15	-58.03 ppm
Berkeley, CA	12	5.06	-58.02 ppm
Seattle, WA	9	15.12	-58.01 ppm
Princeton, NJ	14	36.97	-57.91 ppm
Boston, MA	13	41.09	-58.10 ppm
U. Kingdom	21	86.45	-58.18 ppm
Switzerland	21	84.07	-58.40 ppm
India	16	199.27	-59.60 ppm
Singapore	15	93.55	-58.05 ppm
CAIDA lab	5	0.24	-57.98 ppm

Measurer location	Distance (hops)	Distance (ms)	Skew estimate of laptop
measurer2	8	1.16	-58.03 ppm
San Diego, CA	8	1.15	-58.03 ppm
Berkeley, CA	12	5.06	-58.02 ppm
Seattle, WA	9	15.12	-58.01 ppm
Princeton, NJ	14	36.97	-57.91 ppm
Boston, MA	13	41.09	-58.10 ppm
U. Kingdom	21	86.45	-58.18 ppm
Switzerland	21	84.07	-58.40 ppm
India	16	199.27	-59.60 ppm
Singapore	15	93.55	-58.05 ppm
CAIDA lab	5	0.24	-57.98 ppm

The skew estimates seem (relatively) independent of the topology between laptop and the measurer.

Measurer location	Distance (hops)	Distance (ms)	Skew estimate of laptop
measurer2	8	1.16	-58.03 ppm
San Diego, CA	8	1.15	-58.03 ppm
Berkeley, CA	12	5.06	-58.02 ppm
Seattle, WA	9	15.12	-58.01 ppm
Princeton, NJ	14	36.97	-57.91 ppm
Boston, MA	13	41.09	-58.10 ppm
U. Kingdom	21	86.45	-58.18 ppm
Switzerland	21	84.07	-58.40 ppm
India	16	199.27	-59.60 ppm
Singapore	15	93.55	-58.05 ppm
CAIDA lab	5	0.24	-57.98 ppm

The skew estimates seem (relatively) independent of the measurer itself.

OS on laptop	NTP	TSopt clock skew estimate	System clock skew estimate
Red Hat 9.0	No	-58.20 ppm	-58.16 ppm
Red Hat 9.0	Yes	-58.16 ppm	-0.14 ppm
Windows XP	No	-85.20 ppm	-85.42 ppm
Windows XP	Yes	-84.54 ppm	1.69 ppm

Experiment with laptop running Red Hat 9.0 and Windows XP, both with and without NTP-based system time synchronization.

OS on laptop	NTP	TSopt clock skew estimate	System clock skew estimate
Red Hat 9.0	No	-58.20 ppm	-58.16 ppm
Red Hat 9.0	Yes	-58.16 ppm	-0.14 ppm
Windows XP	No	-85.20 ppm	-85.42 ppm
Windows XP	Yes	-84.54 ppm	1.69 ppm

NTP-based system time adjustments do not seem to affect the systems' TSopt clock skews.

OS on laptop	NTP	TSopt clock skew estimate	System clock skew estimate
Red Hat 9.0	No	-58.20 ppm	-58.16 ppm
Red Hat 9.0	Yes	-58.16 ppm	-0.14 ppm
Windows XP	No	-85.20 ppm	-85.42 ppm
Windows XP	Yes	-84.54 ppm	1.69 ppm

Different operating systems running on the same hardware can have different TSopt clock skews.

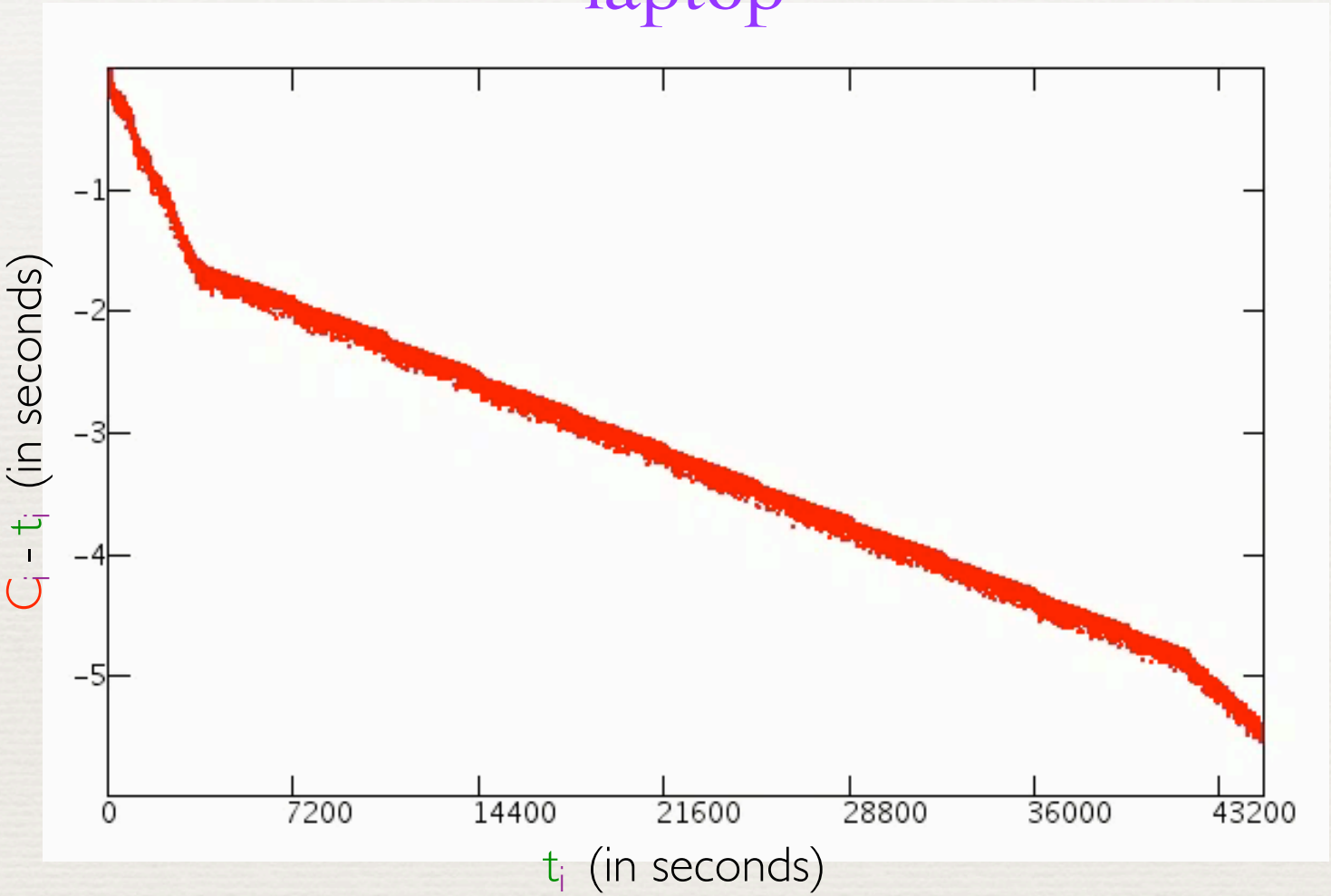
Is there a predictable relationship?

OS on laptop	NTP	TSopt clock skew estimate	System clock skew estimate
Red Hat 9.0	No	-58.20 ppm	-58.16 ppm
Red Hat 9.0	Yes	-58.16 ppm	-0.14 ppm
Windows XP	No	-85.20 ppm	-85.42 ppm
Windows XP	Yes	-84.54 ppm	1.69 ppm

Without NTP-based system time adjustment, a device will have the same TSopt and system time clock skews.

Study Limitations

Windows XP SP2 power management on laptop



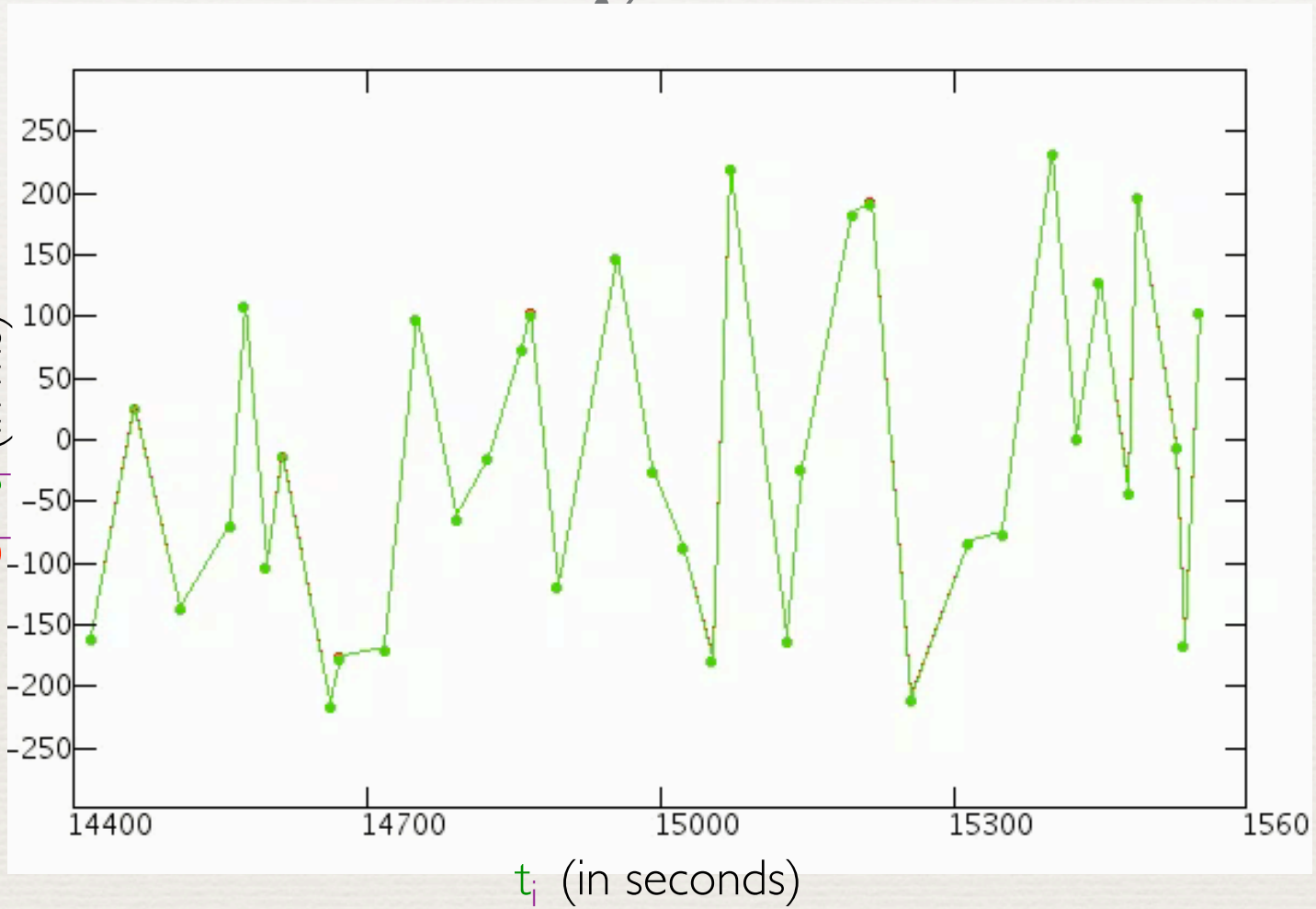
(Additional information leakage?)

Explore Applications

Honeyd 0.8b

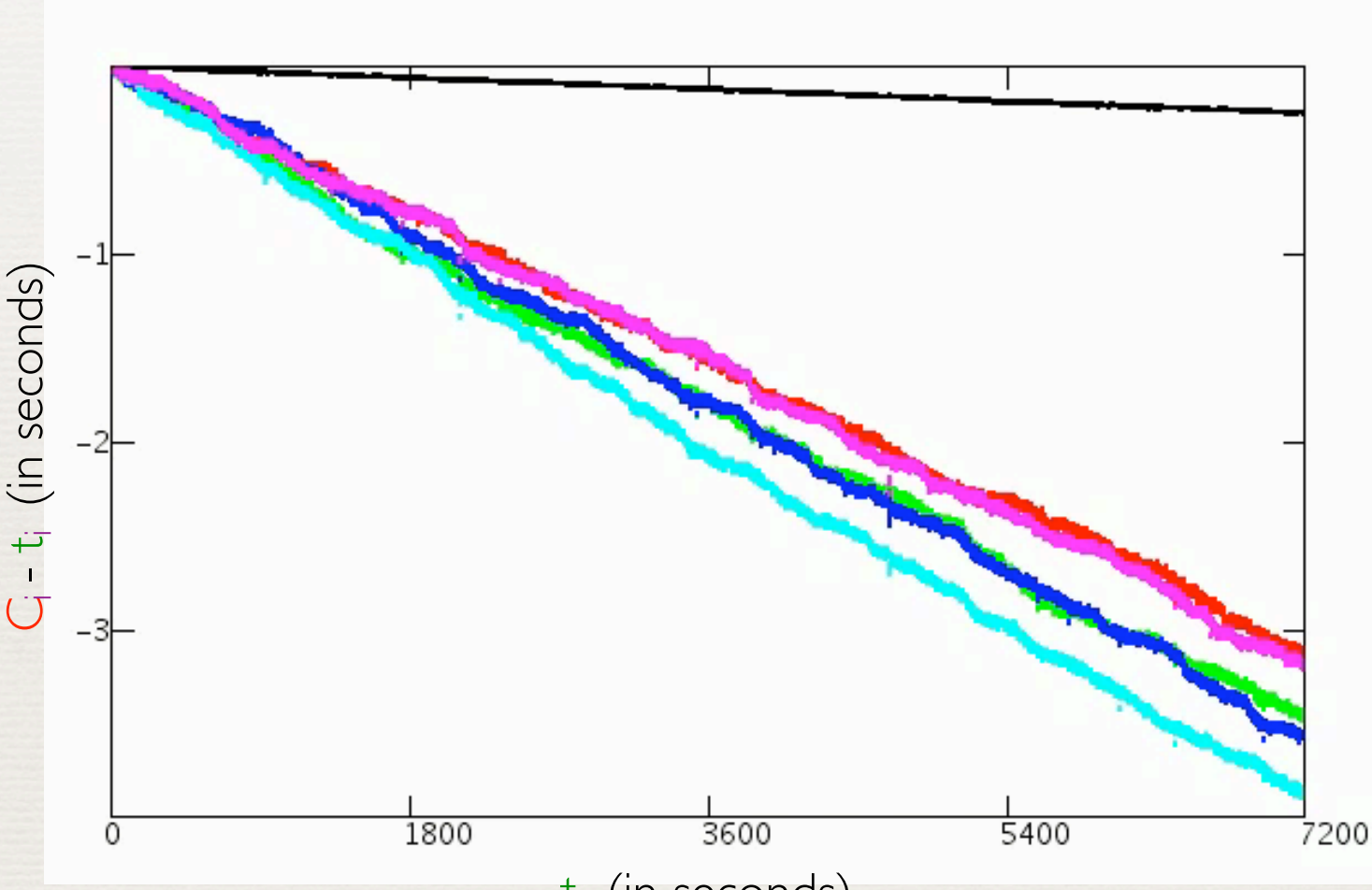
- Honeyd [Provos]: "A framework for virtual honeypots that simulates virtual computer systems at the network level."
- Our observation: All virtual hosts in a honeyd virtual honeynet have approximately the same TSopt clock skew.

Honeyd 0.8b



Example plot for 100 honeyd virtual Windows XP machines on the same host.

VMWare Workstation



Five VMWare Workstation virtual machines running Red Hat 9.0 and the host (also Red Hat 9.0).

Deanonymizing anonymized network traces

- On 2004-04-21, CAIDA took a 2-hour passive trace on a major OC-48 link.
- Since the researchers wanted to use that trace to analyze P2P traffic:
  - The trace contained partial payload data.
  - The IP addresses were anonymized.
- On 2004-04-28, CAIDA took another another 2-hour trace on the same link. This trace contained no payload data and was not anonymized.

Using our techniques, we believe that we deanonymized a number of the IP addresses in the 2004-04-21 trace.

But we could not verify whether we were successful.

Deanonymizing anonymized network traces

- On 2005-01-13 and 2005-01-21 CAIDA took two 2-hour passive trace on an OC-48 link.
- We anonymized the 2005-01-13 trace and then attempted to deanonymize it given the 2005-01-21 trace.

Deanonymizing anonymized network traces

- There were a total of 11862 IP addresses common to both traces.
- Our program output 2170 candidate anonymous-to-real mappings, of which 1902 (88%) were correct.
- Since the anonymization was prefix-preserving, we believe that the 2170 candidate mappings output by our program could catalyze additional deanonymizations.

Other possible applications

- Count the number of devices behind a NAT, even if not all the devices are up at the same time.
- Provide additional information for use with "tracking" physical devices.
- Provide forensics evidence about whether a given device was involved in some action.

Present Defenses

Possible countermeasures

- The TCP Timestamps Option is an option: disable it.
- The timestamps a sender includes in a packet are only later used by itself (they are simply echoed by the other party): don't include real timestamps in outgoing packets.
- Make a device appear to have the clock skew of a different device.

And Mention Open Problems

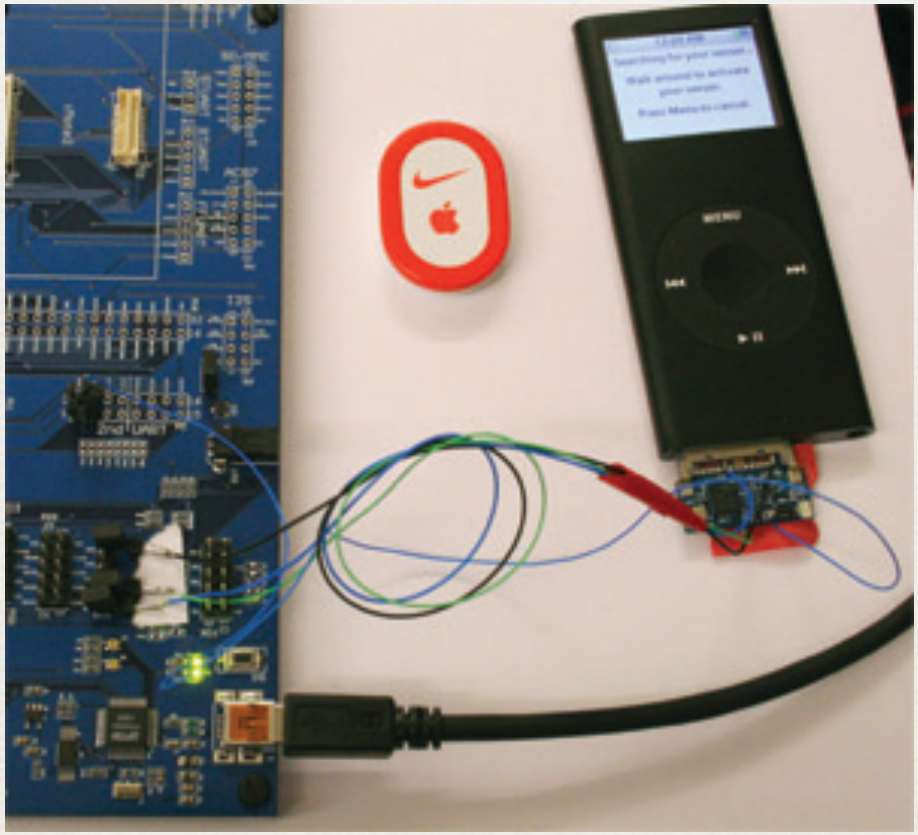
Some open issues

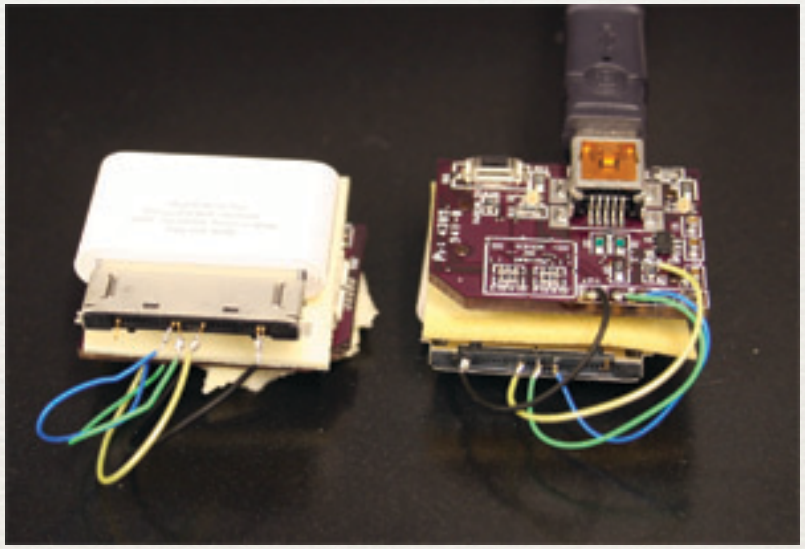
- Better understand the effects of (and possibly additional information leakage from)
  - Temperature variation.
  - Power management.
  - Device load.
  - Operating system.
- Further explore minimum data requirements.

Since 2005

- Our open problems become useful to others
- E.g., Steven Murdoch's CCS 2006 paper
  - "Hot or Not: Revealing Hidden Services by their Clock Skew"
  - Attacks Tor Hidden Services

Nike+iPod Sport Kit





Example: Streaming Media



Slingbox Pro





Sony LocationFree
LF-B20

Internet

Home wireless





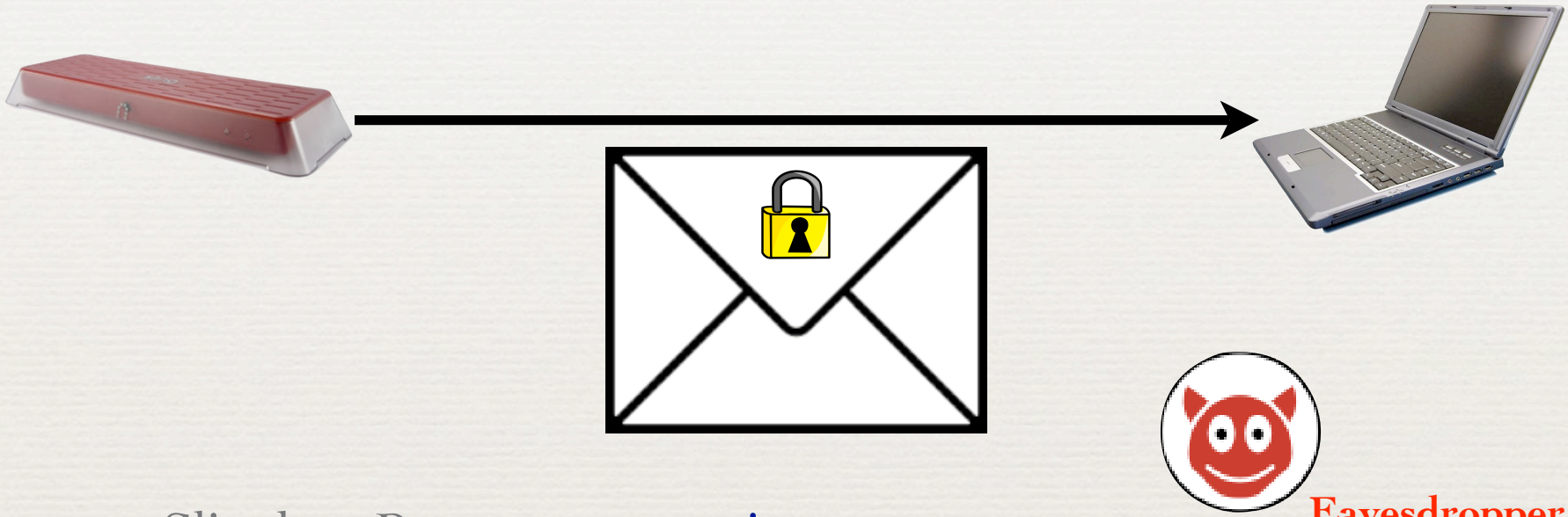
Apple TV





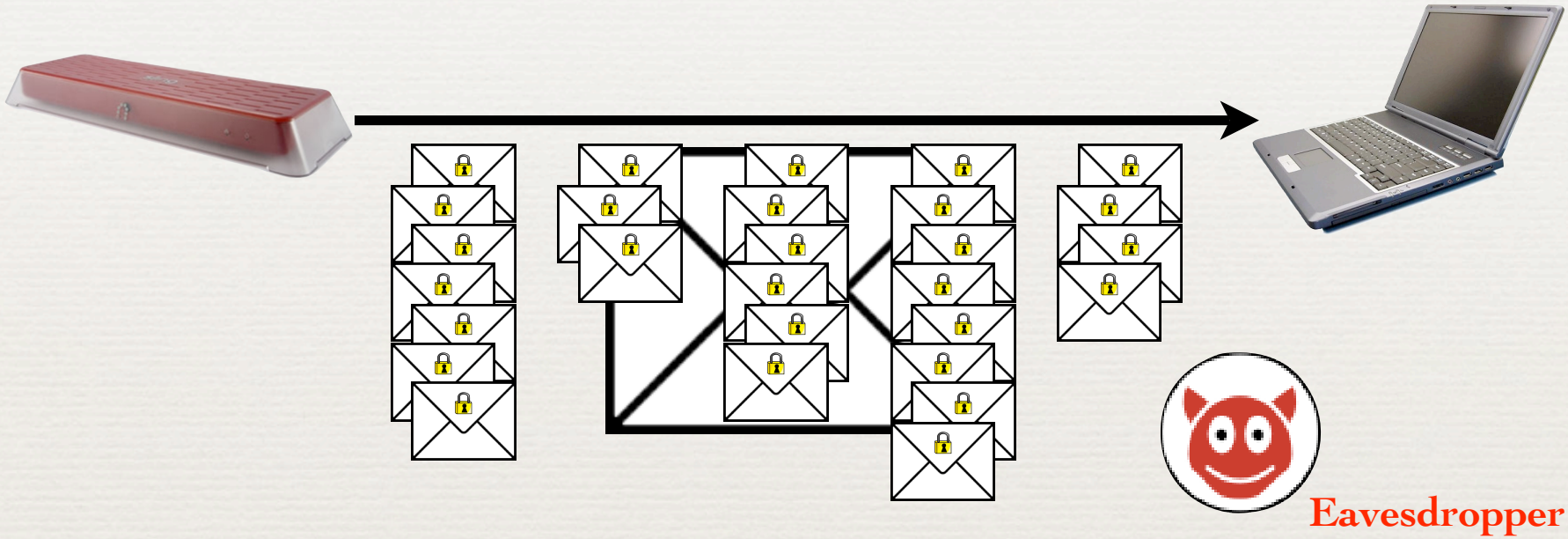
The future of personal entertainment

Encryption and the Slingbox Pro



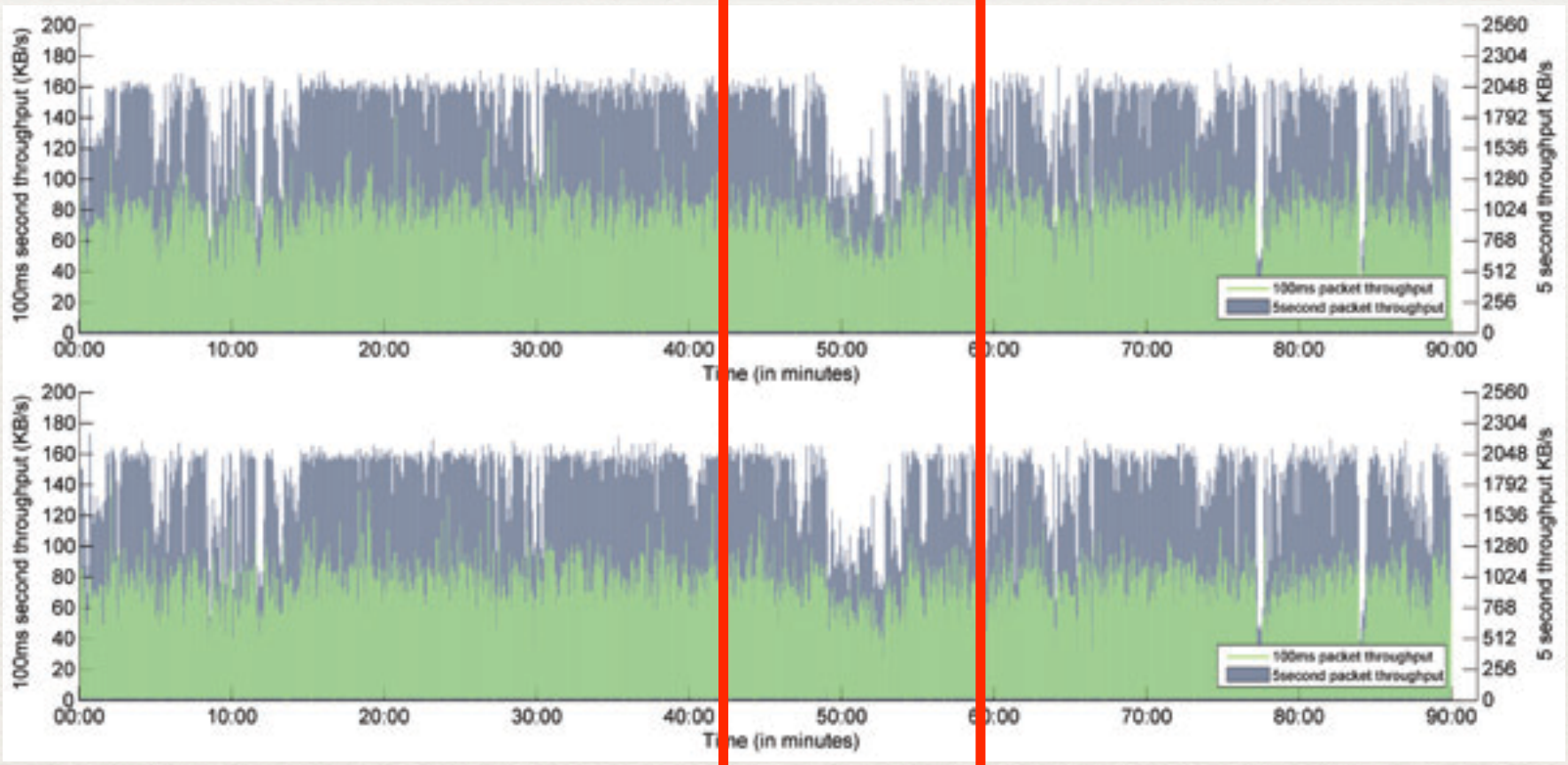
- Slingbox Pro uses encryption
  - To protect privacy of user's viewing habits
  - Pirated or private content
- "Encryption" puts a sealed envelope around messages
  - Only receiver can open
  - Assume we cannot break encryption

Encryption and the Slingbox Pro



- Taking a closer look:
  - Data sent over network (802.11, Internet)
  - Entire movie broken into many envelopes (packets)
- Variable bitrate encoding:
  - Number of packets depend on scene
  - Fingerprint of a movie that survives encryption!

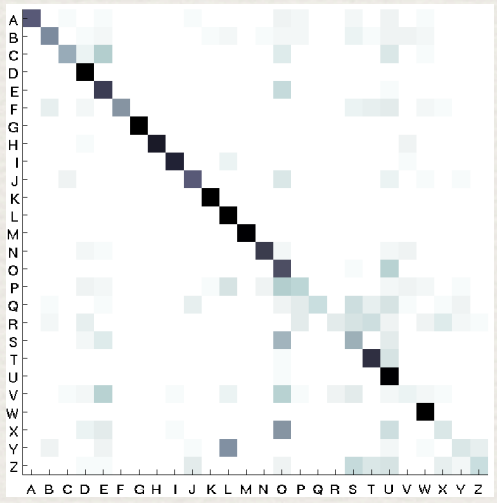
Ocean's Eleven



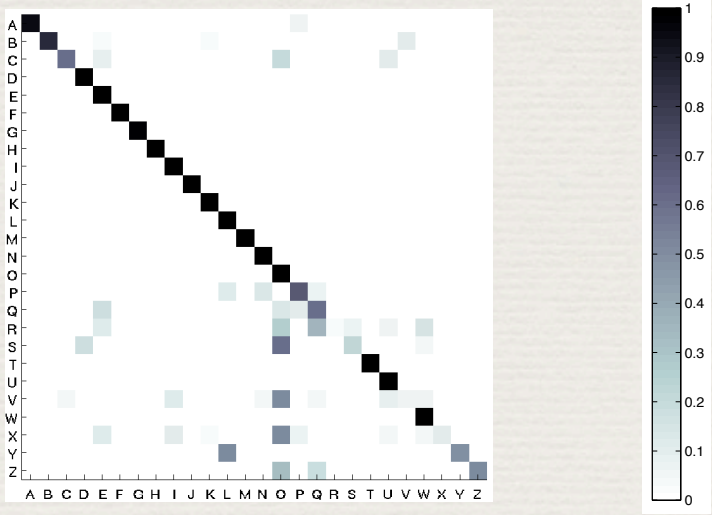
Throughput/time for three traces of Ocean's Eleven

Accuracy

- 26 movies, twice over wireless, twice over wired
- Average identification rates for all 26 movies (compared to < 4% by random guessing)
  - 10 minute sample: 62%
  - 40 minute sample: 77%
- Some movies much better
  - 15 of 26 movies, 40 minute traces, ≥ 98% accuracy



Confusion matrix, 10 min traces



Confusion matrix, 40 min traces

Related Work

- Lots of excellent related works, e.g.:
  - Wright, Ballard, Monrose, Masson. "Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?" USENIX Security 2007
  - Wright, Ballard, Coulls, Monrose, and Masson. "Spot Me If You Can: Recovering Spoken Phrases in Encrypted VoIP Conversations." IEEE Symposium on Security and Privacy 2008.

Defeating Deniable File Systems: A TrueCrypt Case Study

Alexei Czeskis (University of Washington)
David St. Hilaire University of Washington)
Karl Koscher (University of Washington)
Steven D. Gribble University of Washington)
Tadayoshi (Yoshi) Kohno (University of Washington)
Bruce Schneier (BT)

Protecting Your Data

- Can I just encrypt my data? .... well, no
- If an attacker sees that there is encrypted information, he'll just ask you for your password.
- Methods of getting passwords:
  - Algorithmic, fines, jail, extortion, torture

Can US Customs Search & Seize Your Laptop Computer Without Cause? YES They Can!

Ninth Circuit Cour
Agents Can Searc

Executives have been told that they **must hand over their laptop to be analyzed by border police--or be barred from bo**

Customs-Proof Your Laptop

Laptops give up their secrets to U.S. customs agents

By Joe Sharkey

Published: WEDNESDAY, OCTOBE

Taking your laptop into the US? Be sure to hide all your data first

Bruce Schneier
The Guardian, Thursday May 15, 2008
Article history



Photograph: Peter Macdiarmid/Getty Images

Last month a US court ruled that border agents can search your laptop, or any other electronic device, when you're entering the country. They can take your computer and download its entire contents, or keep it for several days. Customs and Border Patrol has not published any rules regarding this practice, and I and others have written a letter to Congress urging it to investigate and regulate this practice.

Customs Officers Can Search Your Lapt

by Tim Stevens, posted Jan 9th 2008 at 10:51AM



Getty Images

If you've ever been through customs, you're probably well aware that the kind, uniforme
sift through your personal belongings as they please and ask you what you've been up
you're headed, and just what it is you're bringing back with you. Now, with more and mo
taking their computers with them, it's becoming more and more clear that those custom
look through your digital files as well.

Deniable File System (DFS)

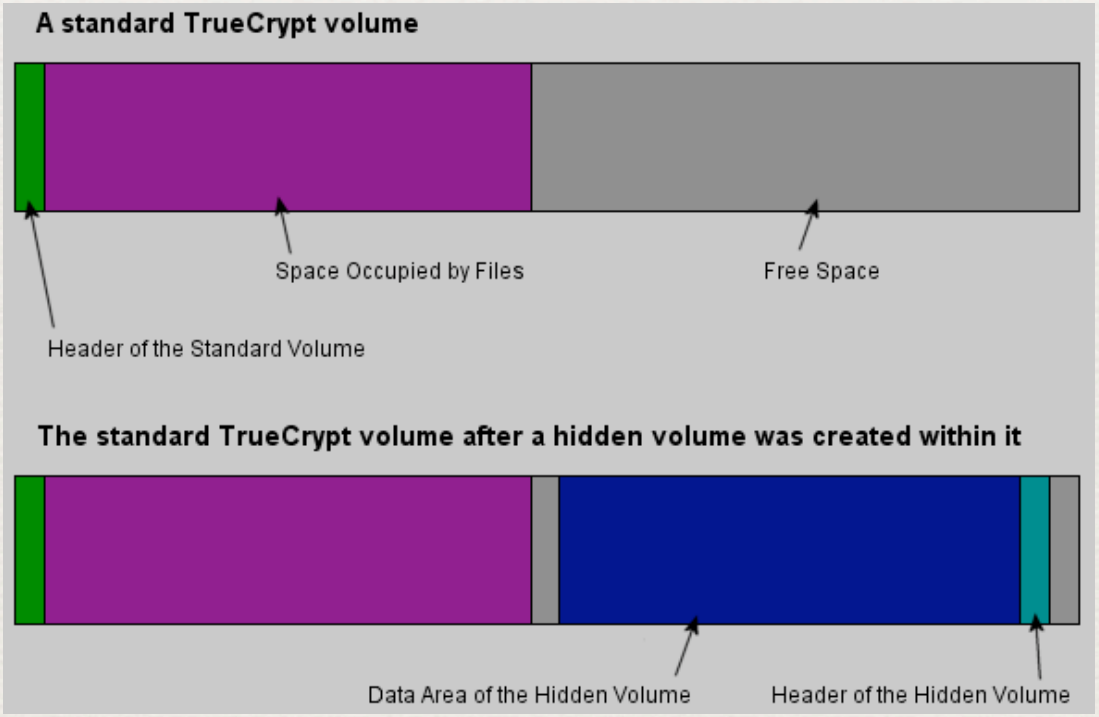
- Idea: hide the existence of a portion of the file system.
- The attacker should not be able to distinguish random free space from data.
  - "Deniable Encryption" by Canetti, et al. (1996).

Analyzing a DFS

- How do we analyze a DFS?
- Are there issues that all Deniable File Systems must overcome?
- Goal: Identify/formalize principles of information leaks in Deniable File Systems
  - Previously: from below (media)
  - Us: from above (OS, applications)

A DFS Implementation: TrueCrypt Hidden Volumes

- Outer Volume
  - Non-hidden
  - Encrypted file
  - Free space is random data
  - A *container*
- Inner Volume
  - Stored inside a container
  - Encrypted with different password



truecrypt.org

Threat Model

- One-Time Access
  - Secret police seize computer
- Intermittent Access
  - HD copied when crossing border in/out
- Regular Access
  - Secret police break into apartment every day

TrueCrypt Case Study

- Your computer tells on you.
- Information leaks (in Vista):
  - Operating system (Shortcuts, Registry)
  - Primary Applications (MS Office, Photoshop, etc...)
  - Non-Primary Apps (Google Desktop)
- Used `OverthrowGovernment.doc`

The OS

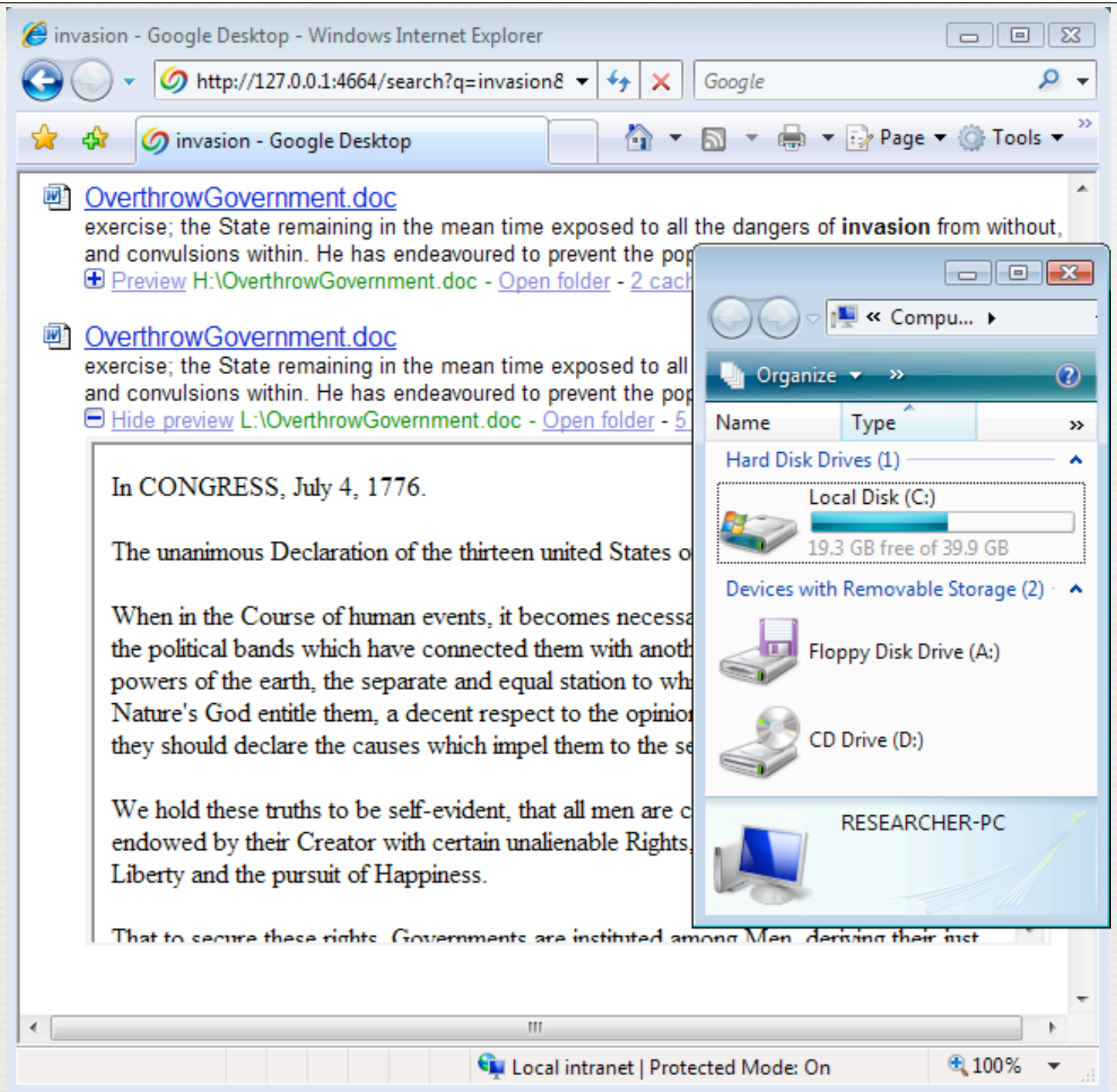
- Registry mentions that a TC volume was mounted - not really a problem
- Recently used shortcuts are generated automatically and show:
  - real file's name
  - its location
  - its creation, modification, access times
  - volume type and serial number it was on

Primary Application

- By default MS Word auto-saves open files to a directory on the c: drive.
  - Deleted when word exits successfully
  - Issues:
    - Remains on disk when process killed
    - Not a clean delete
    - Recoverable even after reboot

Non-Primary Application

- Google Desktop enhanced search
  - Indexes and caches files from hidden volume
- When hidden volume is unmounted, the files remain and are easily recovered.
  - Current and previous versions


invasion - Google Desktop - Windows Internet Explorer
http://127.0.0.1:4664/search?q=invasion&
Google
invasion - Google Desktop
Page
Tools
OverthrowGovernment.doc
exercise; the State remaining in the mean time exposed to all the dangers of invasion from without,
and convulsions within. He has endeavoured to prevent the pop
Preview H:\OverthrowGovernment.doc - Open folder - 2 cach
OverthrowGovernment.doc
exercise; the State remaining in the mean time exposed to all
and convulsions within. He has endeavoured to prevent the pop
Hide preview L:\OverthrowGovernment.doc - Open folder - 5
In CONGRESS, July 4, 1776.
The unanimous Declaration of the thirteen united States o
When in the Course of human events, it becomes necessa
the political bands which have connected them with anoth
powers of the earth, the separate and equal station to wh
Nature's God entitle them, a decent respect to the opinio
they should declare the causes which impel them to the se
We hold these truths to be self-evident, that all men are c
endowed by their Creator with certain unalienable Rights,
Liberty and the pursuit of Happiness.
That to secure these rights, Governments are instituted among Men, deriving their just
« Compu...
Organize
Name
Type
Hard Disk Drives (1)
Local Disk (C:)
19.3 GB free of 39.9 GB
Devices with Removable Storage (2)
Floppy Disk Drive (A:)
CD Drive (D:)
RESEARCHER-PC
Local intranet | Protected Mode: On
100%

The Point is...

- It's hard to have a complete DFS
  - Issue for any DFS: Every process that reads data could potentially store it somewhere else
- Need
  - OS support
  - Hardware support

Type D: Exploring Attacks Against Future Systems

Properties of these projects

- Sometimes the systems we wish to study do not exist yet "in the wild"
- In such cases, we develop and deploy our own systems, and then try to "attack" them
- The goal is to help us better improve the security and privacy of future systems

Exploring Privacy in the RFID Ecosystem

Karl Koscher (University of Washington)
Rest of the RFID Ecosystem Team (University of Washington)

About Karl

- Ph.D. student at the University of Washington
  - Working on all sorts of things
  - Many projects involve RFID and/or privacy
- Previously a research engineer at UW, working on:
  - The RFID Ecosystem
  - Embedded Systems
- Member of the UW Society and Technology Group
- Long history of hacking -- first post to BugTraq in 1997

The Future of RFID

- Old technology -- around since World War 2
- Drastic drops in cost are making the technology pervasive
  - Readers are much less complicated than WiFi access points
  - Economies of scale are the only reason they cost more -- this may change!
- Once price/tag < 5¢, it's economical to tag EVERYTHING

- What happens when this technology is deployed everywhere and in everything?

The RFID Ecosystem

- RFID will become pervasive
- Before that happens, try to figure out:
  - What cool applications does pervasive RFID technology enable?
  - What are the privacy and security issues that arise?



The RFID Ecosystem

- Building-wide deployment in the Allen Center
  - Over 30 readers currently deployed
  - Over 130 antennas currently deployed
  - Covers floors 2 - 6
  - Basement and 1st floor are coming soon

Deployment Challenges

- Some areas are privacy-sensitive (e.g. bathrooms)
  - Exclude these areas from RFID coverage
- Antenna deployment must be aesthetically-pleasing and keep 9” away from bodies
  - Mounted on the bottom of cable trays

Deployment Map



Privacy Issues

- Rogue Surveillance
- Institutional Surveillance
- Setting the right access controls
- Gaming the system
- Unintended consequences of privacy controls

Rogue Surveillance

- Industry is rallying behind EPC Gen2
- Class 1 Gen 2 tags have essentially no security features
- Anyone with a Gen2 reader can read your tags, from potentially far away
- 160+ ft in highly ideal, FCC-compliant tests
- We can track anyone with a Washington Enhanced Drivers License

Institutional Surveillance

- In today's RFID systems, the system owner can track all tags everywhere they have readers
- DEMO
- Is this a real threat?

Tracking customers?

Worker Snooping on Customer Data Common

By RYAN J. FOLEY

MADISON, Wis. (AP) — A landlord snooped on tenants to find out information about their finances. A woman repeatedly accessed her ex-boyfriend's account after a difficult breakup. Another obtained her child's father's address so she could serve him court papers. …

Documents obtained by The Associated Press in an employment case involving Milwaukee-based WE Energies shine a light on a common practice in the utilities, telecommunications and accounting industries, privacy experts say.

Vast computer databases give curious employees the ability to look up sensitive information on people with the click of a mouse. The WE Energies database includes credit and banking information, payment histories, Social Security numbers, addresses, phone numbers, and energy usage. In some cases, it even includes income and medical information.

Experts say some companies do little to stop such abuses even though they could lead to identity theft, stalking and other privacy invasions. And companies that uncover violations can keep them quiet because in many cases it is not illegal to snoop, only to use the data for crimes.

Boeing bosses spy on workers

By ANDREA JAMES
P-I REPORTER

Within its bowels, The Boeing Co. holds volumes of proprietary information deemed so valuable that the company has entire teams dedicated to making sure that private information stays private.

One such team, dubbed "enterprise" investigators, has permission to read the private e-mails of employees, follow them and collect video footage or photos of them. Investigators can also secretly watch employee computer screens in real time and reproduce every keystroke a worker makes, the Seattle P-I has learned.

For years, Boeing workers have held suspicions about being surveilled, according to a long history of P-I contact with sources, but at least three people familiar with investigation tactics have recently confirmed them.

Access Control Policies

- Hard to get right
- Time consuming even for experts
- One option: Reuse existing social networks
  - Facebook application now being developed
- What should a usable “default” be?

Physical Access Control

- Idea: Have access to tag reads that you could have physically seen
- Simple mental model
- Minimal level of access while still being usable
  - Not perfect:
    - Assumes 360 degree vision
    - Can potentially reveal tags through walls

Physical Access Control to Captured RFID Data (2007, Kriplean, Welbourne, Khoussainova, Rastogi, Balazinska, Borriello, Kohno, Suciu)

Gaming the System

- How do we determine your location?
- It's your "person" tag!
- No reason why you have to keep it with you...
- No reason why you can't clone it!
- No reason why you can't put it on someone else!

Unintended Consequences

- What if we notified you when someone queried for your location?
- This reveals potentially private information about the requester!
- Implemented in an undergrad class
  - One student felt unpopular because her location wasn't being queried often by her friends

Part 2: Hacking in the Undergraduate Curriculum

The Security Mindset

Inside the Twisted Mind of the Security Professional

WIRED

Bruce Schneier ✉ 03.20.08

Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and t
ants. My friend expressed surprise th
in the mail.

I replied: "What's really interesting is
tube of live ants to anyone you tell th

Security requires a particular mindse
least the good ones -- see the world d

Which is why CSE 484, an undergraduate computer-security course taught this quarter at the University of Washington, is so interesting to watch. Professor Tadayoshi Kohno is trying to teach a security mindset.

You can see the results in the blog the students are keeping. They're encouraged to post security reviews about random things: smart pill boxes, Quiet Care Elder Care monitors, Apple's Time Capsule, GM's OnStar, traffic lights, safe deposit boxes, and dorm -room security.

The most recent one is about an automobile dealership. The poster

Developing the "**Security Mindset**" in a **University of Washington undergraduate** computer security **course**

Part 3: The Industry Perspective

About Jon

- Co-founder of PGP Corporation
- Been involved in OS security and crypto for many years
- Past work: DEC, Apple, Counterpane
- Co-author of OpenPGP, DKIM standards

How do we feel?

- The smart people love it
  - Part of my goal: to help people get smart
  - Fight-or flight can be powerful

Educates the market

- Market forces frequently punish a secure system
- People have to know about insecurities
  - If people get used to them, it's hard to upgrade

Hacking is Important

- It shows limitations of present thought
- It shows what is important
  - It is believed people won't buy security
  - It is believed people don't care about privacy
- Should we care, ourselves?

We benefit as well

- Does a new technology work as advertised?
- What are its downsides?
- Who is doing something we don't like?

Independent voices are needed

- There is no better way to test a system
- Practice is better than theory

Peer Review

- It adds weight to the results
- It provides safety to the scientists
  - It can protect upsetting results
- It removes political debate
- We get people's attention better

Hackers and Academics

- Some of the best hackers are academics
- Some of the best researchers are hackers
- The two communities should work more closely

We want to work with scientists

- Peer Review helps science and technology
  - PGP source has been available on web for peer review for many years
  - We also hire researchers to test us
- Smart industry players feel the same way

Part 4: Your Turn

Conclusions