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.

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

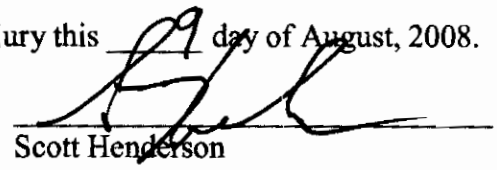
single industry voice for smart card technology, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

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

Sent from my Verizon Wireless BlackBerry