Khudiakova Elena
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

NFC TECHNOLOGY AND ITS INFORMATION SECURITY

Abstract: *NFC data transfer begins when compatible devices are combined. Data transmitted between two smartphones via NFC is not encrypted, so there is a modern problem of personal data security, because we live in a world of the Internet, gadgets and various information threats. This article presents the results of the analysis of threats and methods to protect contactless cards from fraudulent attacks, as well as consideration of an innovative way to unlock smartphones with a tattoo.*

Keywords: *NFC technology, personal data protection, mobile technologies, information security, contactless cards.*

Худякова Елена Алексеевна
студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна
Кандидат педагогических наук, доцент
доцент кафедры иностранных языков и перевода УрФУ

ТЕХНОЛОГИЯ NFC С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *Передача данных NFC начинается, когда совместимые устройства объединены. Данные, передаваемые между двумя смартфонами* *через NFC, не шифруются, поэтому возникает проблема безопасности персональных данных, потому что мы живем в мире Интернета, гаджетов и различных информационных угроз. В данной статье представлены результаты анализа угроз и методов защиты бесконтактных карт от мошеннических атак, а также рассмотрение инновационного способа разблокировки смартфонов с татуировкой*

Ключевые слова: *Технология NFC, защита персональных данных, мобильные технологии, информационная безопасность, бесконтактные карты.*

Introduction

Smartphones began to support NFC technology with the release of Android OS version 4 «Ice Cream Sandwich» in 2011, Apple iPhone 6 in 2014 and smartphones based on WindowsPhone 8.1. A smartphone equipped with NFC is both a smart card used for payment and the reader itself, which is used to transfer money [0].

Therefore, the NFC chip is able to transmit data in both directions and does not require device authentication, it is a simple and more convenient replacement for Bluetooth. You can share links, passwords, contacts and other data between smartphones using this technology.

NFC data transfer begins when NFC-compatible devices are combined, so the user does not know when someone is interacting with his device. When interaction is carried out through reading passive tags or between two smartphones, the phone is able to perform destructive actions without the user's knowledge-download malicious code, steal personal data and take funds from a virtual Bank card associated with a smartphone [0].

In addition, since the data transmitted between two smartphones via NFC is not encrypted, there is a problem of personal data security. This problem is modern, because we live in the world of the Internet, gadgets and various information threats. Theft of personal data is possible by listening or intercepting unencrypted traffic. As a result of implementation of this threat un-authorized write-off of means from accounts of users, taking of logins and passwords from various services is possible.

The purpose of the research is to study the possibility of improving the security of personal data in the transmission using NFC technology in smartphones. The following research issues are considered in this work:

- methods to prevent relay attacks on contactless cards;
- threats and security methods when transferring data over the NFC interface;
- significant advantages of technology combined with a smartphone.

NFC technology and its information security

NFC (Near Field Communication) is a short-range wireless high-frequency communication technology that allows contactless data exchange between mobile phones, smart cards, payment terminals, access control systems and other devices [0].

Taking into account threats from intruders, it should be remembered that information such as personal data of the cardholder or Bank account details, messages should be protected from forgery and eavesdropping. To ensure security measures in contactless cards the following technologies are used in accordance with the scope of their application: secure communication, channel, reader authentication, card authentication и card access control.

Many smartphones are also equipped with Near Field Communication (NFC) interface, which allows them to interact with contactless readers and contactless cards. When interacting with contactless readers, the phone switches to card emulation mode, receiving APDU reader commands and responding with APDU responses over the ISO / IEC 14443 channel, or this circuit may be reversed. So the phenomenon can be controlled by an application on the device that turns it into a card emulator or reader according to its functionality [0]. This is, for example, the case of smart cards placed in a wallet, which in turn is stored next to a mobile phone, for example, in a pocket. In addition, mobile phone cases with some card slots along with the phone itself are also widespread nowadays. If one of the points is carried out, the short distance between the phone and the cards can allow contactless interaction between them, which means that malicious attacks can be implemented.

To defeat any attack, each user could wrap their contactless cards in a piece of aluminum foil. Users can be lazy, so it is usually difficult for people to take out a map, unfold it, and collapse it before each application. Therefore, it is the duty of developers to create an even more secure contactless card technology.

To prevent, even educated, brute force attacks, card responses can be delayed when a series of failed access control attempts have been made. In addition, blocking a card after a certain number of consecutive erroneous contacts is a good deterrent, but it can also be used by an attacker to launch denial-of-service attacks remotely by blocking cards under his control.

It is strongly recommended to protect contactless cards from relay attacks. For example, you can start a call-response session with an accurate measurement of the time of transmitted commands and responses, any delay in time means the presence of an attacker in the network. Thus, the NFC technology in contactless cards is not ideal. A Bank card can be used by an attacker to carry out malicious transactions such as identity theft or fraudulent payment transactions [0]. This can be achieved by using the victim's cards remotely, through the victim's phone being infected by the attacker and under his control. Therefore, users should know the precautions and clearly assess their risks.

NFC technology can be implemented in any sphere of life, so innovative unlock smartphones with NFC tattoos (Figure), which is very safe, was invented. There are several criteria that prevent the introduction of this technology into everyday life. At the moment, not all smartphones have a built-in NFC chip (it depends on the price of the gadget), and the constant activation of NFC leads to battery consumption, which is inconvenient for users [0].

NFC tags have a small amount of memory, they can be programmed as needed, do not have their own power supply, powered by magnetic induction. These labels are usually very small in size (most of them have an area of about 2 square centimeters), and therefore can be easily integrated into other everyday materials. This fact facilitates the introduction of labels into everyday items.

These problems are solved with the help of an innovative digital tattoo, which is simple enough to stick on the hand. Each tattoo is impregnated with an identification code that, when the phone's NFC radio is first detected, provides a quick setup to run, thereby synchronizing the code with the phone. So every time the tattoo falls within the detectable range of the phone, the code is checked and the phone is unlocked.

High quality glue is used to stick the tattoo on the skin. Each tattoo has a lifespan of up to five days. The inner parts of the tattoo are constructed using semiconductors that provide bending flexibility to suit the user's skin [1]. Every five days, the spent tattoo can be replaced with a new one, and the process of synchronization with the phone is repeated.

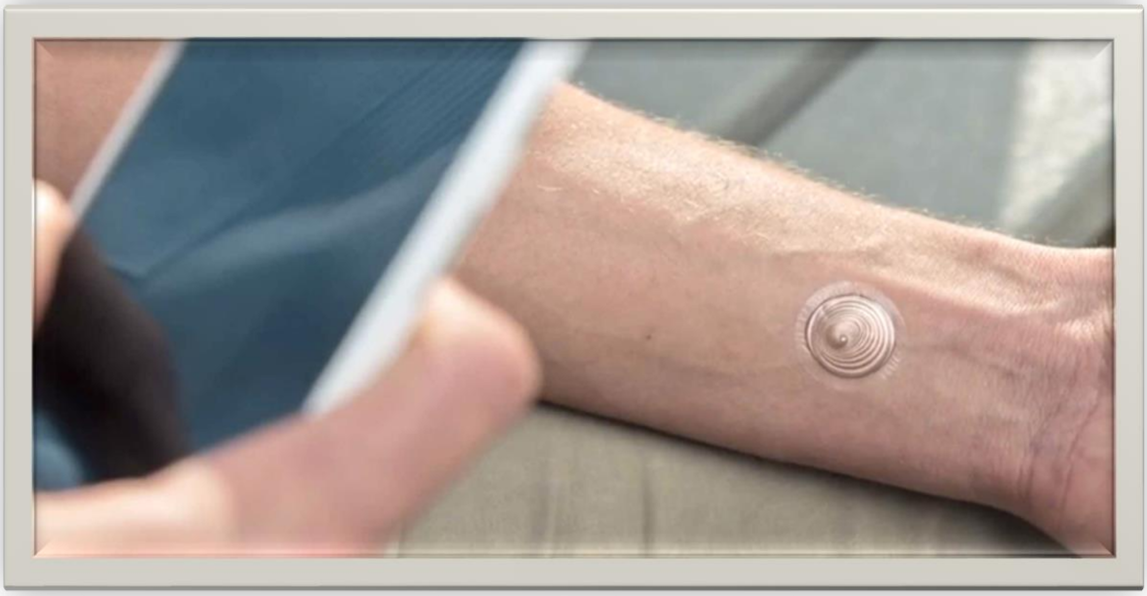

Figure 1. NFC-enabled tattoo

If the tattoo is lost, you do not need to worry, because a combination lock is used for safety. This gives you the right to unlock your smartphone without tattoos. Biometric systems such as fingerprint or retina scanners have a much higher error rate than an NFC-based unlock system. Thus, despite the post-season replacement of tattoos, the overall system is more economical than biometric systems.

Tattoo phone unlock technology is really safe. Thanks to NSF, this solution is very convenient, innovative and interesting, and therefore has the potential for development in society.

Conclusion

Currently, there are more and more contactless smart cards and mobile phones equipped with NFC technology in the world. It has sufficient information security, usability and development potential in the future. People really appreciate the convenience and safety of technology because it makes their lives easier. Of course, the paper contains a minimum number of examples of the NSF technology use, but other areas of this technology application will be studied in the future research.

REFERENCES

1. Sportiello Luigi. Internet of Smart Cards: A pocket attacks scenario. – Procedia Computer Science 45, 2019 – P. 67–83.

2. Jambusaria Utsav, Katwala Neerja. Secure Smartphone Unlocking using NFC. – Procedia Computer Science 45, 2015 – P. 465 – 469.

3. Irene Luque Ruiz, Miguel Angel Gomez-Nieto. Combining of NFC, BLE and Physical Web Technologies for Objects Authentication on IoT Scenarios. – Procedia Computer Science 109C, 2017– P. 265–272.

4. Amjed B. H. Altaweel, Loay Abusalah, Dima M. Qato. Near Field Communication Detection System for Drug-Drug Interactions. – Procedia Computer Science 140, 2018 – P. 314–323.

5. Yasufumi Takamaa, Tomohiro Itoa, Hiroshi Ishikawaa. NFC-based Tangible User Interface for Information Curation and Its Application to Analogy Game. – Procedia Computer Science 60, 2015 – P.1263 – 1270.