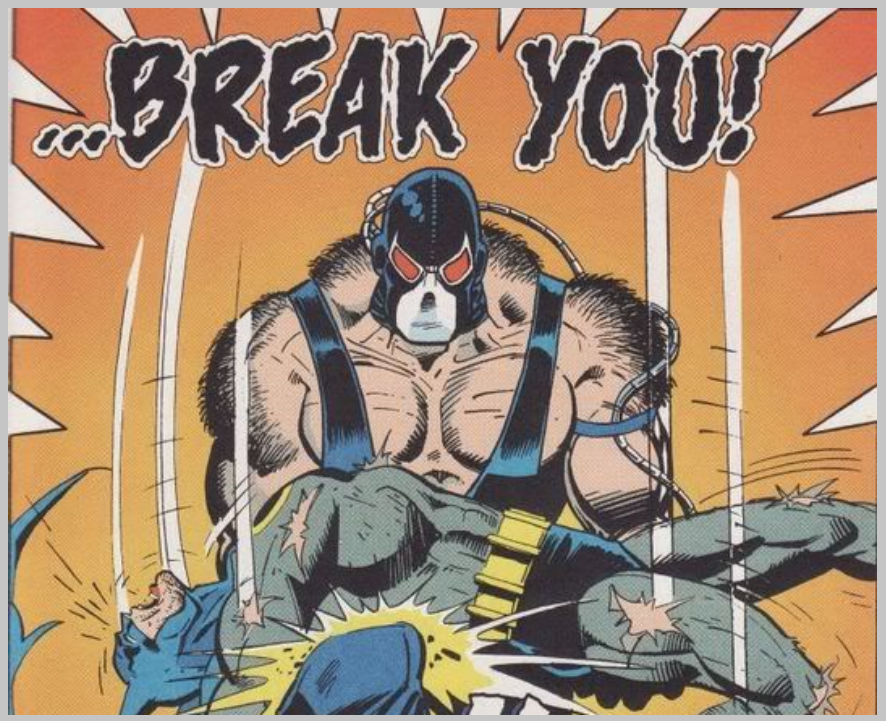
打破后端限制!



DefCon (China) 1, Beijing 2019







Hellfire Security

Gregory Pickett, 获得CISSP, GCIA, GPEN等多项认证

芝加哥, 伊利诺斯州

gregory.pickett@hellfiresecurity.com







概述

- 交通系统
- 逆向工程
- 我的发现
- 漏洞利用
- 经验总结







简史

- 地铁黑客剖析(2008)
- NFC地铁黑客(2012)
- 如何侵入全国交通网络（2012）
- 利用边信道攻击破解韩国交通卡（2017）







有何不同

- 绝不违法
  - 我们不会偷偷溜进车站
  - 我们不会攻击终端
  - 我们不利用社会工程学，也不攻击有线/无线网络
- 无关硬件
  - 我们不会破解任何人的密码
  - 我们不会克隆磁条、无线射频卡、NFC等







有何不同

- 而是关于
  - 应用程序的逻辑缺陷
  - 好吧，实际上用到了克隆，但不是将其作为漏洞进行利用
  - 利用应用程序安全来攻击现实世界中复杂的多层次解决方案

城铁

- 曼谷捷运公司（BTS）
- 曼谷城铁交通系统
- 服务于整个曼谷地区
- 由曼谷捷运公司（BTSC）运营
- 两条城铁线，沿途共43个车站

车票

- 储值卡（NFC）
- 单日票（磁条）和单程票（磁条）

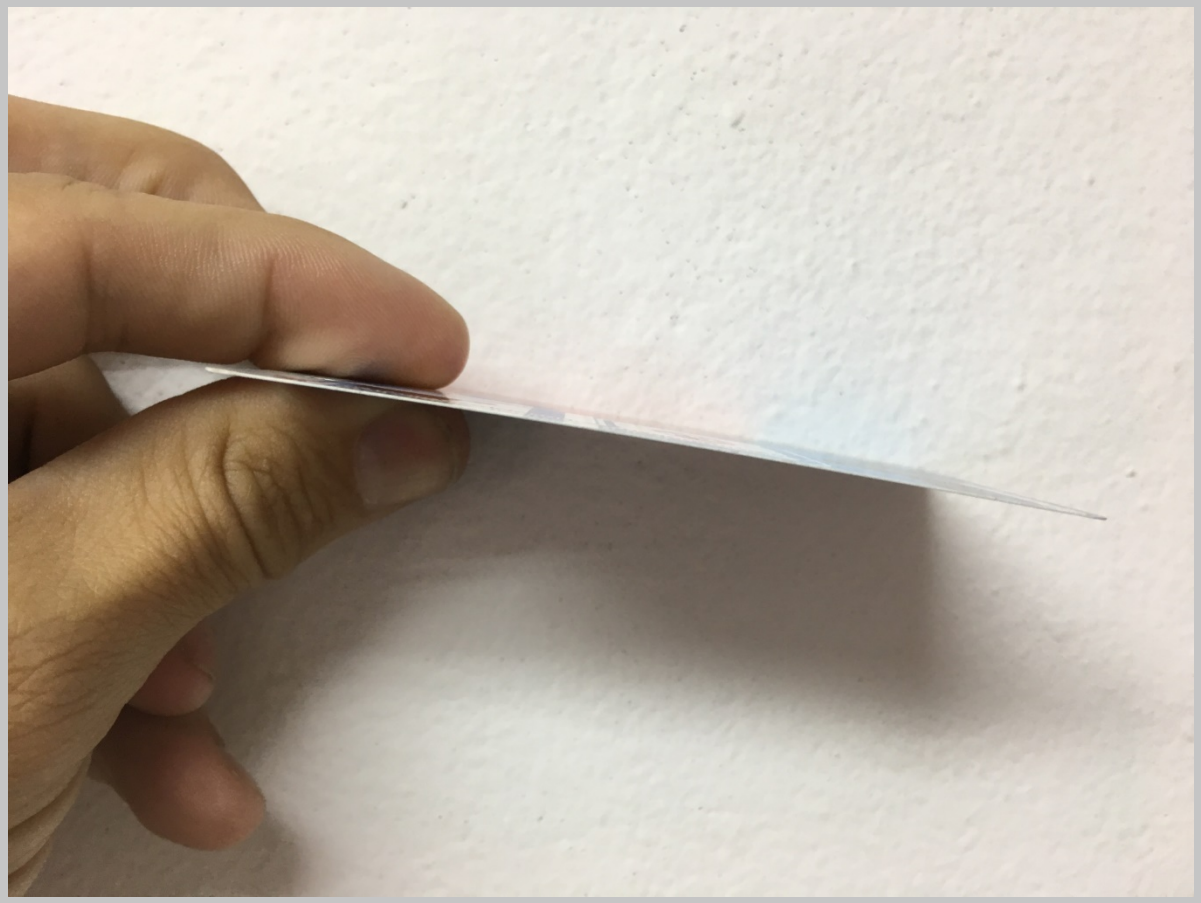
车票

- 设有两个磁条
- 打孔穿过其中一个磁条
- 薄厚仅0.27毫米

车票


สตรีมีครรภ์หรือผู้ที่จำเป็นต้องใช้ประตูพิเศษ
กรุณาติดต่อพนักงานนะครับ
Pregnant women, or other passengers
in need of assistance, please contact
BTS staff to enter or exit through
the swing gate.
ตั๋วโดยสารรถไฟฟ้าบีทีเอส ประเภทเที่ยวเดียว
BTS Single Journey Ticket
BTS Single Journey Pass
BTS One-Day Pass
Bangkok Local Museum (Bangrak)
(Bangkok's Folk Museum)

车票



闸门

- 进站
- 出站









为什么选择他们?

- 真的只有磁条吗?
- 一定还有其他东西!
- 长久以来饱受威胁
- 不得不继续前进...



设备

- 标准读/写器
- 中国制造
- 标准或原始读数
- 错误罕见
- 可靠的性能



问题

- 数据位置
- 编码方案
- 数据变化
- 数据含义
- 系统响应
  - 数据篡改
  - 重复状态或无序转换

实验室工作

- 读取磁条
- 解码数据



实验室工作

E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438
E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438
0x00

E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A
E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A
0x00

实验室工作

- 尝试标准解码
  - 国际标准化组织
  - 6位字符集和4位字符集
  - 有些使用奇偶校验，有些则不使用
- 尝试对其前后数据解码
- 未使用相关标准

实验室工作

E0E64211A5 7826 FC2E843A ~~00FF74~~ 00C20EFCE0933438

~~E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438~~

0x00

~~E0E64211A5~~ 5826 E62E8E0A ~~00E0E64211A55826E62E8E0A~~

~~E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A~~

0x00

Known

Duplicate

* The section marked “Known” is always 100 + the price of the ticket



实验室工作

- 没有加密
- 没有奇偶校验
- 没有纵向冗余检查（LRC）
- 没有时间戳



现场工作

- 在城铁系统中使用车票
- 每次使用不同输入值
- 观察数据变化
- 通过变化来确认其含义

现场工作

~~E0~~E64211A5 ~~7826~~ FC2E843A ~~00FF74~~ 00C20EFCE0933438

~~E0E64211A5 7826 FC2E843A 00FF74 00C20EFCE0933438~~

~~E0E64211A5~~ ~~5826~~ E62E8E0A ~~00E0E64211A55826E62E8E0A~~

~~E0E64211A5 5826 E62E8E0A 00E0E64211A55826E62E8E0A~~

Known

Duplicate

Never Changes (Station to Station, Year to Year)

Overwritten on Use

现场工作

Date	Baht	Station	GUID	First	GUID		Second
2017	15	Ari	D0403AE7	F51CC51D	00D60F	F5A8 8 9A6C5	D01CCF12
2017	22	Ari	E0406C15	F52CD5A9	00D60F	F5A8 8 AA67B	E12CDD95
10/23/2017	16	Ari	A341760E	B02D364D	00D20F	B081 A 6087B	A42D3E71
10/23/2017	16	Ari	7A4101A9	B02DA6D4	00D60F	B081 A 72AC5	7A2DAE36
9/1/2018	16	Ari	78401A32	E91E76ED	00D20F	E948 A E0A41	781C7D55
9/19/2018	16	Sanam Pao	E542D0B4	FB1EA6FC	00C20E	FBD8 8 D38D2	E51EAECA
9/20/2018	16	Sanam Pao	E64211A5	FC2E843A	00C20E	FCE0 9 33438	E62E8E0A
9/30/2018	16	Ari	32404A91	062FF509	00D60F	0631 D 72460	322CFF14
9/30/2018	23	Ari	FF421002	061F35FF	00D60F	0631 D 72498	001F3DD1
10/7/2018	16	Ari	03430838	0D2F7759	00D20F	0D69 7 408E8	042F7F78
10/19/2018	140	Sanam Pao	E9D69E36	192FE79A	N/A	N/A	E92EE6CF
11/1/2018	140	Sanam Pao	E9D64094	262FF7C9	00820E	2631 7 E1CC0	E92EF6A3

GUID		Second
801C0F	E948 D 8681B	781C7D55
801C0F	0D69 9 D6A2C	042F7F78
801C0F	19C9 D 5EA0A	E92EE6CF
00060F	2631 E 58E52	E92EF6A3

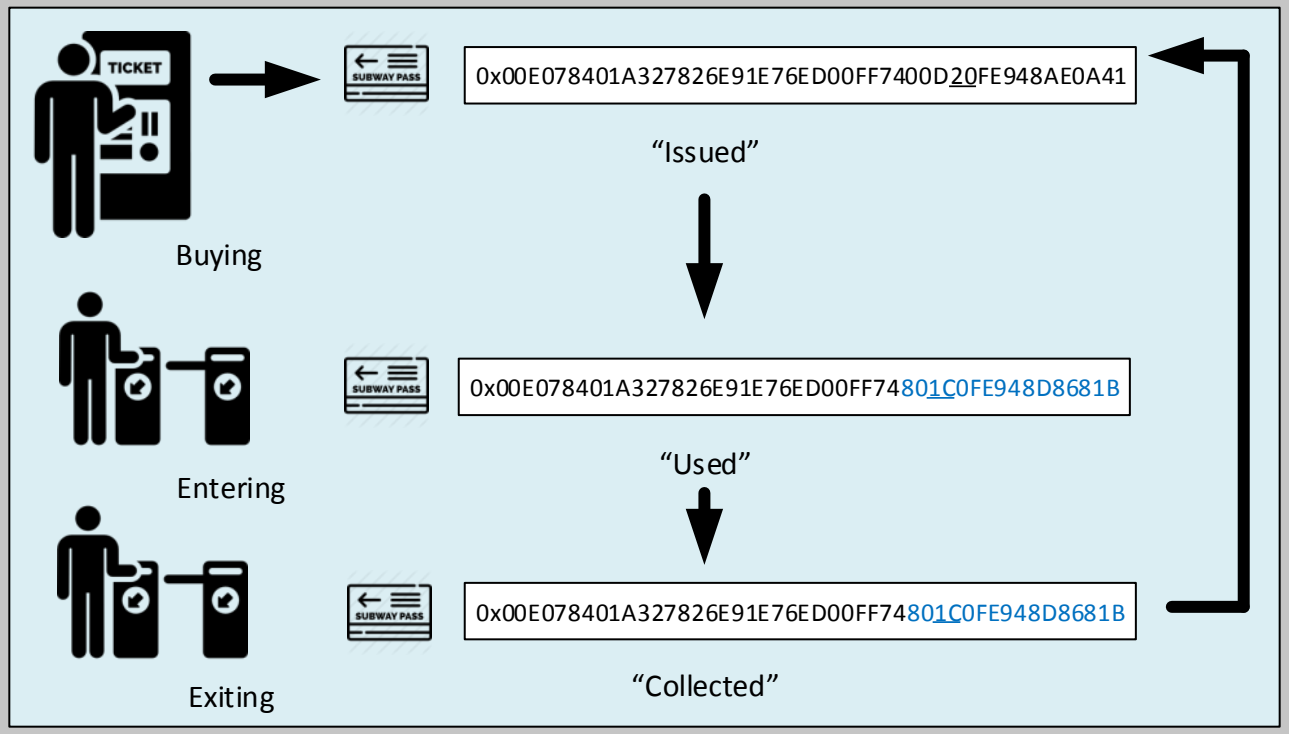
Station

Dispenser

Station

Turn-style

现场工作


TICKET
SUBWAY PASS
0x00E078401A327826E91E76ED00FF7400D20FE948AE0A41
"Issued"
Buying
SUBWAY PASS
0x00E078401A327826E91E76ED00FF74801C0FE948D8681B
"Used"
Entering
SUBWAY PASS
0x00E078401A327826E91E76ED00FF74801C0FE948D8681B
"Collected"
Exiting

现场工作

- 对于单日票，已知部分或者“100+价格”部分，被用来追踪行程
- 单日票有一项独特的“永不变更”项

处理规则

- 进站，
  - 购票前，车票必须处于“collected”状态
  - 进站前，车票必须处于“Issued”阶段
- 出站，出站前，车票必须处于“Used”状态

军政府的研究

- 局势
- 合法权益



尽量不被逮捕

- 躲避安检
- 浸渍
- 终极手段



当地文化

- 因扰乱秩序而受罚
  - 不会留意
  - 不会关心
  - 哪些规程?
- Avoiding Farang

利用该系统



- 当前已知信息
- 系统安全措施
- BTS的假设
- 对假设进行攻击
- 史诗般的失败!







当前已知信息

- 基于对象
  - 物理对象
  - 数据库对象
- 属性
  - 识别
  - 值
  - 位置

当前已知信息

- 状态
  - Issued
  - Used
  - Collected
- 历史

系统安全措施

- 交通卡的组成和设计
- 镜像物理对象和数据库对象
- 处理规则定义了如何有效使用对象
- 使用周期限制为24小时
- 交通卡用完后将被回收

BTS的假设



- 没人能复制我们的交通卡
- 我们的系统只存在有效对象
- 处理规则能够防止车票并发使用
- 使用周期的限制降低了损害的发生
- 使用后，车票将在我们手中

对假设进行攻击



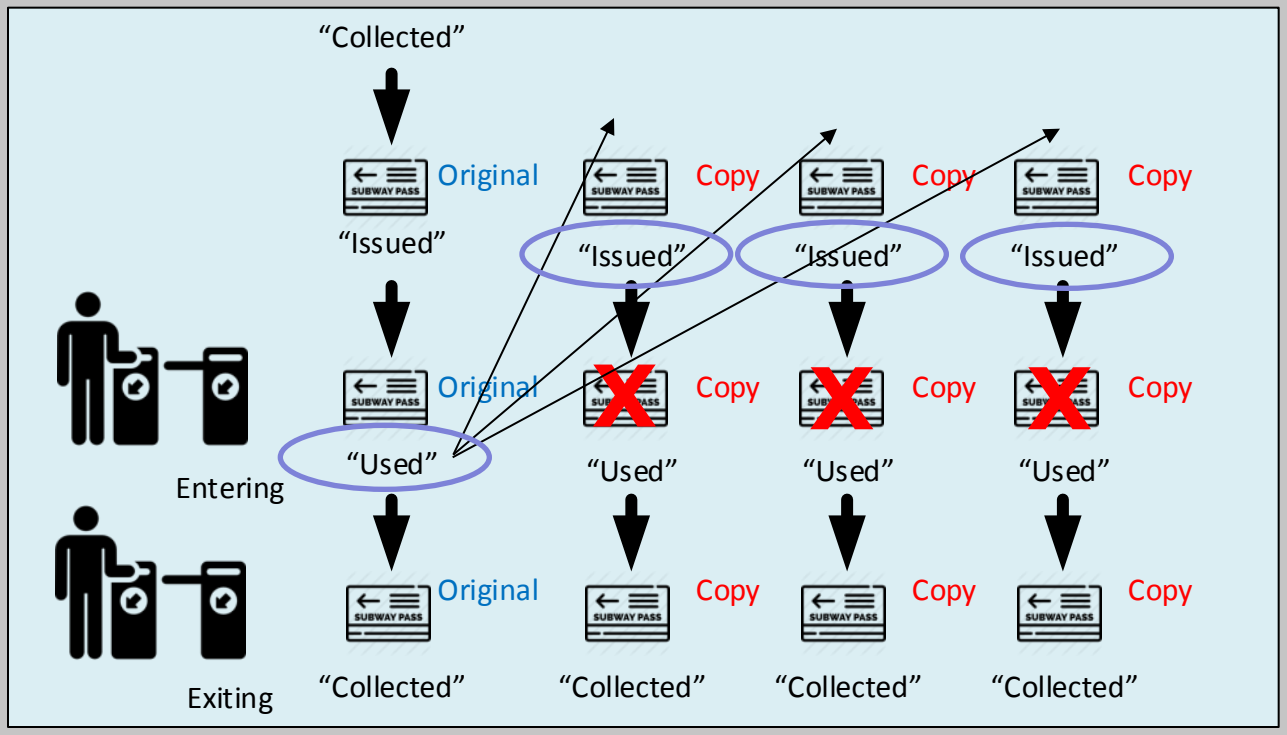
- 获取合适的车票
- 捕捉有效对象
- 绕过规则
- 扩展攻击以增加损害



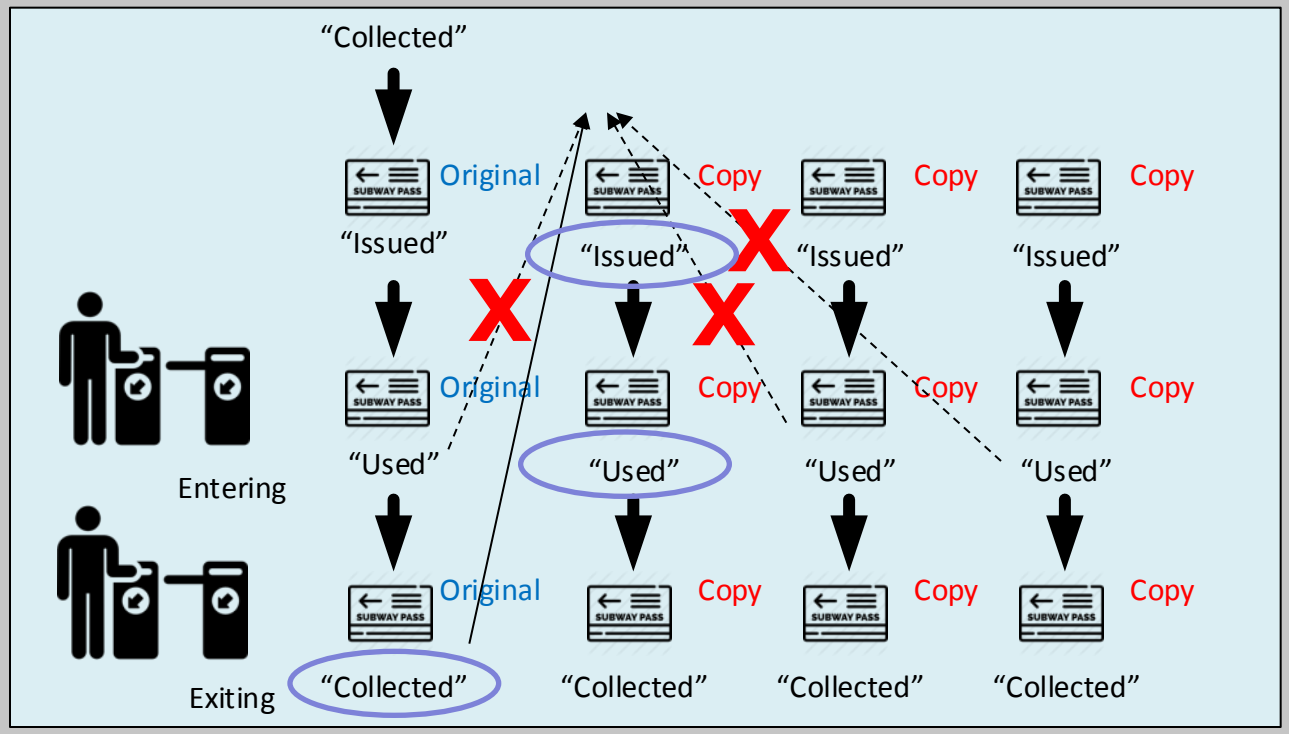
史诗般的失败!

- 制作空白车票
- 复制大量处于“Issued”状态的对象
- 发现处理规则中的缺陷
  - 在当前使用周期中寻找“Collected” 状态
  - 覆盖其他所有状态!
  - 对象最近的状态都为“Collected”
  - 运行原始车票
  - 所有复制票立即生效

史诗般的失败！


“Collected”
Original
Copy
Copy
Copy
“Issued”
“Issued”
“Issued”
“Issued”
Original
Copy
Copy
Copy
“Used”
“Used”
“Used”
“Used”
Entering
Original
Copy
Copy
Copy
Exiting
“Collected”
“Collected”
“Collected”
“Collected”

史诗般的失败！


"Collected"
Original
Copy
Copy
Copy
"Issued"
"Issued"
"Issued"
"Issued"
Original
Copy
Copy
Copy
"Used"
"Used"
"Used"
"Used"
Entering
Original
Copy
Copy
Copy
Exiting
"Collected"
"Collected"
"Collected"
"Collected"

史诗般的失败！



			Before Use	After Use
			First Magstripe (Hole)	First Magstripe (Hole)
Date	Baht	Station	Track #1	Track #1
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 801C0F 0D699D6A2C
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 80040F 0D699F6834
10/7/2018	16	Ari	0x00E0 03430838 7826 0D2F7759 00FF74 00D20F 0D697408E8	0x00E0 03430838 7826 0D2F7759 00FF74 80040F 0D69D26878
11/1/2018	140	Sanam Pao	0x00E0 E9D64094 B846 262FF7C9 00FFF0 00820E 26317E1CC0	0x00E0 E9D64094 B846 262FF7C9 00FFEF 00060F 2631E58E52
11/1/2018	140	Sanam Pao	0x00E0 E9D64094 B846 262FF7C9 00FFF0 00820E 26317E1CC0	0x00E0 E9D64094 B846 262FF7C9 00FFEF 801C0F 2631E5EEA8

史诗般的失败！ （示范）



将漏洞转为攻击

- 车票
- 计划









车票

- 寻找卡片
- 打孔

寻找卡片

- 阿里巴巴的建议邀请书
- 运行试验
- 中标!













阿里巴巴的建议邀请书

- 成千上万的公司（可能数百万）
- 告诉他们你想要什么
- 任何你需要的！
- 他们会为你做的

运行试验



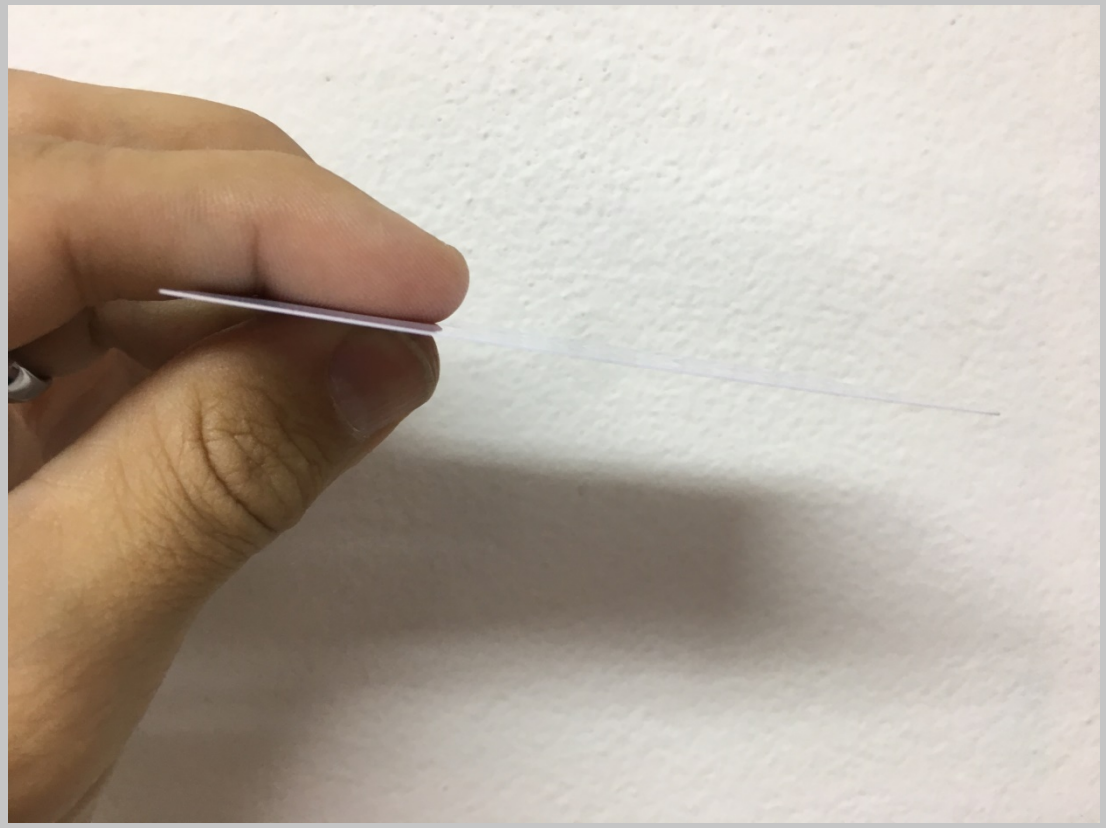
- 很多提供者
- 只有一家公司合格
- 无法满足卡片所需的厚度
- 花了好几个月才找到他们

中标！





中标!



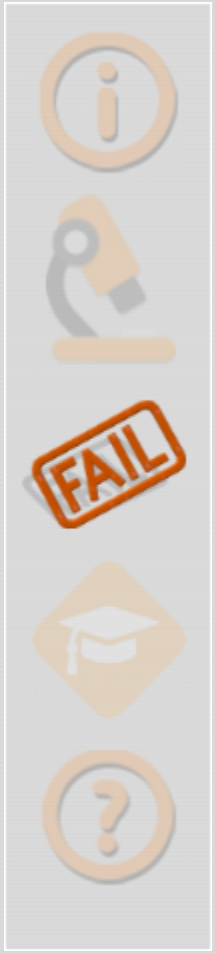
打孔





打孔





计划

- 购票（单日票）
- 复制车票
- 使用原始车票
- 分发复制品
- 玩的开心!
- 明天接着来!

攻击结果

Attack			Damage	
Daily Pass	Counterfeits		Baht	US
฿140	฿15	5	฿700	$ 22.58
฿140	฿30	10	฿1,400	$ 45.16
฿140	฿3,000	1,000	฿140,000	$ 4,516.13

1 Month	฿4,258,333	$ 137,365.59
6 Months	฿25,550,000	$ 824,193.55
1 Year	฿51,100,000	$ 1,648,387.10
5 Years	฿255,500,000	$ 8,241,935.48

Extend the attack!

BTS GROUP

对BTS的影响

- 数百万美元的损失
- 丢脸!



BTS的回应

- 你哪位?
- 不感兴趣!



经验总结

- 对于我们
- 对于BTS



对于我们

- 没有只针对硬件的解决方案
- 解决方案通常很复杂
- 软件无处不在
- 相信假设是危险的
- 不要害怕研究方向
- 行动前明确风险
- 制定包含所有相关方的计划

对于BTS

- 不要让社会习惯蒙蔽双眼
- 不是所有人都按照你的想法和思维做事
- 乐于沟通，坦然交流
- 用证据说话
- 亡羊补牢，为时不晚

避免重蹈覆辙



- 测试解决方案中的所有层级
- 测试应用程序
- 检查你的假设是否合理
- 使用补偿和缓解机制

他们如今在做什么

- 部署第二代系统
- 仍然没有分享渠道
- 仍然忽视“错误的人”
- 仍然无视我



最终感想

- 交通系统很有趣
- 同时也会带来麻烦
- 不去尝试就永远不会知道
- 逆向工程是关键
- 你有种!
- 不要相信那些天花乱坠的宣传
- 应用安全的胜利之路!



链接

- https://wikileaks.org/wiki/Anatomy_of_a_Subway_Hack_2008
- https://file.wikileaks.org/file/anatomy-of-a-subway-hack.pdf
- https://defcon.org/images/defcon-16/dc16-presentations/anderson-ryan-chiesa/47-zack-reply-to-mbta-oppo.pdf
- https://www.computerworld.com/article/2597509/def-con--how-to-hack-all-the-transport-networks-of-a-country.html
- https://www.cio.com/article/2391654/android-nfc-hack-enables-travelers-to-ride-us-subways-for-free--researchers-say.html
- https://www.youtube.com/watch?v=-uvvVMHnC3c
- https://www.blackhat.com/docs/asia-17/materials/asia-17-Kim-Breaking-Korea-Transit-Card-With-Side-Channel-Attack-Unauthorized-Recharging-wp.pdf

链接

- https://www.msrdevice.com
- https://www.msrdevice.com/product/misiri-msr705x-hico-magnetic-card-reader-writer-encoder-msr607-msr608-msr705-msr706
- https://www.alibaba.com/
- https://nexqo.en.alibaba.com
- http://www.nexqo.com/
- https://www.bts.co.th/
- http://www.btsgroup.co.th


Q&A