



**Smart Card
Alliance**

Transit Payment System Security

A Smart Card Alliance Transportation Council White Paper

Publication Date: August 2008

Publication Number: TC-08003

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About 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. 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 cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.

Copyright © 2008 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Table of Contents

TRANSIT PAYMENT SYSTEM SECURITY	4
SUMMARY OF RECENT SECURITY RESEARCH.....	4
TRANSIT PAYMENT SECURITY: SYSTEM-LEVEL CONSIDERATIONS.....	5
THE ECONOMICS OF FRAUD	6
EXAMPLE SECURITY MEASURES IN USE BY TRANSIT AGENCIES	6
TECHNOLOGY UPDATES AND SECURITY	7
DETECTING, PREVENTING AND REACTING TO FRAUD	8
KEEPING CUSTOMER INFORMATION SECURE	8
CONCLUSIONS	9
ABOUT THE SMART CARD ALLIANCE TRANSPORTATION COUNCIL	9

Transit Payment System Security

Transit agencies worldwide have implemented automatic fare collection (AFC) systems that use contactless smart card technology for transit-issued fare media. These systems are popular since they deliver fast, easy access to riders and reduced operating costs and improved efficiencies to transit operators.

Recently, questions about the security of these systems arose when researchers reverse engineered one contactless chip product – the MIFARE Classic product – that is used in many transit AFC systems. The Transportation Council of the Smart Card Alliance prepared this white paper to discuss this research and to outline the approaches that the transit industry uses throughout its payment systems to ensure the security of transactions and data.

The MIFARE Classic product was introduced over 10 years ago as one of the original contactless integrated circuit (IC) products and used encryption and design strategies consistent with the time of development. Since then and since the completion of the ISO/IEC 14443 contactless smart card standard, multiple vendors introduced a variety of contactless IC products. Many of these products incorporate more modern and sophisticated designs and are used in global transit projects and other applications. These newer products have not been exposed to the recently announced breach.

It is also important to remember that while the contactless smart card technology that is used by both transit and financial industries operates on the 13.56MHz frequency band, there are vast differences among the contactless applications and security approaches used.

For example, the MIFARE Classic product is not being used for open bank card payments in the U.S. or in countries implementing EMV¹; these applications have additional security, functionality, and flexibility requirements. **Transit agencies who are implementing fare payment systems that accept contactless credit and debit cards issued by the financial industry or that use other contactless IC products are not affected by the recent breach.** Organizations issuing private label cards, gift cards, retailer cards, and other prepaid cards should continue to follow industry best practices when establishing specifications for payment application requirements (e.g., functional, security, performance) and should perform rigorous review and certification processes to ensure the appropriate level of security is implemented.

As discussed in this white paper, the careful application of contactless IC products and sound system architectural infrastructure, along with proactive strategies and approaches to analyze and oversee operations, will provide transit agencies with confidence in the integrity of their fare collection systems.

Summary of Recent Security Research

During an information technology conference held in Berlin (Germany) in December 2007, a group of researchers indicated that they had successfully reverse-engineered a MIFARE Classic chip.

MIFARE Classic – part of the MIFARE product family, which is owned, developed and licensed by chip technology provider NXP Semiconductors since 1994 – is widely used in different applications requiring contactless proximity transactions with a typical read/write distance of up to 4 inches. The most common applications include fare media in public transport, access management and event ticketing.

Other groups, including university information technology security specialists, were also able to retrieve the algorithm and develop attack scenarios to identify the MIFARE Classic keys within a few minutes of computer analysis time.

¹ Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals. EMV-based credit and debit cards are now being issued and used in Europe, Latin America, Asia Pacific and Canada.

The ability to retrieve the keys is closely related to the length of the keys. When MIFARE Classic was introduced over a decade ago, keys were no longer than 48 bits, which makes a brute force attack today faster and easier than is possible with more recent chip technology. The latest smart card chips use state-of-the-art encryption, such as 3DES and AES, with key lengths of over 100 bits. This reduces the attractiveness of brute force attacks since they take exponential orders of magnitude more time and computing effort. Third party security certifications, such as Common Criteria, also provide a higher security standard for smart card chips.

In order to understand how an algorithm can be retrieved, the concept of “reverse engineering” needs to be understood.

Reverse engineering is a technique that is used to identify the algorithm implemented in a chip by analyzing how all of the transistors on the chip are connected to each other. This analysis requires a variety of tools, including a means for controlled delayering of the chip (etching). Tools such as high-end optical microscopes and automated pattern analyzers are needed at a minimum. This highly sophisticated process reveals the functionality of the chip, including the security-relevant part, but does not actually reveal the cryptographic method itself or the secret keys.

Having access to the algorithm, however, facilitates the extraction of keys which can impose certain risks of card manipulation in a system.

After the algorithm is known, attackers would still need to develop other cryptographic attacks in order to discover the keys which would enable them to compromise the integrity of data stored on the contactless chip. But even then, depending on the chip's usage in the entire security system, the compromise is likely to be limited to obtaining a single card's secret keys, which are not the same for all cards. This makes reverse engineering unattractive for a professional hacker.

It is also important to remember that the security approach designed into a single card is only one element in the security designed into an overall system. The system-level security features of a well-designed system greatly inhibit a criminal's ability to do widespread damage even if a single element has been reverse engineered.

This white paper explores typical system-level security mechanisms that are used to prevent, detect and react to fraud in public transportation fare collection systems that use transit-issued fare media, thus mitigating the risk of tampering at the card level.

Transit Payment Security: System-Level Considerations

Security is not an element in a system that should be added on: it is a core element in the design of the entire end-to-end solution. This is an important consideration, since a properly designed system greatly reduces the risk of compromise due to the failure of any single component.

Security design is based on the principles of prevention, detection and reaction. All security systems are designed with the basic assumption that someone will figure out how to breach any defenses that are created. For this reason, the design must include detection and reaction measures in addition to prevention measures.

Prevention refers to the design elements that are used to make it difficult for a criminal to earn a living by stealing from a business. In the case of transit systems, prevention is typically based on making it very difficult to counterfeit the contactless smart cards that are used to pay fares, to trick the system into thinking a different card is a legitimate fare card, or to add value to a legitimate card without paying. Preventive measures include card security, reader security and system tests. Examples of security measures used in transit are discussed later in this paper.

Detection is a critical element of any security system. Knowing when a counterfeit card has been successfully used is essential to confining losses to small amounts. All transit systems include transaction audits and reporting measures that enable security features to detect improper use.

Reaction refers to the measures available to the system owner to prevent the successful attacker from repeating the process. Security is a “cat and mouse” game. The expectation is that the

motivated criminal will work to break through a system's defenses, but it is also expected that the system will be able to detect the attack such that experts can understand how the breach was achieved and design and deploy effective countermeasures to prevent further loss from that approach. Most transit systems include the capability to make rapid changes to critical defense mechanisms to confine losses while this process goes through the defined cycle.

Transit agencies should discuss system-level security features with their vendors to understand the security that exists in their systems. It may be worth a dry-run of these mechanisms to make sure the operating staff has experience before any crisis arises.

Most security experts believe that security cannot be achieved through secrecy. The best systems reveal how they provide security and challenge legitimate hackers to try and overcome their defenses. Systems that pass "ethical hacks" are generally stronger than those that depend on hidden measures for the obvious reason.

The Economics of Fraud

The cat and mouse game of fraud is not inexpensive for the criminal. A hacker may learn how to beat a system, but gaining real commercial value from that knowledge is a different matter. The source of losses in payment systems is from educated and well-funded criminals performing systematic attacks, not from the occasional hacker beating the system in order to enjoy bragging rights. Thus, an important consideration in evaluating the security of the system is to understand the value of beating it.

Transit systems typically offer services at a low cost. For this reason, a large scale operation would be required to create enough fake cards or fake loading systems to provide an economic return to the criminal. Keep in mind that the detection systems mentioned above will severely limit the usefulness of any individual counterfeit card or reload scheme. How much would a criminal make by producing millions of cards that offered a day pass for the local transit agency? When compared to the benefits of beating more general payment systems (e.g., ones that allow the purchase of goods that can be fenced), the economics for transit attacks don't appear to be very attractive to the criminal.

Nevertheless, bragging rights are powerful motivators, and the embarrassment of providing thousands of free rides makes the need for proper security very real. Transit agencies would be well served to understand the security capabilities of their systems.

Example Security Measures in Use by Transit Agencies

In general there are some commonly accepted guidelines for mechanisms to use for securing transit payment systems. Some approaches are simple, others more complex. What is implemented depends greatly on the specific situation, and especially the physical and financial resources that are available. This white paper is not intended to provide a comprehensive guide to all security measures, but covers examples of common practices.

No matter what type of system has been implemented, some commonly accepted practices should always be followed. For example, every transit employee that requires access to the system should be assigned a unique user ID and password or personal identification number (PIN). This gives the organization the ability to work backwards, starting with the last person to have access, to identify who was on duty, should something go wrong with the system. Another simple item is ensuring that a strong password policy is in effect. This means users cannot have simple passwords such as names or phone numbers, but would need a password that is a mix of letters and numbers and has a minimum length (6 characters seems to be common). Strong passwords ensure a high degree of difficulty for someone attempting to guess a password. Other such straightforward practices are:

- Using a closed network without a connection to the Internet or corporate network. This is one of the best ways to ensure no outside access is granted/gained.
- Linking the IP address to MAC address. This ensures a level of trust that the device is authorized to access your system.

- Using a physical security token such as a one-time password device or smart card for system access. This ensures a level of trust that the device and its holder are authorized to access your system,
- Using hotlists and immediately blocking access when specific IDs are entered or presented to the system.
- Using key diversification, to provide a higher degree of security by giving every card its own specific keys.

Organizations need to ensure that the integrity of their systems is maintained. No matter what is implemented, transit agencies should ensure that access to the system or specific areas of the system is based on a “need to know.” Everyone does not need access; everyone does not need universal access to all areas; everyone does not need full capabilities. In addition, the system shouldn’t rely solely on a single person or position to protect the system or the information it contains. For example, there should be defined roles and responsibilities associated with the definition of security keys and for access to those keys. No one person should have the entire knowledge needed to create keys or be the only individual to have access to them, since this would provide no safeguards if this person is compromised. While there needs to be a level of trust, there should also be programs in place that “keep everybody honest,” such as review of access logs.

Further, the focus on security shouldn’t be limited to the system that is being deployed, but should also cover the overall infrastructure that it will be deployed within. For example, within transit, there are many areas where it is just not feasible to have 24/7 coverage with personnel, so deployment of CCTV cameras is worth considering. Besides the fact that they work around the clock without needing breaks, they also provide a means of recording events, which can help later on in proving what occurred. Also, limiting physical access to the network and putting in place physical controls for those computers authorized to have access to the network are common practices. Other examples of security measures are:

- Installing locked network-only activated jacks.
- Installing and monitoring intrusion detection software and logs.

Technology Updates and Security

Why would a transit agency want to update technology? The agency may have just made a significant investment in a new system, which is supposed to be state-of-the-art. Many systems (even those that are state-of-the-art) are hacked into on a frequent basis. Normally, these systems have a flaw, which if left alone, will be exploited. Stagnant systems are just that – stagnant. Technology is constantly changing so, in order to remain state-of-the-art, the system needs to change as well. However, in changing the system, precautions need to be taken, since even an update that appears benign might open the door to a whole host of new issues.

Establishing some fairly simple guidelines for the organization will go a long way to ensuring that the system is safeguarded against unwanted attacks. Never implement changes from entities that are not known or certified. Also, not everyone in the organization should be allowed to make changes to their computers. These changes should be controlled by the system administrator; otherwise, the door is opened for security leaks with unsuspecting people unknowingly loading malicious applications.

Before any changes are deployed system-wide, they should be tested on a separate system. This allows the system to be safely checked for security flaws, an especially critical test when the system contains personal or sensitive information. In testing the system, adopting the requirements set by the Payment Card Industry Data Security Standard (PCI DSS) guidelines (as applied to credit and debit card processing) will help ensure the different parts of the entire system are checked and maintained.

Another aspect to consider before deploying any change to the system is to look at the business needs and determine whether the change is necessary.

Lastly, hiring an outside firm to audit network security and conduct random checks to see if there are any holes through which attackers could gain access isn't a bad idea. It provides an independent unbiased assessment of the system.

Detecting, Preventing and Reacting to Fraud

Even after following the suggestions above, mechanisms need to be implemented to proactively scan the system to detect and react, as early as possible, to any activity that suggests that someone is trying to use the system fraudulently. Currently, most financial institutions have programs in place that raise flags based on certain types of activities that are detected. For example, charges being made to the same credit card in two different geographical locations should set off alarms. Similarly, within transit, detection of a card being used at two locations relatively simultaneously should raise a flag.

Other monitoring can verify that sales transactions match revenues. If someone has found a way to manipulate the transit card and, for example, add more value, there will not be a corresponding sales transaction record captured in the database. Some ways to proactively detect this would be to conduct random history checks with card usage versus card updates.

Another potential opening for fraud exists with the "auto renew" programs that are often in place in a transit system. For example, transit passes for employers within the transit area should continually be checked for employees that no longer work for those entities so that their passes can be disabled.

Keeping Customer Information Secure

In today's world, the security of personal information is of ever-increasing importance. However, in order to provide improved and/or targeted services, transit agencies need to collect certain personal information. It is critical that transit agencies have in place mechanisms to ensure that this information cannot be compromised and, if there is unauthorized access to systems, that other systems are in place to prevent access to all information that could be obtained.

From the consumer's point of view, transit smart cards are very secure, as most systems feature rider anonymity on the card. A few exceptions exist, for example, with people who qualify for special fares. In this case, the consumer uses a registration process to personalize the card with a picture and electronic information specific to the entitlement and the individual. Even in this case, the card, if registered, usually contains a unique number which can then be used only by the back office to determine the owner.

Customer data is typically held at the back office and is not stored on the card itself. However, the value of obtaining this information is limited and concerned individuals could opt out of programs that require it. For the most part, even when cards are registered for balance protection or autoloading features, transit systems manage personal data at the central system and follow published security system standards to design necessary protection. When using this approach, it is also important that all of the personal information not be located within the same database. Such information should be spread across different databases housed in physically separate systems. Again, the purpose is to protect sensitive data, so that if one area is compromised, not all of an individual's data is available.

The PCI DSS and best practices guideline provides a very good starting point for transit agencies to use when designing how to manage customer information. Implementing PCI within the transit agency for credit and debit payment processing is required, and may also be useful to adapt to other parts of the system. Continually checking the system will help to ensure that personal information is handled in a secure manner.

Card registration should be done in a secure manner and require that the person registering the card creates a username, password, and security question in case the password is forgotten. This question is a way for the customer service agent to verify that the individual is most likely the owner of the card and account. Strong passwords should be required.

Access to personal information by employees is another area of critical importance. Virtually all security experts will agree that a system is more likely to be compromised from within the organization than by an external attack. Therefore, programs need to be in place that ensure access to information is on a “need-to-know” basis.

When access is necessary, the default should be read-only. Only certain employees should be able to make changes. Prior to changes being made, duplicate records should automatically be created.

Other programs that should be in place are:

- User audits, removing inactive users
- Computer permissions audits for access control
- Security reporting audit of individuals' activities on the system

Conclusions

Security is a core element of any payment or access system; a properly-designed system is not dependent on the security of any single component. No single security mechanism provides complete security and, indeed, complete security does not exist. The objective in any secure system design must be to implement the appropriate security measures to address the expected risks and threats to the system. The result should be that the time and effort required to compromise a system is greater than the gain to the organization or individual attempting the compromise.

Transit payment systems have traditionally been designed with multiple layers of security to prevent, detect and react to fraud. While the recent MIFARE Classic security breach may compromise security at the card-level, other security measures used in the transit payment system should limit the exposure that transit agencies have to possible criminal attacks. Transit agencies should work with their systems integrators to review their system security design and practices and understand the security measures that are in place to mitigate risk to the system.

About the Smart Card Alliance Transportation Council

This report was developed by the Smart Card Alliance Transportation Council to outline the approaches that the transit industry uses throughout payment systems to ensure the security of transactions and data and to discuss recent research on one contactless chip product that is used in many transit AFC systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Transportation Council is focused on promoting the adoption of interoperable contactless smart card payment systems for transit and other transportation services. Formed in association with the American Public Transportation Association (APTA), the Council is engaged in projects that support applications of smart card use. The overall goal of the Transportation Council is to help accelerate the deployment of standards-based smart card payment programs within the transportation industry. The Transportation Council includes participants from across the smart card and transportation industry and is managed by a steering committee that includes a broad spectrum of industry leaders.

Transportation Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects. Additional information about the Transportation Council can be found at http://www.smartcardalliance.org/about_alliance/councils_tc.cfm.

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.