# The Authentication Module Using Existing Infrastructure of Smart Cards in the Personified System for Information Filtering

Roman Zharinov, Ulia Trifonova
Saint-Petersburg State University of Aerospace Instrumentation
Saint-Petersburg, Russia
{roman, ulia}@fruct.org

**Abstract**

Since children learn work at the computer an early age, children's protection from inappropriate content becomes more urgent. User authentication is required to the personified system for information filtering. Today, almost every child has a ticket for public transport, which is a RFID-tag. That is why it was decided to use it as an identifier in authorization module. So this article is a detailed description of the system's authorization module which uses Mifare RFID-cards, as well as its advantages and disadvantages.

**Index Terms:** RFID, NFC, Mifare, Authorization.

## I. Introduction

An idea of the personified system for information filtering [1, 2] emerged owing to the change of Russian legislation in September 2012 [3]. So there are types of information, which dissemination are prohibited or restricted depending on the age group of children [4]. The development of the personified system for information filtering began last year. Access to the information processed on a computer is provided, depending on the age category of a particular user. The personified system for information filtering, allows to arrange access to the information, received from the network (Internet, Local Area Network) and local storage (hard disk, CD, flash memory, etc.) Since access to information should depend on the age category of user, it is necessary to develop authorization module.

Most of the distributed multi-user systems to restrict access to the information use the system of accounts. Account implies to each user a unique pair: login and password. Using system of accounts is not acceptable for the personified system for information filtering, as the number and composition of the users changes dynamically.

In order to minimize the final cost of the system would use the existing infrastructure of identifiers. Most children use public transport. The Russian underground may use RFID cards as tickets. This ticket stores personal information about the cardholder, including the full name and date of birth. So it was decided to use RFID card as an identifier in authorization module of the personified system for information filtering.

## II. Existing infrastructure of smart cards

For example at the St. Petersburg public transport is used more than 20 different RFID-cards as a tickets. Ticket stores information depend on its type. Among the variety of cards were chosen cards that store information about its owner, including the name and date of birth. These types of cards are presented in the Table I [5].

Thus 14 of the 20 types of card store information about its owner. To obtain these cards necessary to present document: passport or birth certificate. As the personified system for information filtering is aimed at protecting minors from inappropriate information the special interest are the following smart cards: Pupil travel ticket, Student travel ticket, Card “Kurs”, ISIC and For disadvantaged persons. These types of cards can get the kids up to 14 years.

Reading data is the main problem of using card's from different real systems in the own authorization module. Different brands of smart cards use a variety of sectors to store information about the cardholder. Mifare is the most common brand of contactless smart card today. Its communication is based on the open ISO-14443-A standard and has own proprietary cryptographic protocols for authentication and encryption. In the St. Petersburg underground are using smart cards RFID «Mifare Classic». There are two versions of this type of card: 1K or 4K. They differ in the amount of memory to store user and configuration data - 1K or 4K, respectively.

Mifare Classic card is divided into sectors depending on the type of card number of sectors can be 16 or 40, respectively. Access to each sector is protected by two 48-bit keys A and B, as well as access condition (16 bits) for each block. Fig 1 shows the logical structure of the MIFARE Classic 1K chip. Though the key A is used to read the data, and the key B is used to write it. For secret key A allocated 0 from 0 to 5 bytes of the last block of each sector. For secret key B is allocated from 10 to 15 bytes, but this is optional parameter. And all other capacity is reserved for the access conditions or bits (see Fig. 2).

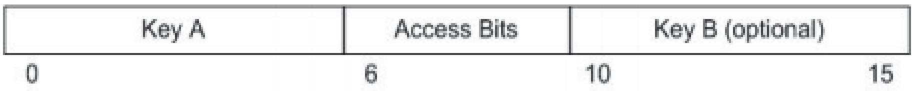


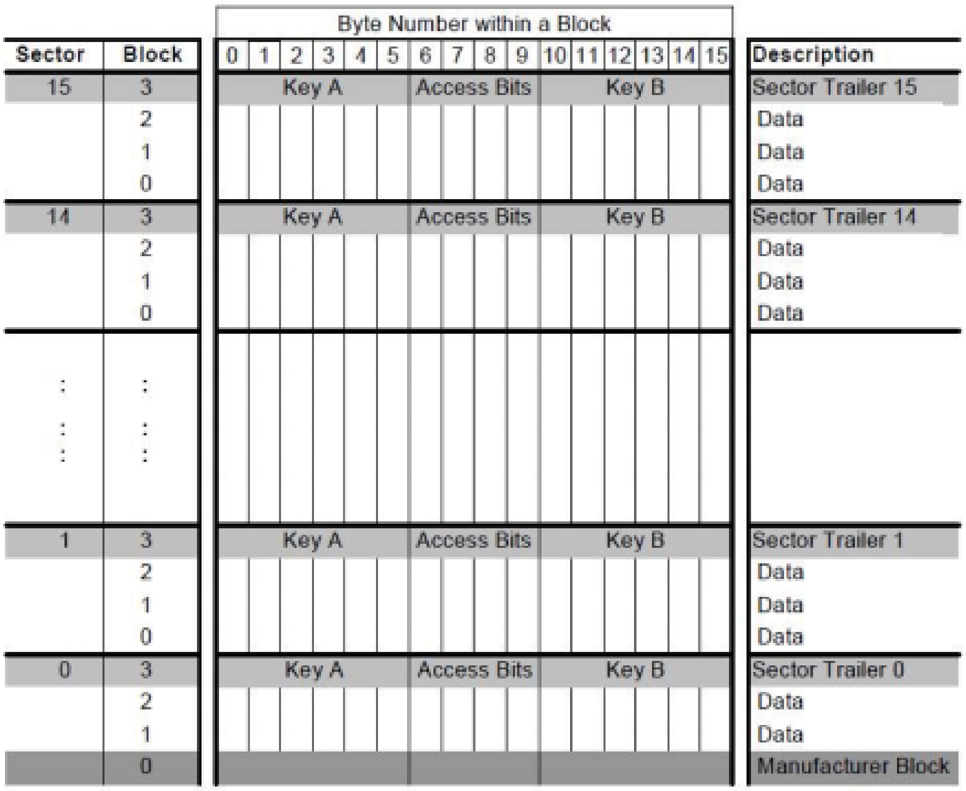
Fig. 1. Sector Trailer

According to the standard MIFARE Application Directory (MAD) [6] the information about card's owner is in the 13-14 sectors of the smart card. The key for reading the data from these sectors is declared in the standard (A: A0A1A2A3A4A5 hex or A: 000000000000 hex).

The remaining sectors of cards are private, so access to them is possible only if you know the keys. However, a closer analysis revealed that public key A is changed in the majority of the smart cards, so it's necessary to restore the key for reading data. Utility Mifare Classic Offline Cracker (MFOC) can make this operation [7], it is in the distribution BackTrack to analyze and assess the security of computer systems and networks [8].

Utility for restore is based on the key's weaknesses in the RFID cards «Mifare Classic» [9]:

- Weak pseudo-random number generator. The most critical weakness are: low entropy of random generator (according to feedback function L(x0x1...x15) := x0 xor x2 xor x3 xor x5 results in an entropy of 2^16), using only odd state bits used to generate keystream and not using leftmost linear feedback shift register (LFSR) bit by filter generator.



|  |  | Byte Number within a Block |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sector | Block | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | Description |
| 15 | 3 | Key A |  |  |  |  |  | Access Bits |  |  |  | Key B |  |  |  |  |  | Sector Trailer 15 |
|  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
| 14 | 3 | Key A |  |  |  |  |  | Access Bits |  |  |  | Key B |  |  |  |  |  | Sector Trailer 14 |
|  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
| : | : |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| : | : |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| : | : |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | 3 | Key A |  |  |  |  |  | Access Bits |  |  |  | Key B |  |  |  |  |  | Sector Trailer 1 |
|  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
| 0 | 3 | Key A |  |  |  |  |  | Access Bits |  |  |  | Key B |  |  |  |  |  | Sector Trailer 0 |
|  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Data |
|  | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Manufacturer Block |

Fig.2. MIFARE Classic 1K Memory

- Weak cryptographic cipher Crypto-1. As was shown in article [10] if we fixed the first three bytes of message {Nr} and varied only the last few bits of {Nr}, the results showed that with a probability of 0.75, the keystream is independent of the last three bits.
- Weaknesses in communication protocol is the inappropriate use of the cipher in the communication. This is a weakness occurs due MIFARE Classic calculates the parity bit over the plaintext, instead of the ciphertext that is sent over the air. This means that both the parity bit and the first bit of the next plaintext byte are encrypted with the same keystream bit (Fig. 2).

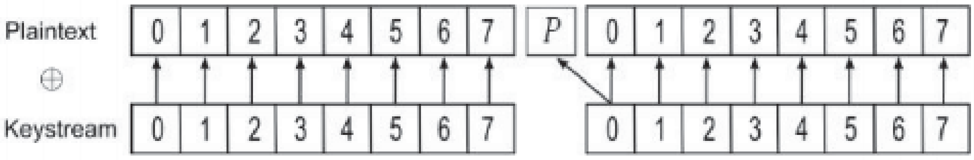


Fig.3. Reuse of One-time Pad

- Weak implementation. This happens because most of chip manufacturers sells their cards with default keys. These default keys are well documented, most uses (in hex format): FFFFFFFFFFFF, A0A1A2A3A4A5, B0B1B2B3B4B5, 4D3A99C351DD, 1A982C7E459A, 000000000000, D3F7D3F7D3F7, AABBCCDDEEFF.

So after a key recovery system will be able to obtain information about the date of birth of the card holder and execute an authorization procedure in accordance with the age category of user.

At impossibility of use standard keys for access to sectors of the storage holder Smart-card, as well as the impossibility signing the contract with Russian undeground and to obtain such access key legal way is possible to construct our own infrastructure of Smart cards type RFID.

Existing vulnerabilities in the authentication module:

Unfortunately, this authentication module is unreliable, because there is potential possibility of cloning or selective filling in unreliable data (modification of 13 and 14 sectors upon which the authentication method).

Cloning can be a physical as well as software. Physical cloning means importing dump (full backup data structures) on blank RFID-card. Software is Mifare standard emulation using NFC technology.

Near field communication (NFC) is a set of standards to establish radio communication into close proximity, usually no more than a five centimeters. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443, FeliCa and ISO/IEC 18092 [11].

## III. Conclusion

It was empirically demonstrated the possibility of using tickets of public transport, which are smart cards, as analog of unique pair: login - password. However, for the cards of Mifare standard, using in the Russian subway, there are a number of vulnerabilities, so it reduces the reliability of the authorization module which was described. During the development of the personified system for information filtering modification of the existing infrastructure of contactless smart cards used in the subway is not possible.

The easiest way to protect from fake smart cards is the use of digital signature. Unique static identifier and information about card holder will be fixed by digital signature. For the implementation of a digital signature is not necessary to change the current architecture, structure of RFID-reader and smart card. All information processing (generation, verification of digital signature) will take place on a computer (it may be operator's computer or server of company). Since the main advantage of the system is using of existing transport infrastructure smart-cards, the decision to implement a digital signature to be taken at the level of subway's administration. It will solve the existing vulnerabilities in the payment system of public transport using contactless tickets.

## References

[1] Trifonova, U. V. и Zharinov, R. F., Concept of the System to Protect Children’s Access to Information, *Proceedings of the 12th Conference of Open Innovations Association FRUCT*, 2012, pp. 142-146.

[2] Zharinov Roman, Trifonova Ulia, Concept of the system to protect children’s access to information in education institutes using RFID-technology, *Scientific and Technical of Information Technologies, Mechanics and Optics*, 2013 (in review process, in Russia).

[3] Federal law of 29.12.2010 № 436-FZ “O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorovyu i razvitiyu” (in Russian).

[4] U.V. Trifonova, “Kids. Protection from ineligible content”, *XIII International Forum Modern information society formation - problems, perspectives, innovation approaches: Proceedings of the International Forum,* Saint-Petersburg, SPb.: SUAI, 2012, pp. 186-190.

[5] Travel ticket of GUP “Peterburgsky metropoliten”, UDP: http://www.metro.spb.ru/ticket.html.

[6] MIFARE Application Directory (MAD), UDP: http://www.nxp.com/documents/application_note/AN10787.pdf.

[7] Utility Mifare Classic Offline Cracker (MFOC), UDP: http://nfc-tools.googlecode.com/files/mfoc-0.10.2.tar.gz.

[8] Distribution BackTrack Linux, UDP: http://www.backtrack-linux.org/.

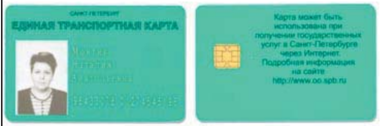
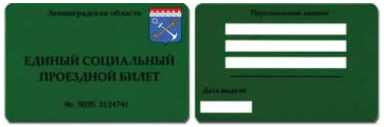
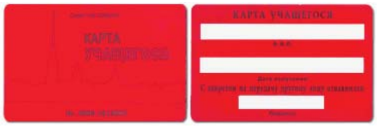
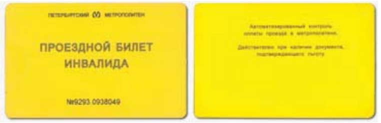
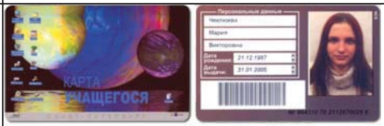
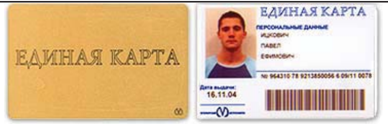
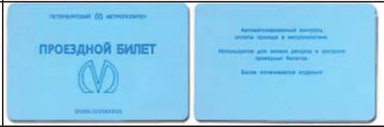
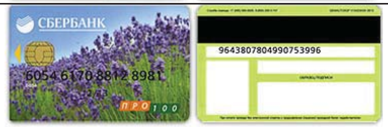
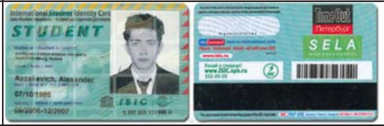
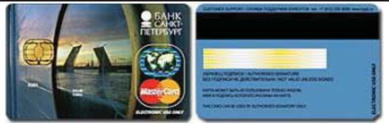
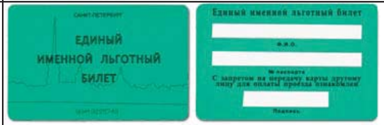
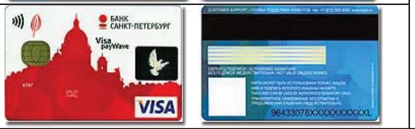
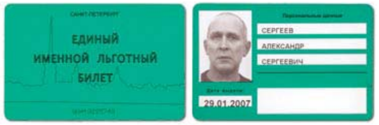
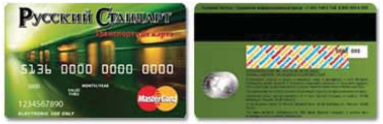
[9] Tan, Wee Hon. Practical Attacks on the MIFARE Classic. Submitted in partial fulfilment of the requirements for the MSc Degree in Computing Science of Imperial College London, September 2009.

[10] Nicolas T. Courtois, The dark side of security by obscurity, *International Conference on Security and Cryptography,* Springer, 2009.

[11] NFC: the present and the future of technology, *Habrahabr*. UDP: http://habrahabr.ru/company/Nokia/blog/129007/.

TABLE I

LIST OF RFID-CARDS OF ST. PETERSBURG UNDERGROUND STORE FULL NAME AND DATE OF BIRTH OF ITS HOLDER

| | Name | Figure | Notes | | Name | Figure | Notes |
|---|---|---|---|---|---|---|---|
| 1 | Unified transport's card |  | This card is the citizens entitled to a reduced fare | 8 | Preferential Smart Card for Leningrad region |  | For pensioners and other benefit recipients are registered in Leningrad region |
| 2 | Pupil travel ticket (without photo) |  | This card is for students grades 1-11 schools, high schools and colleges | 9 | Smart Card for disadvan-taged persons |  | For disadvantaged persons |
| 3 | Student travel ticket (with photo) |  | For undergraduate and graduate students, students of vocational and technical schools, colleges | 10 | Personal Smart Card |  | For everyone over 14 years. |
| 4 | Card “Kurs” |  | For university students, students of vocational and technical schools, colleges studying 1st year | 11 | Smart Card “Pro100” |  | For the employees of the enterprises participating in the pilot projects of Sberbank. |
| 5 | ISIC |  | For students, graduate students (full-time education) and lecturers. | 12 | Smart Card “Card-M” |  | For individuals having bank account in OJSC "Bank "Saint Petersburg". |
| 6 | Preferential Smart Card (without photo) |  | For pensioners and other benefit recipients are registered in St. Petersburg | 13 | Smart Card “Card-M”-“Podorog-nik” |  | |
| 7 | Preferential Smart Card (with photo) |  | | 14 | Smart Card “Russky Standart” |  | For everyone over 14 years. |