Information security of RFID and NFC technologies

M A Masyuk
Reshetnev Siberian State University of Science and Technology, Russia, 660037, Krasnoyarsk, pr. Krasnoyarskiy rabochiy, 31
E-mail: masuk-max@yandex.ru

Abstract. The subject of this work is the information security of radio frequency identification technologies and near field communication (RFID, NFC). The work describes and classifies some currently known vulnerabilities of the corresponding protocols and devices that implement them, and considers cryptanalysis tools and software. The result of the work is an assessment of the risk of using certain specific NFC devices, for example, contactless bank cards. The author’s view on the development prospects of the technology as a whole is also presented.

1. Introduction
Speaking about the technologies of radio frequency identification and near field communication, two indisputable facts can be noted. The first is that today the technology is clearly “in trend”, current economic indicators indicate a continuous annual increase in production volumes of devices supporting this technology [1]. Scopes are expanding, in addition to the usual physical access control system (PACS) and transport cards, technology has stepped into the field of electronic identity cards and contactless electronic payments. The second fact is the presence of a large number of publications in the media space that have big names and conditionally expose critical problems with the safety of technology. The situation is complicated by some confusion associated with the intersection of the names of standards with the names of specific products, the reluctance of equipment manufacturers to strictly adhere to approved standards and even the use of the principle of Security through obscurity [2]. However, similar problems are typical for many rapidly developing areas.

The purpose of this article was to generalize and systematize information on the RFID and NFC devices available on the market and the standards used in them, to describe the known vulnerabilities of some products, and to assess the potential damage from various types of attacks. The work also contains a description of special software and hardware and may be useful to specialists engaged in research in the field of information security of contactless data transmission systems.

2. International standards and trade names related to RFID technology
The abbreviations RFID and NFC combine a large number of different standards and products. Radio frequency identification technologies in their current form and name began to develop in the 1980s. Charles Walton's first patent, mentioning the term RFID, was obtained in 1983 in the United States. At that time, the use of RFID tags was an alternative to bar-code marking of goods with obvious advantages: reading without direct visibility, a large amount of stored data, and resistance to environmental influences. Subsequently, many standards, formats and protocols for the exchange of data related to radio frequency identification were developed and approved. The main role in the
The development of standards was played by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Among the main manufacturers of RFID chips and equipment, NXP Semiconductors (Netherlands), Alien Technology (USA), MIKRON (Russia) can be noted. The correlation of RFID specifications, as well as examples of practical implementations in the form of equipment, its application areas and characteristic features are presented in figure 1.

| Physical level | RFID-technology | Features |
|----------------|-----------------|----------|
| ISO/IEC 18000-2 | Animal identification (ISO 11784, 11785, 14223) | Storage of a small amount of data, low transmission rate, lack of information protection |
|                 | EM Marine tags based on TK4100, EM4100, KS5004X02 et al. | |
|                 | Car immobilizers | |
| ISO/IEC 18000-3 | Proximity smart cards NXP MIFARE et al. (ISO/IEC 14443) | The main standard for SMART cards, the use of encryption and authentication, two-way communication, a wide range of applications, a large amount of data, high speed |
|                 | Vicinity smart cards NXP ICODE et al. (ISO/IEC 15693) | |
|                 | NFC devices (ISO/IEC 18092) | |
| ISO/IEC 18000-7 | Widely used in household devices (remote controls, car alarms) | Ability to use only active tags, high range (up to 1 km), high price |
| 433 MHz Active ultra high Frequency, UHF | | |
| ISO/IEC 18000-6 | Electromagnetic Product Code (EPC) (EPC Tag Data Standard) | Reading distance of more than 10 meters, transfer rate of more than 128 kbps, the ability to simultaneously read a large number of tags |
| 860-960 MHz Ultra high Frequency UHF | Real-time locating systems (RTLS) (ISO/IEC 24730) | |
| ISO/IEC 18000-4 | RFID over WiFi | Ability to use only active tags, high range (up to 1 km), high price of receiver/transmitter |
| 2.45 GHz | | |

Figure 1. RFID technology, standards and equipment.

From figure 1 it can be seen that mainly RFID technologies are divided by the frequency range in which the interaction takes place. The carrier frequency sets physical characteristics and limitations, such as data transfer rate, maximum distance between the receiver and transmitter, noise immunity, which determines the implementation features of higher-level application-level protocols, operational advantages and limitations of equipment operating in the corresponding range (LF, HF, UHF).

Figure 1 also shows that NFC is a specialized subset of the HF frequency family of RFID technologies. An NFC device can be both a reader and a tag at the same time. At the same time, full compatibility with standard smart cards of the ISO / IEC 14443 standard is maintained. This unique ability has made NFC a popular choice for many applications, and most importantly, it has allowed a large volume to bring to the market various mobile devices and even subcutaneous implant, software combining several smart card.
By mass distribution, market leaders include devices of the LF and HF types. However, in terms of information security, class LF devices operating according to the ISO/IEC 18000-2 standard are of little interest. The concept of these devices, as a rule, does not imply cryptographic information security tools. A good example is one of the most common contactless card formats in the world EM-Marin, created by the company of the same name. The working principle of such a card implies only the identification of its owner by transmitting a 40-bit identifier to the reader. At the same time, cloning, emulation and traffic interception are easily implemented using simple equipment, including those produced by the same company. Such RFID devices can be compared with a key to a door lock, which, obviously, is easily compromised by falling into the hands of an attacker.

The situation is different with HF smart cards and NFC devices that work according to the ISO/IEC 14443 and ISO/IEC 18092 standards. Most manufacturers put in their products wide functionality: identification, authentication, encryption of transmitted data, protection against cloning, etc. The next section is devoted to the analysis of known vulnerabilities and methods of hacking such devices.

The question of the degree of protection of RFID devices of other standards is equally important, especially with regard to EPC technology (electronic product code) due to the fast pace of its development and distribution. However, it goes beyond the scope of this article.

3. Types of attacks on smart cards of ISO/IEC 14443 standard and NFC devices

In general, the list of possible attacks on smart cards derives from their functionality: user authentication, storage of key information and cryptographic operations in a trusted environment. Contactless smart cards can be divided into two categories:

- Smart cards using ISO/IEC 14443 as the transport layer and their own proprietary protocols for interoperability at the application level. This category includes cards of the Mifare family, HID iCLASS, etc.
- Smart cards that use ISO/IEC 14443 as the transport layer and ISO/IEC 7816-4 in conjunction with other application protocols for interaction at the application level (application protocol data unit, APDU). This category includes all bank cards, smart cards that are holders of private keys of electronic signatures and other products.

Figure 2 shows examples of smart cards from both groups. We consider both of these cases separately.

![Figure 2. Mifare Classic Smart Card Protocol Stack.](image)

![Figure 3. Bank Card Protocol Stack.](image)
3.1. Contactless smart cards with proprietary data exchange formats

Firstly, the actions of an attacker can be aimed at interfering with the data exchange between the receiver and the transmitter (interaction at the level of ISO/IEC 18000-3, ISO/IEC 14443 in figure 2). The following types of attacks fall into this category: eavesdropping, man in the middle (MITD), denial of service (DoS). Since the standards ISO/IEC 18000-3 and ISO/IEC 14443 do not imply any cryptographic protection, the success of an attacker’s actions in this case depends only on the proximity of the location and the perfection of the hacking equipment used by him. In various studies, it was possible to achieve distances from 2-3 meters to 18 meters with passive listening [3], [4]. If the listening equipment is located at the standard card operating distance of 10 cm, the success of intercepting all the transmitted information is obviously absolute. It is much more difficult to implement a full-fledged MITD attack due to physical limitations associated with the speed of propagation of radio waves and the response time of the equipment. The author is not aware of successful experiments in this direction. But even a successful interception of traffic does not guarantee the occurrence of any damage, since in these types of smart cards information security tools are laid at the application level, so overall security depends on the specific implementation of the device interaction protocol offered by the manufacturer.

A good example in this case is one of the most common smart cards in Russia - Mifare Classic, manufactured by NXP Semiconductors. The card that appeared in the mid-1990s had a closed data exchange format, that violated the Kirkhoff’s principle and led to negative consequences. At first, researchers of Karsten Nohl and David Evans [5] discovered the data exchange protocol using reverse engineering methods. Then, a group of Dutch enthusiasts completely revealed the principle of operation of the Crypto-1 encryption algorithm, which turned out to be unreliable. Currently, despite the fact that Mifare classic continues to be used in many countries, methods for reading the closed sectors of the card and its cloning are described [6], [7] and they are also created and made publicly available allowing to implement this MiFare Classic Universal software tools toolKit (MFCUK), libnfc, Mifare Classic Tool. Hardware devices that can be successfully used for cryptanalysis of any products that support ISO/IEC 14443, ISO/IEC 18000 are also widely available at affordable prices. The author of this work successfully tested a device based on the pn532 v3 chip, which allowed to successfully repeat the known types of attacks on Mifare Classic cards. In these studies, the Adafruit-PN532 software library was used.

NXP Semiconductors, like other manufacturers, took into account the negative experience and expanded the range of smart cards produced, incorporating more reliable encryption algorithms such as AES, 3DES as the basis of their work. However, despite the unwavering authority of these encryption algorithms in terms of cryptographic strength, no one can guarantee a repetition of the situation that occurred with Mifare Classic, due to possible "inherent" design or implementation errors. Messages about the found vulnerabilities of RFID devices appear with enviable regularity and require individual investigation in each individual case.

3.2. Contactless bank smart cards and NFC devices

This category of devices has similar principles of work at the transport level. Therefore, all of the above regarding the possible actions of an attacker to intercept (sniff) data applies to contactless cards that support ISO/IEC 7816-4 and contactless bank cards. In further discussions, we will be based on the fact that an attacker has the ability to completely take control of the data exchanged between a smart card and a reader.

In the case of a bank card (we are talking about cards with chips), the EMV standard developed by Europay, MasterCard and VISA is responsible for the application interaction with international payment systems through payment terminal applications. The differences in the principles of operation of a contact and a contactless card are only in the fact that for a contactless card, APDU data is transmitted using RFID technology, and to be more precise, NFC. NFC is an extension of the ISO/IEC 14443 contactless card standard, allowing you to combine the smart card and reader interface into a single device, as well as emulate multiple smart cards in a single device. The NFC protocol
stack does not provide for cryptography during transmission, just like the ISO/IEC 14443 standard. Consequently, based on our assumptions, with contactless payment for a purchase, an attacker can become aware of all EMV messages between the card and the terminal. Thus, the security of user data is completely dependent on the durability of EMV [8]. Of course, the EMV standard used by international payment systems is considered absolutely protected from any fundamental vulnerabilities. It is practically impossible to clone a bank card with a chip, reliable encryption algorithms are used to authenticate users and confirm transactions, each transaction is protected from electronic replay attacks by electronic signature, EMV applications undergo mandatory multi-level certification upon receipt of permission from the payment system for their use. But when switching to the non-contact option of working with the advent of bank cards that support NFC, a number of problems were revealed that did not matter much earlier when the card was read inside the ATM or payment terminal. In particular, when making a payment, the card number and its validity period is transmitted in an open, unencrypted form, which in itself can be used for purchases in online stores.

If an attacker has the ability to influence on the operation of the payment terminal or invisibly to the card holder to use his own device that interacts with the card, then he will receive the owner’s name, a list of recent payments and other information. Such devices and related software are widely available and are described in the previous section.

Partially, the security problem is solved by using mobile devices with support for Apple Pay, Samsung Pay and other similar systems. The increase in the degree of protection is due to the fact that the exchange of information begins only after its initiation by the user, and not in each case of presenting the reader. If the attacker still managed to intercept the data on the card number and its validity period, he cannot use them for purchases in online stores, since the data used is a special virtual card with limited capabilities, and not a real card.

The above reasoning is also valid for other types of contactless smart cards using NFC technology. Since this technology alone does not provide any cryptographic protection, the security of a particular smart card and the information system in which the smart card is used depends on the security of the application layer algorithms.

4. Conclusion
In general, as practice shows, the technology of radio frequency identification and data transmission of short range does not contain inherent security problems. Manufacturers of software and hardware systems can be advised to proceed from the fact that all messages exchanged between NFC devices can be intercepted by an attacker in one way or another and this should not be a system vulnerability. The problem of unauthorized access to an NFC device lying in the user's pocket, should be solved by additional measures, such as asking the user for a password to initiate the exchange, or using additional biometric authentication methods for these purposes.

Assessing risks, companies should take into account the facts of the widespread adoption of technology in user devices and the reducing costs of equipment that can interact with NFC devices at a low level by sending non-standard commands. All this makes cryptanalysis very affordable, sometimes it is enough to use a smartphone.

We can confidently say that RFID and NFC technologies have a great future. This is confirmed by the fact that such large manufacturers of electronic devices as Apple and Samsung not only include support for relevant standards in their devices, but also remove restrictions for software developers to fully program and emulate NFC devices. In the near future, it will allow users to independently configure their personal electronic devices for use as a single electronic access key. In this case, the user should be responsible for his actions.

Reference
[1] IDTechEx. RFID Forecasts, Players and Opportunities 2018-2028. www.idtechex.com.
   Available at: https://www.idtechex.com/fr/research-report/rfid-forecasts-players-and-opportunities-2018-2028/642
[2] Courtois N The dark side of security by obscurity - And cloning MiFare Classic rail and building passes, anywhere, anytime ICETE 2009 pp 331-8
[3] Hancke G 2011 Practical eavesdropping and skimming attacks on high-frequency RFID tokens RFIDSec 9440 259-88
[4] Engelhardt M, Pfeiffer F, Finkenzeller K and Biebl E Extending ISO/IEC 14443 type a eavesdropping range using higher harmonics Smart SysTech 2013 pp 1–8
[5] Nohl K, Evans D, Starbug and Henryk Plotz 2008 Reverse-Engineering a Cryptographic RFID Tag 17th USENIX Security Symposium pp 185-93
[6] Gu W, Huang Y, Qian R, Liu Z and Gu R 2018 Attacking crypto-1 cipher based on parallel computing using GPU ATCSI 2017 pp 293-303
[7] Ahn H, Lee Y, Lee S-J and Han D-G 2016 Optimal MIFARE classic attack flow on actual environment Transactions of the Korean Institute of Electrical Engineers 65 pp 2240-50
[8] Yang M-H 2014 Security enhanced emv-based mobile payment protocol Scientific World Journal