Security of Contactless Cards

Ashritha Rasa, Rajiv Gautham Champati

***Abstract*— The focus of our paper is a review of the weaknesses of the MIFARE Class cards and the security features of newer MIFARE PLUS cards. We explain the weaknesses in Crypto-1 cipher which is used in MIFARE Plus. We then discuss about three different types of attacks that are executed on MIFARE plus, based on the discussed weaknesses. We then analyze security and implementation of MIFARE Plus which is MIFARE Classic compatible smartcard, currently used by WMATA in Washington D.C area. MIFARE plus X has a solid Architecture and a great chip design. The cryptographic algorithm used in it is AES-128 which is considered secure.**

I. Introduction

MIFARE is a series of chips widely used in contactless smart cards and proximity cards. The MIFARE Classic chip is used in hundreds of transportation systems as in Boston, Los Angeles, Brisbane, Amsterdam, Shanghai, Rio de Janeiro etc. It is also being used as an access pass in thousands of companies schools, hospitals and government buildings around Britain and the rest of the world and is said to cover more than 70% of the market share for access control world-wide. The specification of such a widely used card was kept secret for more than 10 years. The reverse engineering of these cards in later years discovered several very serious attacks and that the product used an incredibly weak stream cipher Crypto-1 that can be broken in 0.1s. This system which could be so badly compromised was shown to be even more insecure by the researchers by discovering card only attacks on MIFARE classic. Huge properties invested by millions of people, governments and businesses world-wide went into risk due to the attacks on MIFARE classic cards. The MIFARE classic story provides strong evidence that the use of proprietary cryptography should be avoided in public systems.
Through this case study, we aim to analyze the security and vulnerability of the MIFARE classic, various types of attacks performed and the drawbacks of the schemes to better understand how such attacks occurred. We also aim to analyze the improvements made in the next generations of the MIFARE line of chips to resist such kinds of attacks.
A case-study on MIFARE series of chips is like a door-way into the knowledge on how cryptography is implemented in public transportation systems. Through this paper, we will learn about different types of encryption used in these systems, initial weaknesses in the implementation, attacks performed based on this weakness and what new systems took place of the old ones. Additionally we will be investigating the metro cards used in Washington D.C. Based on our learning from the case-study on MIFARE.

A.Rasa and R.Champati are with George Mason University. Manuscript revised December 07, 2014.

II. Structure of MIFARE Classic

The basic unit of MIFARE Classic chip is an EEPROM memory with 16 byte data blocks, these data blocks are grouped to form sectors. MIFARE Classic cards are divided into two categories depending upon their memory as 1K and 4K.

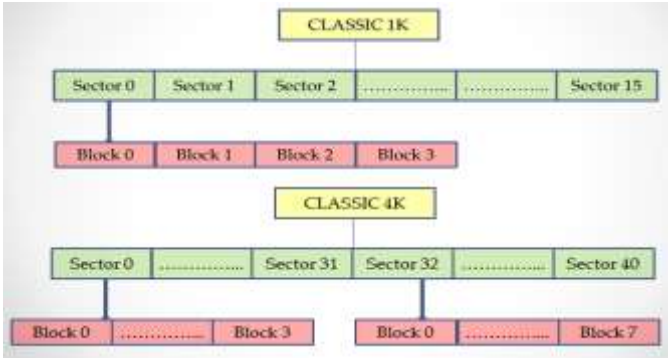

Figure A

Each sector in classic 1K contains four blocks. In the Classic 4K the first 32 sectors consists of four blocks and the remaining 8 sectors has 16 blocks each. The last block of every sector is called a sector trailer. The sector trailer defines keys and access conditions to the blocks in that sector.

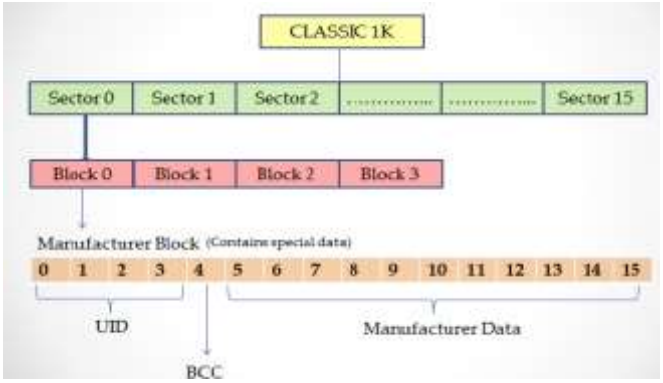

Figure B

Block zero is called the manufacture block and it contains special data like Unique ID (UID), Bit Count Check (BCC) and manufacture data. The contents of this block cannot be changed. Before performing any operations on a data block of a sector, the reader needs to be authenticated for that sector.

This authentication process is governed by the sector trailer. The sector trailer has secret key A and secret key B ranging from bytes 0-5 and 10-15 respectively. Byte 6-9 contains the access conditions of the four blocks.

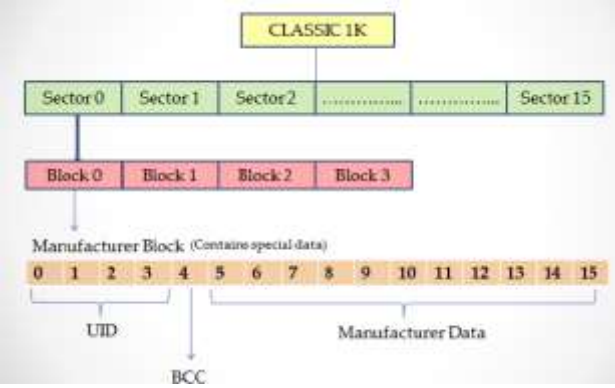

Figure C

User does not have access to key A and he can only access key B when key A is available. The data blocks are of two types Read/Write blocks and Value block. These data blocks are specified by the access bits. In the Classic 1K card the blocks available to store data are second and third blocks of sector 0 and first three blocks of sector 1-15. Modification to the data block can be made only if the corresponding sector is authenticated.

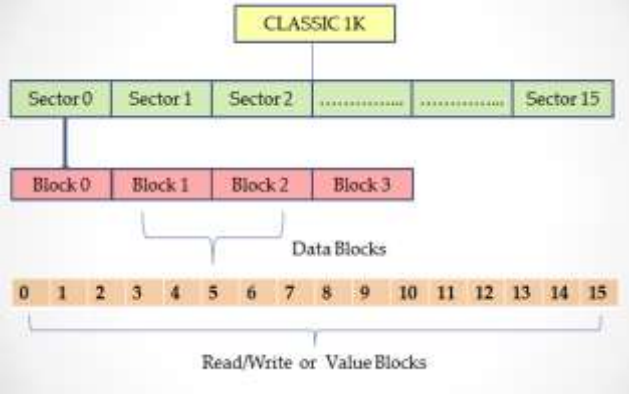

Figure D

A. Memory Access Conditions

Both Classic 1 K and classic 4K chips define 6 operations to access the data blocks. The sector trailer of each data block has 3 bits which define the access conditions.

Operation	Description	Valid for Block Type
Read	Reads a single memory block	Read/Write, Value and Sector trailer
Write	Writes a single memory block	Read/Write, Value and Sector trailer
Increment	Increments the value and stores the result in the internal data register	Value
Decrement	Decrements the value and stores the result in the internal data register	Value
Transfer	Transfers the contents of internal data register to a block	Value
Restore	Reads contents of a block into an internal data register	Value

Figure E

III. STRUCTURE OF MIFARE CLASSIC

MIFARE Classic is a passive type Proximity Integrated Circuit Card (PICC). It depends on the electronic field of the reader for power. The reader is called proximity coupling device (PCD). It generates an electronic field during communication which can be used to power the PICC. MIFARE Classic chip follows the ISO-14443-A Part3 Standard. This standardization ensures the interoperability of MIFARE Classic with various components produced worldwide.

A. Communication between MIFARE Classic and PCD

POWER ON RESET (POR): This is the state of the card when it is not in the electric field of the reader.
REQUEST COMMAND, TYPE A (REQA): The reader detects cards by sending repeated request standard comments in its operating field.
ANSWER TO REQUEST, TYPE A (ATQA): When the card is in the range of the reader it responds to this this command.

B. Anti-Collision Phase

In this phase the UID of the card is obtained by the reader with the ANTICOLLISION COMMAND, AC. This happens if there is only one tag in the vicinity of the reader. A collision occurs of there are many tags in the vicinity. Collision occurs when two cards simultaneously transmits bit patterns. Making note of the bit collision position the reader reads only the bits that are valid. Now this read data is utilized as search criteria. Another AC which is updated with the new search criteria is sent out by the reader. The UID of the card which matches to the new search criterion will now respond to the reader.
SELECT CARD COMMAND (SEL):
This command is sent by the reader to the chosen card for authentication and memory access to which the card replies with a SELECT ACKNOWLEDGEMNT (SAK).

IV. Three-Pass Authentication

The reader uses key A or key B to access a particular sector. The card reads the secret key, access conditions from the sector trailer and sends nonce as a challenge. The reader calculates response to card's challenge. It then sends the response to the card along with its own nonce challenge. The card verifies the reader's response and sends back the calculated response to reader's challenge. The reader finally verifies the response from card and three-pass authentication is achieved.

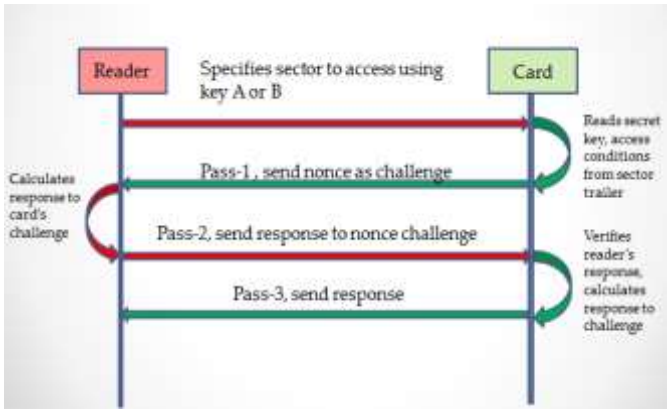

Figure F

HALT COMMAND, TYPE A (HLTA): Using this command the reader can send the tag into a halt state. The card can again be awakened by WUPA command.

V. MIFARE Classic Algorithm

The algorithm implemented on MIFARE Classic chip is Crypto-1 . Crypto-1 is a proprietary encryption algorithm specially designed for MIFARE Classic chip. As the name indicates, it is a secret algorithm whose security relies on the secrecy of the Crypto-1 algorithm.

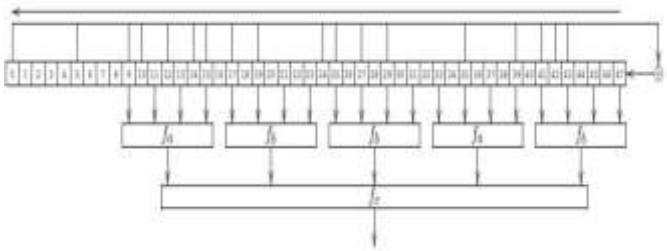

Figure G

The architecture of the Crypto-1 algorithm is as shown in the figure. It is essentially a stream cipher with pseudo random number generator which is used to produce key-stream bits. As the figure indicates, the pseudo random number generator is made up of a 48-bit LFSR with a two layer non-linear filter generator. The non-linear filter generator generates one key-stream bit every clock cycle using random 20 bits (secret key) from the LFSR. The process of generating the key-stream bit continues by shifting one bit of LFSR to the left by discarding the left most bit and adding a new bit to the right. The following equation represents the bits selected from the pseudo random number generator which produces a key-stream bit.

A. Pseudo Random Number Generator

As discussed earlier, MIFARE Classic follows three pass authentications. The challenge is a 32-bit nonce, which is generated with a PRNG of 16-bit LFSR. This PRNG is different from the 48-bit PRNG used for the Crypto-1 cipher. This characteristic is a weakness of the cipher as a 32-bit nonce is generated with a 16-bit LFSR (other weaknesses of the cipher are further discussed). For the 16-bit LFSR to generate a 32-bit challenge nonce, a successor function SUC is used.

$$L(x_0 x_1 \ldots x_{47}) := x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$

The role of the successor is of a pre-determined function with is the output of the response to a challenge. The input of this predetermined function is the challenge again.

VI. Weaknesses of Crypto-1

Crypto-1 weaknesses can be divided into 4 categories.

A. Weakness in Pseudo Random Number Generator

A number generated from PRNG is said to be truly random if the number of bits given as inputs to PRNG is much greater than the number of bits taken out. In the case of Crypto-1, we can see that the number of bits present in the PRNG is 48 and the number of bits used by the function generator to produce the key-stream is 21, which is almost 50 percent of the input bits. By this we can say that the key-stream bits generated are not truly random. This weakness helps the attacker to predict the key using different tools. (Proxmark-3).

B. Weakness in Cryptographic Cipher

There are two weaknesses under this category. These weaknesses are due to bits used to generate key-stream, LSFR bit not used by filter generator. The first weakness in this category is Bits used to Generate Key-stream. The function generator in Crypto-1 uses 20-bits from the LFSR to generate first key-stream bit. As discussed earlier, after the first key-stream bit is generated, the first bit from the 20-bits used is discarded and a feedback is inserted as a new right most bit. This forms a new set of 19-bits used to generate the next key-stream bit. If the attacker has any 2 key-stream-bits, he can use these 21-bits (20 bits + a feedback bit) to find the random numbers used by discarding the bits that do not produce the key-streams. The second weakness is called LFSR bit not used by Filter Generator. From the figure of Crypto-1 architecture,

we can see that the left most 8-bits are not used by filter generator. This helps the attacker can perform a rollback to the LFSR state bit by bit enough number of times to recall the initial state of the LFSR, which is the secret key of the Crypto-1.

C. Weakness in Communication Protocol

First weakness in this category is Parity Weakness.

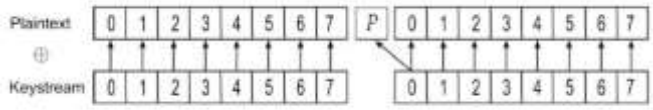

Figure H

In MIFARE Classic, a parity bit is added to ensure that the number of bits with value 1 is odd. The weakness is recognized due to this addition of parity bit as it is added in plaintext instead if cipher text. As the encryption of the second set of plaintext is done after 1st key-stream bit is generated. But the parity bit is added to the plaintext after the key-stream generation. Therefore it is encrypted using the second set of plaintext. This weakness is taken advantage by the attacker.
The second weakness is called ad Information Leak. When the three pass authentication is initialized, the reader sends reader nonce {Nr} and reader response {Ar}. The tag checks for the correctness of the parity bits and responds to it if the parity bits are correct, else the tag does not respond. If all the parity bits are correct and the response {Ar} is wrong, the tag responds with a 4-bit error code which is encrypted. The attacker can combine the error code with the encrypted version and recovers 4 Key-stream bits.

D. Weakness in Implementation

Deploying product with default keys is the only type of weakness in this category. The manufacturers deploy the chips with default keys to make the testing for the companies easy. These default keys are also documented. Some companies ignore the documentation and deploy the product with these default keys still active. As these are well documented the attacker can easily attack card.

VII. ATTACKS

MIFARE classic was reverse engineered by KarstenNohl in 2008. they discovered that both the card and the reader are flawed and the product used an incredibly weak stream cipher Crypto-1. Depending on the weaknesses discussed above. There are three types of practical attack scenarios.

- Passive, Genuine session scenario (Man in the Middle attack)
- Active, Genuine reader scenario
- Active, Genuine tag only scenario

Each scenario above includes different types of attacks. These scenarios will be explained in the further sections using one example each.

A. Brute-Force Attack (Genuine Card Scenario)

The attacker tries to authenticate for a sector by playing a role of a reader. When a challenge comes from the card the attacker answers the challenge with eight random bytes and eight random parity bits. The card responds with a 4-bit error code (encrypted) if the parity bits are correct. The probability of this happening is 1/256. If this attempt is successful, 12 bits of entropy is leaked (out of 48). Sufficient repetitions of the above attempt uniquely determine the key in practice 6 attempts are enough? Since the length of the key is only 48 bits Brute-force can be performed by the attacker. The attacker just needs to check which of the 2^48 combinations of keys produce the correct parity bits and receive response (all 6 times). In practice this can be done in less than 1 second. The time taken to perform a Brute-Force attack strongly depends on the resources the attacker has.

B. Genuine Reader Scenario

In this scenario, the attacker only communicates with the reader. Keys of a sector can be recovered using a single of authentication. To perform this attack we need two assumptions. First, we assume that the card's ID can be obtained by the attacker using ProxMark to eaves drop. Second, the attacker communicates with a genuine reader using ProxMark.
In a single authentication attack a random sequence is sent by the ProxMark as a challenge nonce of the card. At this point the cards legal information is not verified by the reader. Then the sector's is computed by the reader using card's UID and the block which requires to be authenticated. The reader then sends an encrypted challenge nonce and responds to the challenge nonce sent by the card. We can recover the secret key by intercepting two partial authentication sessions and using Garcia's second attack [5] . The attacker can derive the secret key of the sector if the reader does not verify whether a card is legal or not.

C. Passive Genuine Session Scenario (Man in the Middle Attack)

In this attack the key used to encrypt an intercepted authentication between genuine reader and tag can be recovered. After the communication has been successfully intercepted, key recovery can be done offline. We use ProxMark tool in this attack. Interception on the ProxMark is started by running the hi14asnoop command. hi14asnoop command will take the ProxMark into sniffing mode to capture communication between a card and a reader. After a complete authentication has been obtained using ProxMark an offline recovery of the secret key is performed. For this, we use Crapto1 which is a C library implementation of Crypto1 cipher in software.

VIII. SMARTRIP

The Washington Metropolitan Area Transit Authority (WMATA) smart trip card is introduced to metro rail customers in 1999. It was the first smart card-based transit fare payment system in United States. Since that time, over 5 million smart trip cards have been sold. Today's smart trip cards are used to pay for nearly 80 percent of the 350 million annual transit trips in Washington Metropolitan region.

IX. MIFARE PLUS IN SAMRTRIP

Smart Trip card uses MIFARE Plus X version of the MIFARE Plus family. MIFARE Plus is designed by NXP semiconductors. It is the only mainstream IC compactable with MIFARE Classic 1K and 4K which offers an upgrade path for existing infrastructure and services.

	MiFare Classic	MiFare Plus X
Memory	1 kB or 4 kB EEPROM	2 kB or 4 kB EEPROM
UID	4-byte (fixed)	Supports 4-byte and 7-byte The customer must decide which UID length to use when ordering the product
Crypto	Crypto-1	128-bit AES , Crypto-1
Key storage	stored as MIFARE CRYPTO1 keys (2 × 48-bit per sector)	can be stored as MIFARE CRYPTO1 keys (2 × 48-bit per sector) and as AES keys (2 × 128-bit per sector)
Proximity Check	No	Yes

Figure I

The above figure shows the differences between MIFARE Classic and MIFARE Plus x. MIFARE Plus uses 128 bit AES as a cryptographic algorithm in addition to Crypto-1. The memory of MIFARE Plus can be described as 2K or 4K EEPROM. The UID in MIFARE Plus supports 4 bytes and 7 bytes of length. The customer is given a choice of UID length when ordering the product. The keys in MIFARE Plus can be store as MifareCrypto-1 keys and as AES keys. The key feature of MIFARE Plus is the proximity check which ensures the security of the card which is not present in MIFARE Classic.
Some of its special features are discussed below.

A. Anti-Tearing Mechanism

This feature allows the values store in each counter to be protected if a power down occurs during the programming cycle. In this case, the counter value is not updated and the previous value is retained. The anti-tearing algorithm is based on the following principles. The counter retains the active value and a non-volatile register CA is erased, while the other register CB is programmed with the new counter value.

B. Proximity Check

The security level-3 offers a feature to verify that the PICC is in close proximity to the PCD. This functionality can be used to effectively prevent relay attacks. The proximity check is based on a precise time measurement of challenge response pairs in combination with cryptographic methods.

C. Communication Protocol

The ISO/ICE 14443-3 anti-collision mechanism allows for simultaneous handling of multiple PICCs in the field. The anti-collision algorithm selects each PICC individually and ensures that execution of a transaction with a selected PICC is performed correctly without data corruption forms other PICCs in the field. There are three different versions of the PICC. A unique 7-byte serial number, unique 4-byte serial number and a Non-unique 4-byte serial number. The customers must decide which UID length to use in ordering the product.

X. SECURITY FEATURES OF MIFARE PLUS

The MIFARE Plus offers a unique feature to migrate from crypto-1 algorithm to AES algorithm, which is done using different security levels supporting different protocols.

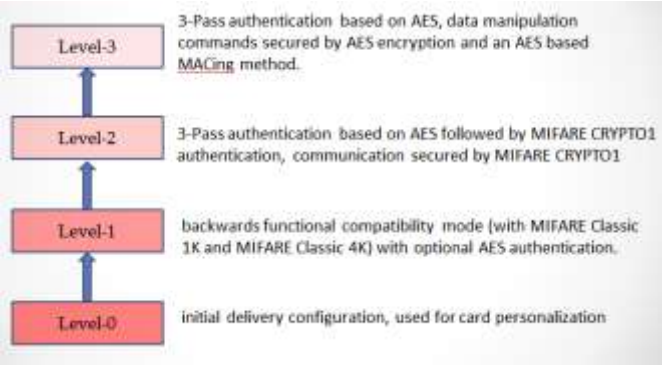

Figure J

There are three security levels. Security level 0, in this level supports initial delivery configuration used for card personalization. Security level 1, in this level has backward functional compatibility mode with MIFARE Classic card. It also includes optional AES authentication. Security level 3, in this level consists of three pass authentication based on AES, data manipulation commands secured by AES encryption and an AES based MACing method. The switching between different security levels is performed by AES authentication switching keys. The level of security can only be switches from lower level to higher level, never in the opposite direction.

XI. CONCLUSION

Any technology is reliable only if it has the best security features. Our project has emphasized the security analysis of the smart cards that we use in our daily life. The team has

elaborated on the first generation of MIFARE class of card, its weaknesses and attacks done on it. The most frequently used smart card in Washington DC area is Smartrip which has be explained in detail. The main focus was on the cryptographic algorithm used in Smartrip. The MIFARE Plus is used in Smartrip. It is the most secure algorithm and is best suited for smart cards in transportation.

XII. REFERENCES

[1] Sean Gallagher. "Researchers hack crypto on RFID smart cards used for j=key less entry" Internet: http://arstechnica.com/business/2011/10/researchers-hack-crypto-on-rfid-smart-cards-used-for-keyless-entry-and-transit-pass/ , Oct 12, 2011 [Oct 10, 2014].

[2] E. Keith Mayes and Carlos Cid (November, 2010). "The MIFARE Classic story." Information Security Technical Report [online].15(1), pp.8-12. Available: http://ac.els-cdn.com.mutex.gmu.edu/S1363412710000348/1-s2.0-S1363412710000348-main.pdf?_tid=b4275686-3da6-11e4-b576-00000aacb35d&acdnat=1410874872_5bd27943ae920ba9d6f78f3ed8784aed[September16,2014]

[3] Ya Liu. DawuGu. Bailan Li. Bo Qu (July,2013). "Legitimate-reader-only attack on MIFARE Classic." Mathematical and computer modeling [online]. 58(1-2), pp. 219-226. Available: http://www.sciencedirect.com.mutex.gmu.edu/science/article/pii/S0895717712002038 [September 16,2014]

[4] D. Flavio Gracia. en Peter van Rossum. RoelVerdult. Ronny WichersSchreur. "Wirelessly Pickpocketing a Mifare Classic Card," presented at the 30th IEEE Symposium on Security and Privacy , California, USA, 2009.

[5]F.D. Garcia. P. Van Rossum. R. Verdult . R.W. Schreur. "Wireless pickpocketing a MIFARE classic card" in IEEE symposium on Security and Privacy, May 2009, pp.3-15

[6] D. Garcia Flavio . Gerhard de KoningGans. Ruben Muijrers. Peter van Rossum. RoelVerdult. Ronny WichersSchreur. Bart Jacobs . "Dismantling MIFARE Classic," Presented at 13th European Symposium on Research in Computer Security (ESORICS 2008), Malaga , Spain 2008

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

[8] E. Keith Meyes. "Transport Ticketing Security and Fraud controls",*Information security Technicalreport.* Volume 14, Issue 2, pp.87-95, May 2009.

[9] Gerhard de KoningGans, Jaap-HenkHoepman, and D. Flavio Garcia. "A Practicle Attack on MIFARE Classic" Internet: http://www.proxmark.org/documents/mifare_weakness.pdf, [Sep 15, 2014]

[10] S. Burton KaliskiJr. K. Cetin Koc. ChristofPaar, "Cryptographic hardware and embedded systems- CHES 2002", Volume 4, [Online], pp: 13-27.

[11] M. Merhi . J.C. Hernandez-Castro. P. Peris-lopez."Studying the pseudo random number generator of low-cost RFID tag" in 2011 IEEE International Conference on RFID- Technologies and Applications (RFID-TA), 2011, PP. 381-385.

[12] "MIFARE", Internet: http://www.mifare.net/en/products/mifare-smartcard-ic-s/ , [Oct 26,2014].

[13] Vijay Ratnam, Aaron Hunter, Cesar Corzo. "Security of Metro/Subway Cards", Project proposal for ECE 646, George Mason University, 2012.

[14] Kurt Raschke. "And The Winner Is…MIFARE Plus", Internet: https://kurtraschke.com/tag/smartrip , [Oct 25,2014].