Revisiting RFID *Mifare Classic* security in the context of investigations that account millionaire losses a case study based on the ticketing system implemented in Brazil

Revisitando a segurança do RFID *Mifare Classic* no contexto de investigações que contabilizam perdas milionárias um estudo de caso baseado no sistema de bilhética implementado no Brasil

DOI:10.34117/bjdv8n3-287

Recebimento dos originais: 14/02/2022
Aceitação para publicação: 22/03/2022

Leandro de Souza Oliveira
Especialista em Computação Forense e Perícia Digital
Instituição: Instituto de Criminalística da PCDF
Endereço: Complexo da PCDF s/n SPO 23 A, Brasília - DF, CEP: 70610-907
E-mail: leosol@gmail.com

João Paulo C. de Sousa
Mestre em Computação pela UNB
Instituição: Instituto de Criminalística da PCDF
Endereço: Complexo da PCDF s/n SPO 23 A, Brasília - DF, CEP: 70610-907
E-mail: jpclaudino@gmail.com

Otávio Augusto P. da Silva Maciel
Perito oficial com atribuições relacionadas com perícias de Informática
Instituição: Instituto de Criminalística da PCDF
Endereço: Complexo da PCDF s/n SPO 23 A, Brasília - DF, CEP: 70610-907
E-mail: otavio.parreiras@gmail.com

ABSTRACT

Electronic systems in the infrastructure of public and private transport services are increasing. This growth comes from the various benefits for its implementation. In the capital of Brazil, the Federal District, as well as other federative entities, an electronic ticketing system based on smart cards was adopted. The card adopted in the capital belongs to the Mifare Classic series whose internal characteristics are widely known. Although several vulnerabilities are known, this card is still widely used in Brazil and worldwide. The focus of this study is on the security of this card as a credit storage medium within the ticketing system adopted locally. The most relevant and known vulnerabilities were enumerated. These vulnerabilities were confronted with the real possibility of building a cloned card. As an expected result, it was possible to build a cloned and accepted card within the system. Finally, significant storage areas were revealed: serial number location, registration number, credit total, credit batches and a 64 bits signature. This reinforces the need to withdraw Mifare Classic cards urgently.

Keywords: card cloning, smart cards, mifare classic, automatic ticketing system, ticketing.

RESUMO
Os sistemas electrónicos nas infra-estruturas de serviços de transporte público e privado estão a aumentar. Este crescimento provém dos vários benefícios para a sua implementação. Na capital do Brasil, o Distrito Federal, assim como outras entidades federativas, foi adoptado um sistema de bilhética electrónica baseado em cartões inteligentes. O cartão adoptado na capital pertence à série Mifare Classic, cujas características internas são amplamente conhecidas. Embora sejam conhecidas várias vulnerabilidades, este cartão é ainda amplamente utilizado no Brasil e em todo o mundo. O foco deste estudo é a segurança deste cartão como meio de armazenamento de crédito dentro do sistema de bilhética adoptado localmente. As vulnerabilidades mais relevantes e conhecidas foram enumeradas. Estas vulnerabilidades foram confrontadas com a possibilidade real de construção de um cartão clonado. Como resultado esperado, foi possível construir um cartão clonado e aceite dentro do sistema. Finalmente, foram reveladas áreas de armazenamento significativas: localização do número de série, número de registo, total de crédito, lotes de crédito e uma assinatura de 64 bits. Isto reforça a necessidade de retirar urgentemente os cartões Mifare Classic.

Palavras-chave: clonagem de cartões, cartões inteligentes, mifare classic, sistema automático de emissão de bilhetes, emissão de bilhetes.

1 INTRODUCTION

The use of electronic systems is growing in the infrastructure of public and private transport services. This growth comes from several points favorable to its implementation, such as: the possibility to collect data; mapping and individualizing access to transport services through the use of smart cards; optimized application of public tariff policies; a single payment method provides greater security; possibility of integration with multiple kinds of transport; cost reduction; and greater convenience for end users. However, electronic systems initially have a high cost of implementation and are slow to be accepted by the public since new elements are introduced in the user's daily life. In addition, there is a high risk resulting from the investment in a certain technology and the success of the project depends on the acceptance of the end user [PELLETIER; MORENCY; TRÉPANIER, 2011].

In the capital of Brazil, Distrito Federal - DF, as well as in other federative entities, an electronic ticketing system was adopted that locally received the name of Automatic Ticketing System - ATS. The end user of the ATS uses a smart card from the Mifare Classic series whose internal characteristics are widely known. Although several vulnerabilities are known [MEIJER; VERDULT, 2015], this card remains widely used in public transport systems in Brazil and worldwide. Among the uses of this card in electronic ticketing systems are: Dublin Bus (Ireland); Tarjeta Bip! (Chile); EasyCard

(Taiwan); BusCARD (Croatia); TransLink Go Card (Australia); ATS (Brasília, Brazil); TRI (Porto Alegre, Brazil) [Open Content].

Since its implementation, the ATS has been the target of investigations and has appeared several times in the local news as subject of investigations that account millionaire losses to the local government [PINHEIRO, 2019].

This work begins with an analysis of the general characteristics of smart cards used in integrated transport systems. Next, the software and hardware components perceived by the end user of the Automatic Ticketing System - ATS, adopted in the capital of Brazil, the Federal District - DF, are presented. Considering that the focus of this study is on the security of the card used in the whole solution, at a later stage its technical details are presented and the most relevant and known vulnerabilities are enumerated. These vulnerabilities will be confronted with the real possibility of building a cloned card within the ATS, without its official issuance occurring, including assessing the possibility of obtaining free credit and free transit between the transport systems, being simple cloning an expected results by the known vulnerabilities, analysis of cards content will be taken.

As a result, it is intended to produce knowledge to support the work of security analysts, to propose measures to remedy the vulnerabilities found, as well as to contribute to the safety of the ATS and the end users of the Brazilian public transport system.

2 MATERIALS AND METHODS

A notebook with an Intel Core i5 processor, with an onboard Intel HD Graphics 4000 graphics card, containing an installation of the Debian version 9 GNU / Linux distribution and a component for reading and writing contactless cards model ACR122U, compatible with ISO / IEC 14443. The reader acquired has an average value of $20.00 and is capable of functioning on any personal computer running Linux operating system. Two cards were also required: an officially issued card and a blank card, capable of being read and written by the ACR122U component. The memory dumps were analyzed using the Visual Binary Diff [PROXOFT, 2017] and Binary Viewer [MADSEN, 2017] tools. The work consisted of: analysis of the internal characteristics of the card; technical vulnerability survey; and carrying out a technical experiment.

3 THEORETICAL REFERENCE

This section presents concepts related to electronic ticketing systems and the general characteristics of smart cards that are commonly found in this context.

3.1 INTEGRATED TICKETING SYSTEMS

These are systems that allow the user to use different kinds of transport through a single payment mechanism (ticket). The objective is to provide greater efficiency and simplify the transport service [BLYTHE, 2004]. Fig. 1 shows equipment typically used for validating access to transport services.

Figure 1. Equipment used for access validation. Image extracted from: BLYTHE, 2004.

Integrated Ticketing Systems are highly complex corporate information systems and usually contain several features, such as user identification and authorization network, transaction control and financial history, fleet control by the use of GPS devices; tariff segmentation by location and user profile (student, worker, etc.); existence of a central service that concentrates the data and allows the administrator to organize fleets, schedules, routes. There is still a need to establish authorized points of sale and credit recharge [PELLETIER; MORENCY; TRÉPANIER, 2011].

3.2 SMART CARDS

They are electronic devices normally found inserted in plastic material, with size similar of a credit card. They are normally used to control access to a resource and follow the standards ISO / IEC 14.443, ISO / IEC 7810 and ISO / IEC 7816. Smart cards can only be equipped with a memory or they can contain a microprocessor capable of running

short programs. To establish communication, they may require contact or be contactless. When contact is needed, the card needs to be connected to the reader, that is, it is necessary to establish physical connection points. The contactless type communicates with the reader by means of electromagnetic waves that provide the necessary energy for processing and reading data, providing communication up to a certain distance from the reader. The amount of memory on the card varies depending on the application for which it is intended. It is observed between 2 and 4 kilobytes for financial applications, reaching up to 64 kilobytes [USING ITS IN PUBLIC TRANSPORT AND IN EMERGENCY SERVICES, 1999]. For applications in transport systems, a small amount of memory is required since most of it is not stored directly on the card [PELLETIER; MORENCY; TRÉPANIER, 2011].

4 THE CAPITAL OF BRAZIL

Within the Federal District, the user can obtain the following types of cards [GDF, 2018]:

- Citizen Card that is offered to all users.
- Vale-Transporte Card, which is the anticipation of the expenses for transportation between residence and work and vice versa for workers.
- Student Free Pass Card, which consists of a free benefit of the fees to students.
- Card for People with Special Needs, which guarantees free public transport for people with disabilities.

Credit purchases can be made at points of sale that use terminal-type devices (Point of Sale - POS). Subway buses, regular buses and other kinds of transport services that make part of the system receive a device similar to that shown in fig. 2. This device is called locally as validator.

Figure 2. Access validator and card.

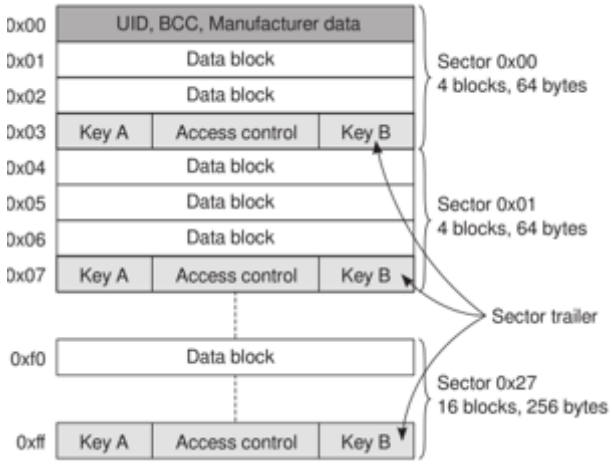
Source: Local news.

The corporate system adopted is named TDMax and is a product by the company Transdata Smart. The characteristics of the adopted smart-card are: contactless, made in the format and dimensions, standardized by ISO 14443 ID 01, with an ISO / IEC DIS 9798-2 information exchange standard, with Mifare A and B compatibility, with processor and memory.

5 MIFARE CLASSIC

The Mifare Classic series cards are contactless devices with a considerable amount of memory (between 1 and 4 kilobytes) and cryptographic capabilities that make it interesting for several applications such as access control and ticketing. Fig. 3 shows the internal structure of the Mifare Classic 1k card. The 2k and 4k variations have a similar structure, with a greater number of sectors.

Figure 3. Internal structure of the Mifare Classic 1k card.



Source: MEIJER; VERDULT, 2015.

It is observed that the total storage is divided into 16 (sixteen) sectors. Each sector has 4 (four) blocks, each with 16 (sixteen) bytes. The last 16 (sixteen) bytes of each block correspond to two keys and an access control field. The first block of sector zero is reserved for the manufacturer and the card identifier is recorded on it. The other sectors are for use by applications that have 752 bytes available for net storage. Each sector is protected by access keys known as “Key A” and “Key B”. Each key can be programmed to allow reading, writing and incrementing operations. The manufacturer of Mifare Classic never exposed the internal characteristics of its encryption algorithm, known by the name CRYPTO1 [MEIJER; VERDULT, 2015], however, its functioning was fully understood in 2008 [USENIX Security Symposium, 2008]. Communication between the reader and the RFID tag begins with the sending of the UID to the reader, which then requests authentication in a given sector. The authentication request is answered by the tag with a challenge. From this point on, all communications between the reader and the tag are encrypted by the use of a flow key (keystream). The reader needs to correctly answer the challenge generated by the tag and generate a new challenge. The tag responds to the challenge, completing the authentication step of CRIPTO1 [MEIJER; VERDULT, 2015].

5.1 VULNERABILITIES

Below are the main vulnerabilities of the cards in the Mifare Classic series.

- Reduced cryptographic key size of just 48 bits. This size is unable to prevent a brute force attack. For example, considering that an attacker spends 6 milliseconds to attempt authentication, it would take 44,000 years to cover the 48 bits. If a mechanism is installed to speed up the authentication process, this time can be reduced to one week [MEIJER; VERDULT, 2015];
- Predictability of generating random numbers that are used in the encryption process. The nonces used by Mifare Classic are 32 bits, however, some cards implement the random number generator based on an internal generator of only 16 bits. That is, every 65,535 cycles, the nonces are repeated [MEIJER; VERDULT, 2015].
- If the card has a nonce generator based on an internal 16-bit generator and an attacker has at least one Key A or Key B key, there is a flaw in the nested authentication process, which is the process of requesting authentication for a

sector, while authentication has already been successfully completed to another sector. The application of Nested Authentication Attack can reveal 32 bits of the keystream [30TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2009];

- Mifare Classic, contrary to ISO / IEC 14443-A, does not separate the link and communication layers. That is, it sends parity bits that are applied across the plaintext [MEIJER; VERDULT, 2015].
- During the authentication process, the tag always checks for a parity bit, the one applied over the plaintext indicated in the previous item. If at least one parity bit, among the eight sent, is incorrect, the tag does not respond. If the eight parity bits are correct, but the challenge response is incorrect, the card responds with the 4-bit error code: 0x5, indicating authentication failure. The error code is sent encrypted, although the reader has yet to complete authentication, this error treatment reveals 4 bits of the keystream. This vulnerability can be mitigated by producing cards that simply do not send error messages [MEIJER; VERDULT, 2015].
- The internal state of the card can be calculated, given that the UID is known, a challenge sent by the card and a challenge sent by the reader [GARCIA F. et al., 2009].
- The keystream, which is a non-linear function applied to the result of the linear function that generates the pseudo-random numbers, uses only the odd bits among the 48 bits. This basically halves the computational power needed to obtain data about the key [MEIJER; VERDULT, 2015].

With the publication of these vulnerabilities, the Mifare Classic card series underwent improvements and became known as Hardened Mifare Classic. The improvements were not sufficient to maintain the security of the card. In [MEIJER; VERDULT, 2015], a method was built based on characteristics of CRIPTO1 that cannot be changed without breaking backward compatibility. This method exploits the parity bit, applied to the plaintext; the fact that only the odd bits of the pseudo-random number generator are used in the generation of the keystream; and the possibility to restore the internal state of the card. This method can be applied offline, that is, it can be done in a controlled environment. Those authors notified the manufacturer of the Mifare Classic who recognized the vulnerabilities described, as well as the card's fragility. Those authors

also were invited to review the manufacturer's notification letter to customers that recommended discontinuity of the card.

6 EXPERIMENT

Several tools are available on the internet to exploit the described vulnerabilities, including the method presented in [MEIJER; VERDULT, 2015], being useful to mention the following: MiLazyCracker [NFC-Tools, 2017]; MFOC: Mifare Offline Nested Attack [NFC-Tools, 2015] and MFOC: MFOC with Hardnested Attack [KIVACHUK, 2018]. This experiment used na MFOC tool with Hardnested Attack. An environment composed of a notebook with an Intel Core i5 processor, with an Intel HD Graphics 4000 graphics card, was built, containing an installation of the Debian version 9 GNU / Linux distribution and an ACR122U contactless card reading and writing component, compatible with ISO / IEC 14443 standard. The reader purchased has an average value of $20.00 and is capable of functioning on any personal computer with Linux.
Two cards were also required: an officially issued card and a blank card, capable of being read and written by the ACR122U component.

Figure 4. Material used in the experiment.

Early on, the MFOC with Hardnested Attack identified the card as Hardened Mifare Classic. Then, he attempted authentication using an internal key bank, achieving success in 5 sectors. Then he applied the method described in [MEIJER; VERDULT, 2015]. The application starts the nonce collection thread and performs the analysis of the Sum and Bit Flip properties. As a result, it managed to greatly reduce the scope of the brute force attack. After approximately 4 (four) hours, all key pairs were identified, showing the vulnerabilities found and described in [MEIJER; VERDULT, 2015] and the fragility of the card. Fig. 5 shows that, as reported in [MEIJER; VERDULT, 2015], which states that it is common for unused sectors to remain with the default key, there were 5

(five) key pairs with the default value 0xffffffffffff, greatly facilitating the discovery of other encryption keys and, of course, enabling the application of the Hardnested Attack in all other sectors. For security, the keys have been partially omitted with the yellow rectangles.

Figure 5. After approximately 4 (four) hours of processing, all key pairs were revealed.

After exposing the keys, it was possible to make a full copy of the data stored on the card. In order to understand the allocated memory areas, several transactions were carried out using the valid and officially issued card. It should be noted that all credit loading, credit unloading or usage reports were procedures carried out by official entities properly inserted in the transport system. The operations carried out were (values are in local currency):

1. Loading of R$ 10.00;
2. Loading of R$ 15.00;
3. Unloading of R$ 5.00 (trip);
4. Loading of R$ 5.00;
5. Loading of R$ 5.00;
6. Loading of R$ 5.00;
7. Unloading R$ 5.00 (trip).

For each event, usage reports were generated at specific official entities. Fig. 6 shows one of these reports and the fields that were printed. After each event listed above, the procedure for dumping the card's internal memory was also performed. The cashier who was responsible for generating usage reports also told the user that to calculate the final balance one should need to sum every balance field that was printed. Another interesting information was the credit batch id which the cashier said to be related to the origin of credit.

Figure 6. Usage reports with emphasis on possible data areas that could be found in the card.

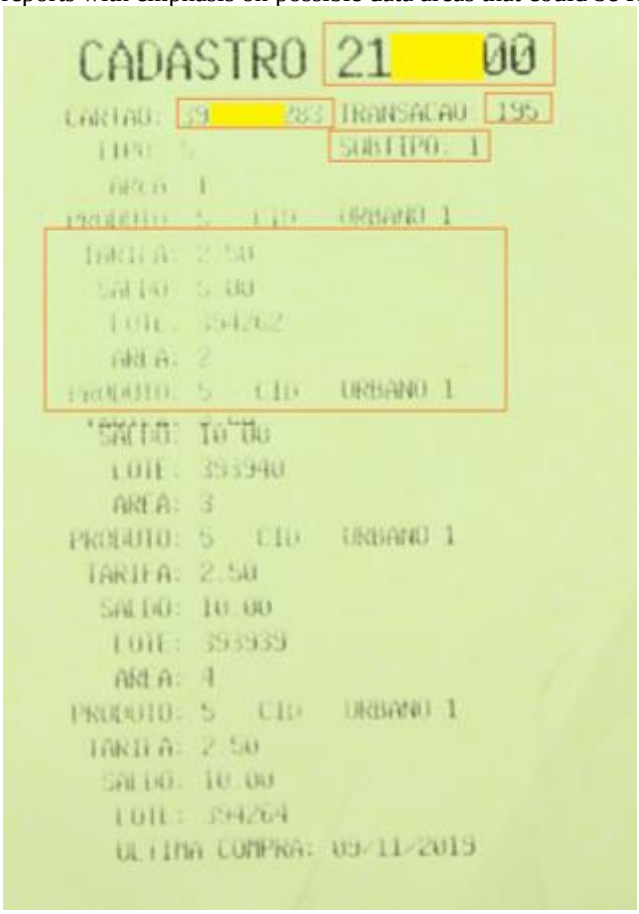


Table 1. Fields transcribed from the extract shown in fig. 6.

Field	**Value**
Cadastro	21###00
Card Serial Number	39#####283
Card type	5
Transaction counter	195
Area	1
Product	5 (Urban 1)
Tariff	R$ 2.50
Balance	R$ 5.00
Credit batch id	394262
Area	2
Product	5 (Urban 1)
Tariff	R$ 2.50
Balance	R$ 10.00
Credit batch id	393940
Area	3
Product	5 (Urban 1)
Tariff	R$ 2.50
Balance	R$ 10,00
Credit batch id	393939
Area	4
Product	5 (Urban 1)
Tariff	R$ 2.50
Balance	R$ 10,00
Credit batch id	394264

Last usage	2019-11-09
Total Balance (calculated by the user)	R$ 25,00

Each memory dump was compared to each other using the VisualBinaryDiff tool. With this tool, it was possible to see the differences between the binary files. From the printed extracts and observing the gradual differences between the binary files, it was possible to identify the storage position of the following fields:

1. Position 0x00: card serial number that corresponded with hexadecimal value shown on the statement for 39 ##### 283 (4 bytes);
2. Position 0x40: registration code that corresponded with the hexadecimal value shown on the statement for 21 ### 00 (3 bytes); in position 0x4D, a value equivalent to the type of register was perceived;
3. Position 0x54: transaction number. Around the transaction field there was an integrity check occupying 4 bytes before and 4 bytes after. Thus, there was an allocation of 12 bytes for the transaction number;
4. Position 0xD0: date of the last transaction, occupying 4 bytes and in unix epoch format.
5. Position: 0xE0: card signature, with 8 bytes.
6. At position 0x140: there were four integers each with 4 little endian bytes. Each integer stored values compatible with 1,000 times the number of existing credits for each lot. For each R $ 5.00 recharge / discharge (which was the value of 1 trip on the date of the experiment), this number was added or deducted from 1,000, indicating that it is the mechanism used for handling decimal values;
7. In position 0x160: start of the enumeration of the credit originating lots.

Fig. 7 shows the memory discharge after the last transaction was carried out and the memory areas that were identified. It also shows an integrity verification feature widely used in card design: copying data from one block to another. Note that the data that begins at address 0x140 is fully repeated from address 0x180.

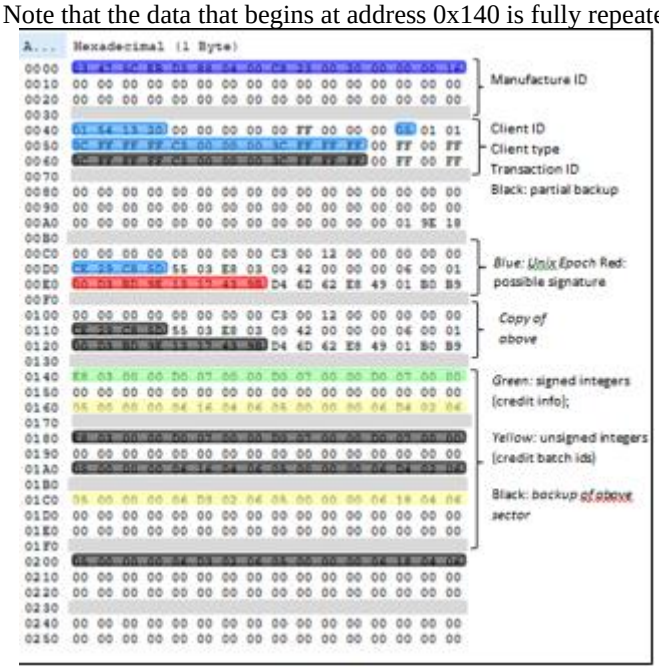


Figure 7. Memory dump with emphasis on data areas.

The memory sectors of the card were used as follows:

- Sector 1: card manufacturer id;
- Sector 2: user data such as registration code (client id), client type and transaction identifier;
- Sector 3: during the experiment, it presented most of its data empty (zeros) and it was not possible to identify its usage;
- Sector 4: last usage date in unix epoch and a possible signature (hash) of the card.
- Sector 5: backup of block 4;
- Sector 6: start of the credits and credits batch ids area;
- Sector 7: backup of block 6;
- Sector 8: continuity of the credits and credits batch ids area;
- Sector 9: backup of block 8.
- Sector 10 to 16: no significant data was stored in these memory areas during the experiment.

Using the contactless card reading and writing component model ACR122U, compatible with the ISO / IEC 14443 standard, and a blank card, the command to write the data extracted after the last transaction on the official card was executed. This

procedure resulted in a card identical to the first one. When presented in a terminal to print user information, it was possible to validate and obtain all info as if it were officially built, meaning that it was easily possible to return the card to its initial state, with the total balance amount that was on that date before credit discharge. We found needless to try to spend credits since there are plenty of videos and tutorials on internet.

It was found that, after each credit loading or unloading operation, the eight-byte sequence started at position 0x120 presented a pattern quite different from the previous one. This field was identified as a type of hash or signature performed by some proprietary algorithm.

It seems that the only way to trace the usage of cloned cards might be by identifying repetitions of the field Transaction ID. Since the whole system works offline with required periodic online time for updates, it might be the case that identifying usage of cloned cards will take long periods since updates and movement synchronizations must happen before identifying repetitions of the Transaction ID field.

These results were made available to the company in charge of the ATS in 2019.

We've also requested material such as validators and access to a testing environment to assess and verify the security of the signature algorithm, but none was provided to the authors of this experiment until today.

7 CONCLUSIONS

In the Federal District of Brazil, an electronic system was implemented in the public transport service that received the name of Automatic Ticket System, ATS. Since its implementation, the ATS has been the target of investigations and fraud. In order to produce knowledge to support the work of security analysts, this work identified the main software and hardware components involved in the ATS, from the point of view of the end user. The type of card that is used as a credit wallet is a contactless card belonging to the Hardened Mifare Classic 1k series. The bibliographic review and the practical application of the attacks described in [MEIJER; VERDULT, 2015] confirmed that the data stored in the card cannot be kept safe. In the tests carried out, it was possible to overcome encryption and fully recover the data stored on the card.

The card security breach procedure was performed on a computer running Linux and used a reader compatible with the Mifare Classic card, whose average value was $ 20.00, showing that the attack environment can be easily reproduced with hardware low cost, just as expected.

Legitimate transactions have been carried out within the ATS. After the registration of each transaction, a full data reading procedure was carried out which allowed, with few transactions, to identify significant areas of the card's memory. Among the areas that were identified are: location of credit records, credit batch ids, registration numbers and serial number, date of the last transaction and the last transaction id.

It was possible to fully reproduce the status of a card officially purchased on a blank card (cloning process). We found needless to try to spend credits since there are plenty of videos and tutorials on internet.

It seems that the only way to trace the usage of cloned cards might be by identifying repetitions of the field Transaction ID. Since the whole system works offline with required periodic online time for updates, it might be the case that identifying usage of cloned cards will take long periods since updates and movement synchronizations must happen before identifying repetitions of the Transaction ID field.

Besides that, if someone manages to create a valid signature, it would be possible to have cards with completely illegal cash, without being detectable.

These results were made available to the company in charge of the ATS in 2019. We've also requested material such as validators and access to a testing environment to assess and verify the security of the signature algorithm, but none was provided to the authors of this experiment until today.

The exploited vulnerabilities are located in the encryption algorithm and not only in cards or readers. In this way, it is not enough to just change this equipment, but the whole set must be replaced by safer components.

As an object of future study, analysis of the signature or hash field is recommended. This field is only 64 bits, which is half the space occupied by MD5. If an attacker manages to generate a valid signature, it will be possible to write any amount for the fields of registration, serial number, number of credits and credits.

REFERENCES

PELLETIER, M.; MORENCY, C.; TRÉPANIER, M. Smart card data use in public transit: A literature review. Transportation Research Part C Emerging Technologies, 2011.

MEIJER C.; VERDULT R. Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards. In: CCS '15: pp 18-30, 2015.

PINHEIRO, MIRELLE. Polícia procura suspeito de fraudar bilhetagem do DFTrans. In: Jornal Metrópoles. [S. l.], 6 nov. 2019. Available at: https://www.metropoles.com/distrito-federal/policia-procura-suspeito-de-fraudar-bilhetagem-do-dftrans . Visited: sept. 23 of 2020.

CONTEÚDO aberto. MIFARE. In: Wikipédia: a enciclopédia livre. Available at: < https://en.wikipedia.org/wiki/MIFARE >, Visited: sept. 23 of 2020.

PINHEIRO M., "Polícia procura suspeito de fraudar bilhetagem do DFTrans", Metrópoles. Available at: < https://www.metropoles.com/distrito-federal/policia-procura-suspeito-de-fraudar-bilhetagem-do-dftrans >, Visited: sept. 23 of 2020.

BLYTHE, Philip. Improving public transport ticketing through smart cards. Municipal Engineer, [s. l.], v. 157, p. 47-54, 2004.

PROXOFT (Estados Unidos). Binary Viewer. In: Binary Viewer. 6.16.01.01. [S. l.], 2 jan. 2017. Available at: https://www.proxoft.com/ . Visited: sept. 23 of 2020.

MADSEN, Christopher. Vbindiff. In: Vbindiff. 3.0 beta 5. [S. l.], 10 set. 2017. Available at: https://www.cjmweb.net/vbindiff/ . Visited: sept. 23 of 2020.

USING ITS IN PUBLIC TRANSPORT AND IN EMERGENCY SERVICES, 1998/524., 1999, University of Newcastle upon Tyne, UK. Integrated ticketing smart cards in transport [...]. [S. l.: s. n.], 1999.

SECRETARIA de Transportes e Mobilidade. Brasília, Distrito Federal. Available at: http://www.dftrans.df.gov.br/ . Visited: sept. 23 of 2020.

VAMOS juntos construir meios para expandir a mobilidade humana?. [S. l.], 2019. Available at: https://www.itstransdata.com/ . Visited: sept. 23 of 2020.

USENIX SECURITY SYMPOSIUM, 2008, San Jose, CA. Reverse-Engineering a Cryptographic RFID Tag [...]. [S. l.: s. n.], 2008.

GARCIA F. et al., Dismantling MIFARE Classic, Computer Security-ESORICS 2008, pp 97–114, 2008.

30TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2009, Oakland, California, USA. Wirelessly Pickpocketing a Mifare Classic Card [...]. [S. l.: s. n.], 2009.

TEUWEN, Philippe; QUATTLEBAUM, Robert; CONTY, Romuald. NFC-Tools: MiLazyCracker. [S. l.], 2017. Available at: https://github.com/nfc-tools/miLazyCracker . Visited: sept. 23 of 2020.

TEUWEN, Philippe; QUATTLEBAUM, Robert; CONTY, Romuald. NFC-Tools: MFOC. [S. l.], 2015. Available at: https://github.com/nfc-tools/mfoc . Visited: sept. 23 of 2020.

KIVACHUK, V; NFC-Tools: MFOC with Hardnested Attack. [S. l.], 2018. Available at: https://github.com/vk496/mfoc . Visited: sept. 23 of 2020.