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.