Security of the Metro System Cards

Aaron Hunter, Cesar Corzo

***Abstract*—This project analyzes the security and implementation of farecards and smartcards used by the Metro in the Washington D.C. metropolitan area. Weaknesses in paper based farecards are briefly surveyed. The focus of this paper is a review of the vulnerabilities of the MIFARE Class cards and an investigation of the architecture and security features of newer MIFARE Plus cards.**

***Index Terms*—WMATA, Metro, MIFARE Plus, MIFARE Classic**

I. Introduction

BY 2015, there will be 60 megacities servicing 600 million citizens. [5] The need for a reliable and secure transportation system is necessary to provide and fulfill the growing need of mobility. Being the second largest metro network in the U.S., and located in and around the national capital, the security of the Washington Metropolitan Area Transit Authority (WMATA) Metro system is of significant importance. Many metro and subway systems of the world use Near Field Communication (NFC) based contactless smartcards equipped with security features for access control and fare collection purposes. These features protect transportation authorities, customers data and money against fraudulent use or unauthorized access.

MIFARE is a contactless smartcard technology that is widely used for in the metro and subway systems in the across the world. [1] Several of these systems have experienced flaws in both design and implementation automatic fare collection schemes.The MIFARE Classic cards were implemented in the 1990s, and the technology was designed with the intent of cost effectiveness and practicality. The processing power available to attackers has vastly increased since the Classic cards were developed, rendering the cryptographic schemes used by MIFARE Classic insecure. As a result, several vulnerable transit systems such as Londons Oyster card, Netherlands OV-Chipcard, and US Bostons CharlieCard have been documented in academic literature due to their use of MIFARE Classic cards.

The main purpose of this project is to analyze the security, and implementation of farecards and smartcards of the Metro in the Washington D.C. metropolitan area. There are now current technologies that implement stronger algorithms that make these smartcards harder to crack. This paper will investigate the internals of the MIFARE system and its derivatives including the architecture, communication protocols and implementation of software/hardware.

II. Metro Farecard System Operation

WMATA has a tri-reader supplied by Cubic. This reader can handle different kinds of smartcards and supports at different kinds of encryption. It also has a magnetic stripe reader to support paper farecards.

A. Hunter and C. Corzo are with George Mason University.
Manuscript revised December 16, 2012.

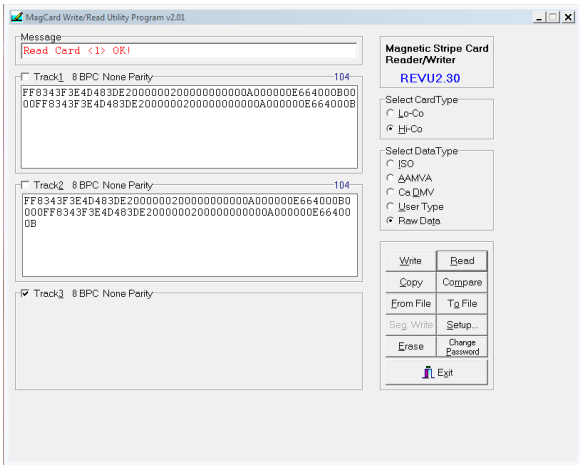

Fig. 1. Hexadecimal value stored onto paper farecard

A. Paper Farecard and Security

Paper farecards are used in many major metro systems, including WMATA. The D.C. metro uses this card with magnetic stripe technology. The simplicity of this technology makes farecards vulnerable and unlikely to be encrypted or secured.

For this research, the group got a hold of magnetic stripe reader/writer and three paper farecards with different values. The device can read the two tracks of the farecards and extract the raw data (hexadecimal) as shown in (Fig. 1). The three cards were mostly similar except for a few bytes. This implies two things: the cards are not encrypted (as we suspected) and the cards can be reverse engineered and forged. This was pretty similar to a hack done on Boston Metros CharlieTicket by Anderson, Russell and Chiesa. [3] [13]

The paper farecard maximum value is $45.00. So, if any hacker plans this kind of attack and decide he/she wants to keep low profile, a forge value must be under the limit.

B. Contactless Smartcards

It is pocket size card with embedded integrated chip. The card interfaces and is powered by the Radio frequency induction technology. The card comes with an embedded antenna. This card uses ISO 14443, a standard protocol to communicate with a reader.

The international standard for proximity or contactless communication is ISO-14443. The standard describes how smartcards and terminals must interface to ensure industry-wide compatibility. It operates on 13.56MHz and uses magnetic

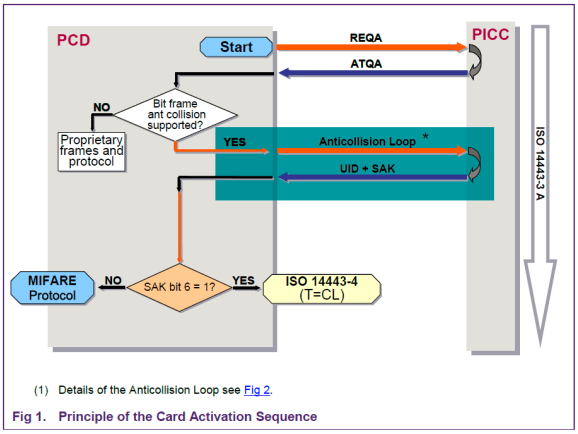

Fig. 2. Activation Sequence

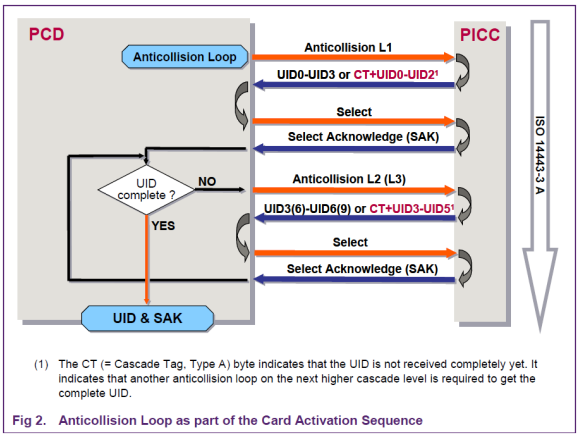

Fig. 3. Anticollision Loop as a part of the Activation Sequence

coupling between the reader (PCD) and the card (PICC). The standard is comprise of four layers: physical characteristics, radio frequency power and signal interface, initialization and anticollision, and transmission protocol. This protocol specifies two operation modes A and B. The principal differences between these types concern modulation methods, coding schemes and protocol initialization procedures.

III. MIFARE Cards Operation

In this project, the team researched 2 major Mifare chips: Mifare Classic and Mifare Plus. [1] The initialization and anticollision for both, classic and plus, are identical. The PCD (reader) typically polls for PICCs (cards) in the field. This is done with the REQA (Request Command, Type A). When a PICC is within the operating range of the PCD and receives the REQA, any MIFARE PICC returns the ATQA (Answer to request.). The content of the ATQA should be ignored in a real application, even though according to the ISO/IEC 14443 it indicates that the PICC supports the Anticollision scheme. The complete card activation sequence is shown in the (Fig. 2) and (Fig. 3). The bit 63 in the SAK (Select Acknowledge) indicates, whether the PICC is compliant to the ISO/IEC14443-4 or not. [12]

After this initialization sequence, MIFARE cards will initiate security level sequences as shown in (Fig. 4). These

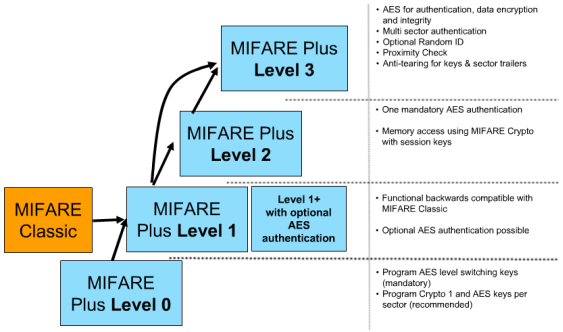

Fig. 4. State Transistions of the four Security Levels

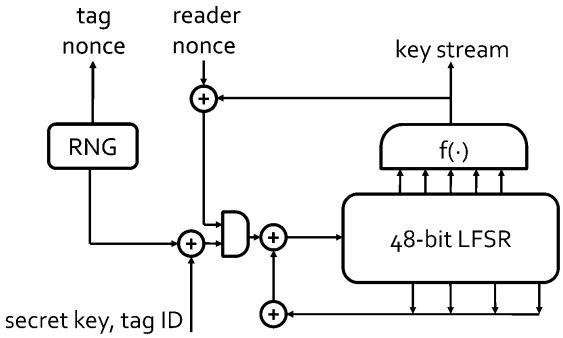

Fig. 5. Block diagram of CRYPTO-1 cipher

levels includes multi sector authentication and the use of cryptographic algorithms.

IV. Historical Attacks Against MIFARE Classic Cards

In December 2007, Karsten Nohl and Henryk Pltz presented the first attack against MIFARE Classic at the Chaos Computer Club. Before this time, the CRYPTO-1 cipher (Fig. 5) used by the Classic cards was a secret design of NXP. The keystream is derived from a 48-bit Linear Feedback Shift Register (LFSR) and a reducing function. Their attack method was to repeated turn the PCD (and hence the PICC) on and off and then eavesdropping on the communication between the PICC and PCD. The Psuedo Random Number Generator (PRNG) used by CRYPTO-1 is also based off an 16-bit LFSR, the value of which depends on the time when it is accessed. By controlling the time between when the PICC is powered up and when it is accessed, the PRNG will return the a consistent value, this will cause all parts of the cipher to be non-random and allowing the recovery of the secret key. [14]

A research group from Radboud University Nijmegen published an attack on Classic card on March 12th, 2008. In contrast to the hardware work by Nohl/Plotz, this paper summarises a protocol-based attack against the card and reader. It abuses the authentication protocol in order to reveal information about CRYPTO-1 cipher. A large table is produced by running the CRYPTO-1 cipher offline. Then authentication attempts are made with the genuine reader, by indexing the results in the table, the key can be recovered in several hours. [17]

Shortly after their first paper, the Nijmegen group released a preprint version of their second paper on March 15th, 2008. This paper would later be published in CARDIS 2008. This paper exploits a weakness in the PRNG that allows the keystream to be recovered without a key. There is another weakness that was exploited, which allows the first six bytes of any block to be read after eavesdropping on one transaction. Frequently, the last six bytes are able to be read also, leaving only four unknown bytes in each block of a given sector. For the keystream recovery attack, an eavesdropped and record conversation will be required. [18]

Nohl also worked with Nicolas T. Courtois and Sean O'Neil to create a so called algebraic attack against MIFARE Classic, which involves writing a large number of simple equations that relate message text, ciphertext, and IV bits. By solving these equations, the key is able to be obtained. It is claimed that this attack is an order of magnitude faster than previous attacks and do not require active interaction with the card or reader. Only one transaction has to be eavesdropped on.

> We can recover the full 48-bit key of MiFare Crypto-1 algorithm in 200 seconds on one 1.66 GHz Centrino CPU, given 1 known IV and 50 output bits (from one single encryption). With 4 chosen IVs we can recover the key in 12 seconds.

The output bits can be obtained by the technique used by the second Nijmegen paper. [15]

Nohl also documented and expanded on the earlier work done with Plotz with his third paper published on July 31st, 2008. In this paper, they show how they reverse engineered the Classic chip. They first dissolved the cards to gain access to the chips inside. This was followed by sanding away the covering of the chip revealing the layers of circuitry inside. These layers were photographed under a microscope and imaged processed to properly reconstruct the layers in software. Pattern matching was used to identify and translate the transistors in the layers to gate and register level logic. While this work was painstaking, it was not overly complex. This work was done by researchers using relatively simple tools. The authors also noticed that there were weaknesses in the PRNG that allowed random nonces to be frequently repeated. Based on this evidence, attacks that are far more efficient than brute force are possible. [16]

The third paper from the Nijmegen group, published Oct 6th, 2008, presented two attacks against MIFARE Classic.The first attack precomputes a 1 TB table based on the offline use of the CRYPTO-1 cipher. Then 4096 authentications are performed with a card reader. This takes between 2-14 minutes. The second attack uses one or two partial authentications between a genuine card and reader in order to recover the key in 0.05 seconds. This attack requires the challenging ability to eavesdrop on the communication between PICC and PCD in order to recover the keystream. [19]

The final Nijmegen paper, published in May 2009, details a card-only attack that is able to be executed using 4096 authentication attempts, with a 384 GB table that holds internal states of the cipher. Nicolas T. Courtois later proposes a technique in July that uses only 300 card queries and no precomputation. This card-only attack is able to clone a card in less than ten seconds. [21]

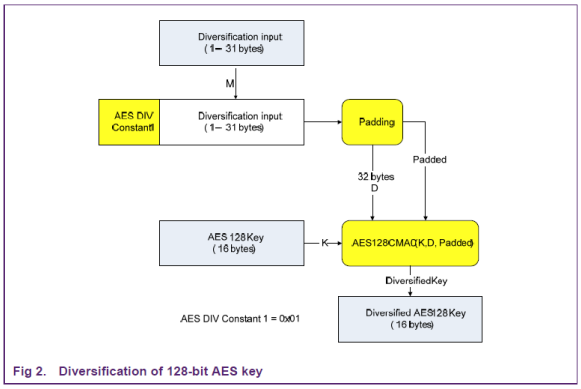

Fig 2. Diversification of 128-bit AES key

Fig. 6. Key Diversification Scheme For AES Keys

V. MIFARE Plus Security Assessment

NXP has learned from mifare classic chip failures, and came with a better chip which tackle most, if not all, of MIFARE classic chip weaknesses. MIFARE Plus was developed as a replacement from its predecessor.

- MIFARE Plus offers a mutual authentication between the reader and the card, and it is bidirectional using AES module. This means both card and reader share the same secret key, symmetric encryption. Thus, ensuring confidentiality. [11]
- Proximity check ensures that a smartcard is physically close to the reader. [8] [11]
- The integrity of the communication can be implemented by attaching a MAC generated by the AES-based CMAC module over the messages.
- MIFARE Plus supports key diversification schemes (Fig. 6) which it is highly recommended to prevent different cards use the same key. [10]
- The use of sessions keys during authentication.

VI. Current SmarTrip

The WMATA has been using the GO Card based SmarTrip since it was introduced in 1999. The GO Card is developed by Giesecke & Devrient (G&D) and uses a Fujitsu chip with FeRAM technology. [7] The GO Card offers 3DES authentication and uses ISO 14443 type B (not MIFARE). Fujitsu has discontinue manufacturing this chip and metro authorities has selected Mifare Plus as a replacement. The WMATA is transitioning to this new technology. [4] [6]

Smartrip with Mifare Plus X chip must come with at least 6-byte (implying 7-byte chips will be use for operation) and must have at least 2KB of memory. WMATA defined the use of AES-128 for encryption and must support key diversification using the manufactured chip ID (UID). Smartrip accommodates standard card personalization, initialization, and anticollision. [6]

	GOCard	MIFARE Plus
Protocol	ISO 14443 type B	ISO 14443 type A
Crypto	3DES	128-bit AES
Memory	2KB	2KB or 4KB
Op. Frequency	13.5 MHz	13.5 MHz
Chip Manufacturer	Fujitsu	NXP

Fig. 7. Comparision of features between GO Card and MIFARE Plus

VII. Conclusion

It is well-known that it is not possible to implement a security system that is 100% secure, there will be always some kind security holes. Our brief analysis of paper farecards showed us that this type of card technology is not secure and prompt to attacks by either cloning or forging. The group analyzed the Mifare Plus technology, which smartrip cards recently introduced, and have not found any significant weaknesses in the chip technology. NXP introduced a solid smartcard architecture, great chip design, and the cryptographic module (AES-128) is considered secure. The selection of MiFare Plus X by WMATA is a step in the right direction as long as it implements the aforementioned techniques to prevent fraud.

References

[1] MIFARE. Wikipedia, the Free Encyclopedia. Wikimedia Foundation, Inc., September 18, 2012. http://en.wikipedia.org/w/index.php?title=MIFARE&oldid=509828434.

[2] Mifare.net:: MIFARE DESFire EV1, n.d. http://mifare.net/products/mifare-smartcard-ic-s/mifare-desfire-ev1/.

[3] Exclusive Interview with MIT Subway Hacker Zack Anderson. Popular Mechanics, n.d. http://www.popularmechanics.com/technology/how-to/computer-security/4278892.

[4] Raschke, Kurt. Raschke on Transport — Transport News and Analysis. Raschke on Transport, September 11, 2012. http://transport.kurtraschke.com/.

[5] Kraas, F. Megacities and Global Change in East, Southeast and South Asia. In The German Journal on Contemporary Asia, 103. Bonn, Germany, 2007. http://www.asienkunde.de/asienzeitschrift/2007/103.html.

[6] WMATA. MIFARE Cards. Request for Proposal, November 29, 2011. http://wmata.com/business/procurement_and_contracting/solicitations/uploads/CQ-12089 11 28 11A MiFare Cards Final Nov29.pdf.

[7] Giesecke & Devrient. Go Card brochure. Technical Data. http://www.gi-de.com/gd_media/media/en/documents/brochures/government_1/GO-CARD.pdf

[8] NXP Application Note AN10969. System Level Security measures for MIFARE installations. Rev 1.0. August 10, 2010.

[9] NXP Application Note AN10957. Generic Access control data model. Rev. 1.1. March 7, 2011.

[10] NXP Application Note AN10922. Symmetric Key Diversification. Rev. 1.3. March 17, 2010.

[11] NXP MF1SPLUSx0y1. Mainstream contactless smart card IC for fast and easy solution development. Rev. 3.2. February 21, 2011.

[12] NXP Application note AN10833. MIFARE Type Application procedure. Rev. 3.2. August 29, 2011.

[13] Anderson, Russell, and Chiesa. Anatomy of a Subway Hack. Spring 2008. http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf

[14] Karsten Nohl and Henryk Pltz. Mifare, little security, despite obscurity. Presentation on the 24th Congress of the Chaos Computer Club in Berlin, December 2007.

[15] Nicolas T. Courtois, Karsten Nohl, and Sean ONeil, Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166, 2008.

[16] Karsten Nohl, David Evans, Starbug, and Henryk Pltz, Reverse-Engineering a Cryptographic RFID Tag, in Proceedings of the 17th usenix security symposium, 2008, pp. 185193.

[17] Ronny Wichers Schreur, Peter van Rossum, Flavio Garcia, Wouter Teepe, JaapHenk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, Vinesh Kali: Security Flaw in Mifare Classic, Press release, Digital Security group, Radboud University Nijmegen, March 12, 2008, http://www.sos.cs.ru.nl/applications/rd/pressrelease.en.html.

[18] de Koning Gans, G., Hoepman, J.-H., Garcia, F.D.: A practical attack on the MIFARE Classic. In: Proceedings of the 8th Smart Card Research and Advanced Application Workshop (CARDIS 2008). LNCS, vol. 5189, pp. 267282. Springer, Heidelberg (2008)

[19] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling MIFARE Classic. In Sushil Jajodia and Javier Lopez, editors, European Symposium on Research in Computer Security (ESORICS 08), volume 5283 of Lecture Notes in Computer Science, pages 97114. Springer, 2008.

[20] Garcia, F. D., van Rossum, P., Verdult, R., and Wichers Schreur, R. (2009). Wirelessly Pickpocketing a Mifare Classic Card. In Accepted at Oakland IEEE Symposium on Security and Privacy

[21] Nicolas T. Courtois, The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime, presented at the The 5th Workshop on RFID Security, Leuven, Belgium, 2009.