RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP, year II, v.2, n. 2, Jul./Dec. 2022.

NFC (Near Field Communication) understanding and acceptance

NFC understanding and acceptance (Near Field Communication)

Sanderson Vinicius Pereira Fonseca[1]
Welton Gomes Azevedo[two]
Guilherme Bessa Alves[3]
Jonathan Costa Pereira Julio[4]
Prof. Luciano Pimenta Valadares (Advisor)[5]

Submitted on: 08/18/2022
Approved on: 08/18/2022
Published on: 08/20/2022 DOI:
10.51473/rcmos.v2i2.341

SUMMARY

Although humanity's inevitable dependence on computers is no longer what surprises and admires some, despite its use being irreversible, there are other technological systems that go unnoticed, as is the case with the popularization of wireless communication interfaces between computers. The adoption of these wireless interfaces is happening in stages and, interestingly, the individual's lifestyle as a whole has changed, as NFC (Near Field Communication) technology allows the exchange of information quickly and on a short-term basis across devices. fully automatic compatible. This feature can be used with cell phones, tablets, electronic cards, tags or any device that has NFC technology. However, the lack of information about the device raises the question of how to adapt NFC and control its route? Since this mechanism not only eliminates the financial loss of physical interface wear and consequent service interruption, it also makes it possible for countless applications to require only one active device, marking the next big step in the propagation of wireless communication interfaces. For this reason, it is necessary to analyze how NFC technology works. Since for financial balance or any control of wireless communication, it requires balance, no matter how much the system is used, but effective control of use so that objectives can be achieved in less time and at the lowest possible cost. This type of transfer, therefore, makes it possible to exchange files between cell phones, such as photos, videos, music, website links, encrypted data, bank transactions, and can even replace the use of a credit card.

Keywords:NFC technology. Access control. Wireless interfaces. Short-term information.

ABSTRACT

Although the inevitable dependence of humanity on computers is no longer what surprises and amazes some, despite its irreversible use, there are other technological systems that go unnoticed, such as the popularization of wireless communication interfaces between computers. The adoption of these wireless interfaces is happening in stages and, curiously, the individual's lifestyle as a whole has changed, for, NFC (Near Field Communication) technology allows the exchange of information in a fast and short-term manner through fully automatic compatible devices . This feature can be used with cell phones, tablets, electronic cards, tags, or any device that has NFC technology. However, the lack of information about the device generates a question of how to adapt NFC and control its path? This mechanism not only eliminates the financial loss from the physical wear and tear of the interface and the consequent interruption of service, but also makes it possible for countless applications to require only one active device, marking the next big step in the propagation of wireless communication interfaces. For this reason, it is necessary to analyze how NFC technology works. Since the financial balance or any control of wireless communication requires balance, it does not matter how much the system is used, but the effective control of the use, so that the objectives are achieved in less time and at the lowest possible cost.

This type of transfer, therefore, enables the exchange of files between cell phones, such as photos, videos, music, website links, encrypted data, banking transactions, and may even replace the use of a credit card.

Keywords:NFC technology. Access control. Wireless interfaces. Short term information.

1 Sanderson Vinicius Pereira Fonseca.sanderson.fonseca@es.estudante.senai.br
two Welton Gomes Azevedo.welton.azevedo@es.estudante.senai.br Guilherme Bessa
3 Alves.bessaguilherme51@gmail.com Jonathan Costa Pereira Julio.
4 Jonathan.julio@es.estudante.senai.br
5 Luciano Pimenta Valadares. (Advisor).luciano.valadares@es.docente.senai.br

1. INTRODUCTION

Near Field Communication, better known as NFC, has changed the way we exchange information on a daily basis. Through this new technology it is possible to make approximate payments, the information from which can be transmitted to other devices without the need for a wired connection. This new system allows data to be exchanged from one device to another without a software intermediary, just by bringing a device that contains NFC technology closer to another and the data exchange takes place in a fraction of seconds. This problem-solving technique emerged in Japan between 2002 and 2004 due to some companies feeling the need for a device that transmitted short-distance communication, developing NFC.

Therefore, the rise of wireless networks and the development of electronic miniaturization have opened the doors for mass adoption of smartphones. In addition to enabling wireless communication via NFC, the same device can replace conventional cards with electronic payments, where it will soon be possible to make payments simply by bringing the smartphone closer to the receiver, in a faster and more practical way than that used today with magnetic cards or with a chip.

For this reason, the purpose of this research is to understand how technology is used via NFC, given that humanity is still dependent on solid connection interfaces, where some electronic devices that have this interface provide many connections and disconnections. Daily over time, they undergo mechanical degradation, being the main cause of failure and malfunction, causing losses. Therefore, this research is divided into three chapters, the first of which: refers to NFC technology; the second: the advantage of NFC for users; and, the third: the adaptation of NFC in devices.

2 NFC TECHNOLOGY

NFC technology uses a frequency of 13.56 MHz, bandwidth up to 424 Kbps for short-range wireless communication. The device needs to be within 4 cm away to initiate communication. This technology is known to work with a single approach to work, that is, wireless communication. Devices capable of supporting the NFC system are new Smartphones and Tablets that have NFC antennas in their components. The fusion of this technology has increased the popularity of NFC, greatly expanding its range of applications. The most common today are used to control access to public transport and leisure attractions and credit card point-of-sale terminals.

NFC tags are embeddable memory chips most commonly found in stickers and cards. They do not have a power source (passive), so their operation depends on an NFC reader and a magnetic field activated by the mobile device (active).

For a device to be compatible with the technology, it must contain an NFC antenna, which uses the contactless communication protocol set out in ISO 14443 (ORGANIZATION, 2003 p. 120). The need to control access to events has always existed, which is why the entire process from purchasing a ticket to entering the event is well known. This control develops over time. Using a smartphone and NFC to control access to events is a new part of this innovation. As it is relatively new, including in other areas of application, it is assumed that most users are inexperienced with the technology.

Adoption of NFC in mobile devices has grown rapidly and manufacturers have been adding the technology to their mobile device designs. It is estimated that around 400 million NFC-equipped mobile devices have been sold worldwide, and that number is expected to reach more than one billion by 2022.

2.1 Advantages of using NFC (Near Field Communication)

The main advantages for end users using NFC are: easy connection, quick transactions and easy data sharing. One of the foundations of information security is based on integrity, which aims to guarantee

that a document does not change its content after it is signed. To do this, the system must be able to detect unauthorized changes to content. The objective is for the recipient to verify that the data has not been improperly modified.

According to (Bruce Schneier, 1996) There are several techniques to ensure data integrity, one of them is called Hash or Hash sum, which is based on the creation of a unique sequence of symbols based on the document or data set.

The appeal of security for all types of transactions has led to the development of systems that use NFC technology, as its properties inherently provide an additional level of security in the systems in which it is applied. In the case of card replacement, it prevents “relay attacks”, which occur when smart card communications are relayed over long distances via alternative data channels. Among the different types of systems, one of them refers to authentication, which leads to the entry of events into the control application. Although it is not completely fraud-proof.

In the US and Japan, the technology has been used to buy train tickets, event tickets and even pay for purchases. On the Tokyo subway system, you can buy a ticket by simply holding your phone near the gate. This simple function has changed the way domestic travel and increased confidence in technology.

2.2 Adapting NFC to devices

The implementation of mobile computing services using NFC technology depends on security mechanisms for its operation. The techniques described allow the creation of functional solutions, but have usability or security limitations. Therefore, it is important that there are friendly and secure authentication protocols between mobile devices and servers that have the NFC system.

These protocols are called Protecting Touch (PT), PT1 is used for NFC storage tags, while PT2 uses MIFARE DESFire processor tags. Regarding the first protocol, it works with any storage tag and can be used as an authentication factor. This tag is used to store an authentication key that associates the application with another.

The cryptographic material stored on the smartphone is used to link the tag content to the installed application instance. This material can be symmetric or asymmetric to encrypt and authenticate NDEF messages.

PT1 data is conditioned in NDEF messages and can be stored on any type of NFC tag. The OTK Payload of One-time Registration (OTK) contains the user identifier (IDuser) where a counter index key (CT OTK), and the one-time key (kOTK). The registry payload is encrypted and contains a message verification code. Message encryption and authentication are done using keys known to the application and stored in a key vault implemented in the operating system. A random initialization vector for chaining cipher blocks is kept in the application's memory.

Assuming that the IDuser is 4 bytes for CT OTK, the length of the kOTK is 32 bytes, and the encryption is AES-128 and the encoding of the authentication message is HMAC-SHA-256 (32 bytes), the payload of the OTK record will occupy 80 bytes. And then it will be necessary to add an NDEF header of the type “fkaway.br:ptotk” with an OTK record name that can fit in 100 bytes, although the HMAC-SHA-512 and AES-256 record can fit in 130 bytes.

NFC tags can contain an NDEF record where it will activate the device automatically, through the Android Application Record (AAR) as shown in the image below.

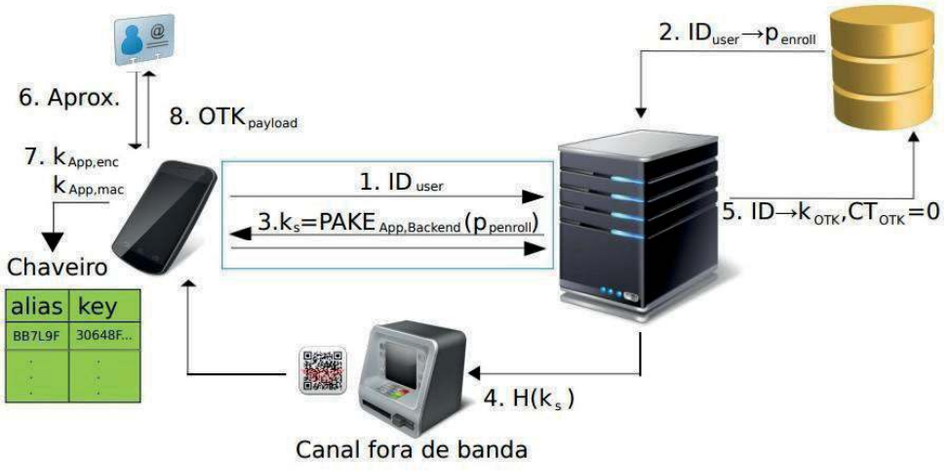

Figura 23 – Cadastramento inicial de etiqueta do Protecting Touch 1

During the initial registration of the tag, the application generates a new pair of keys and stores them in its keychain, thus the initialization protocol is triggered by the user where it will be entered in the IDuser (identifier) and Pen Roll (password).

The application begins interaction with the server by sending a user ID and indicates a new label, App æ Server: IDuser, is registered. Then the server loads the registration password from its database (using IDuser-based) and the authentication phase begins. If there is no match, communication with the application will be terminated. Therefore, the application and the server perform a key exchange, authenticated by the Pen Roll (password) (Application+Server: ks = PAKEApp, Backend (Penroll).

If the registration password is not considered strong enough, in some application scenarios, the authentication phase tication can be performed via an out-of-band channel. To do this, both the server and the application generate a hash using the shared key ks, so that the server passes the hash to the application through the out-of-band channel. The application compares the hashes to verify that it is communicating directly with the server. This out-of-band channel could be an ATM machine, which displays the hash in the form of an app-readable quick response (QR) code and prompts the user for verification results and once logged in, uses their bank account card and password. The application and server count down to zero and get KOTK from the session key. The server stores a one-time key and a starting counter in its database.

The user approaches the NFC tag after being instructed to complete the process through the app. Then the application generates new symmetric keys like kApp,mac and kApp,enc in your keychain. If it does not support it quickly, a new pair of asymmetric keys will be generated. And so, the temporary random keys kApp, mac and kApp,enc are generated, encrypted where they will be stored in the device's memory. Then the same application generates a new record - OTK and IDuser, which is nothing more than the initial key index counter together with a single-use key both encrypted to add message verification code using temporary symmetric or asymmetric keys and sends it for storage on the label.

Application + Label: OTK Payload

The authentication protocol is initiated by bringing the NFC tag closer to the mobile device. This can happen after the app instructs the user to approach the label, when the user taps the label, even if the app is not running.

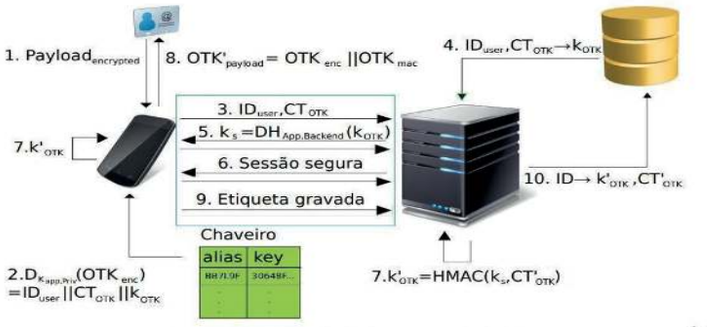

Figura 24 – Operação do Protecting Touch 1

The application reads the NDEF message from the NFC tag and extracts the OTK record.

Application + Label: OTK Payload

CONCLUSION

This work presents a method of applying NFC technology to a billing system, ticket control, messages or access control. One of the priorities of the work is to evaluate the acceptance of NFC technology among Brazilian users. The results show that the proposed model and NFC technology are well accepted in all aspects. Due to the small sample of users evaluated, the observed acceptance should be considered only as an indicator of the high acceptance of NFC technology in the Brazilian market for access control in any type of enterprise. Currently, NFC technology is mainly used for contactless payments, allowing smartphones to be used as credit cards making the process safer. The system does not only have this function, on the contrary, NFC has other functionalities, making it very useful to understand its functionalities on the cell phone. It is currently becoming popular in Brazil.

Therefore, it can be understood that NFC was designed to transmit data via electromagnetic waves remotely between the device.

The feature also has slower transfer speeds compared to Bluetooth. On the other hand, the advantages are almost instantaneous pairing and low power consumption. Therefore, the technology is considered safe precisely because it operates over shorter distances. Thus, NFC is a practical technology with many possibilities for use.

An example that is already being used on a large scale in Brazil is the use of NFC to pay for bus and subway tickets. In São Paulo, some cities, such as São Paulo, started offering the possibility of paying for buses directly with a credit card or even a smartphone with NFC. Just tap the machine, no need to enter a password, like any other bus card. NFC is a technology that goes hand in hand with the Internet or IoT (Internet of Things), which is a concept that means transforming everyday objects into smart and connected objects. It's about making it easier to use and more practical in daily work. NFC is precisely the ability to connect objects to a network and allow communication between them.

REFERENCES

ABDUL, DS; ELMINAAM, HMAK; HADHOUD, MM Performance**evaluation of symmetric encryption algorithms.**Communications of the IBIMA, v. 8, 2009.

BARCLAYS.**Contactless Mobile.**2012.. Accessed: 2015-09-30.

BOULOS, M., WHEELER, S., TAVARES, C., JONES, R., How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX,**BioMedical Engineering Online,**Vol. 10, 2011.

BURKE, B.**RESTful Java with JAX-RS.**[Sl]: O'Reilly Media, 2010.

CEIPIDOR, UB, et al., NFC:**Integration between RFID and Mobile, state of the art and future developments**, Emerging Technologies for Radiofrequency Identification, p.78-81, 2008.

FIDO Alliance.**FIDO NFC Protocol Specification v1.0.**2015. Implementation Draft.

FIDO Alliance.UB, MEDAGLIA, CM, MARINO, A., MORENA, M., SPOSATO, S., MORONI, A., Di ROLLO, P., MORGIA, M.La, **Mobile ticketing with NFC management for transport companies.**Problems and solutions, 5th International Workshop on Near Field Communication (NFC), 2013.

CHEN, L. Recommendation for key derivation using pseudorandom functions.**NIST special publication**, v. 800, p. 108, 2008.

CHOU, W.**Elliptic curve cryptography and its applications to mobile devices.**2003.

COSKUN, V.; OK, K.; OZDENIZCI, B.**Professional Application Development for Android.**[Sl]: Wrox, 2013.

COSKUN, V.; OK, K.; OZDENIZCI, B.**Professional NFC application development for Android.**[Sl]: John Wiley & Sons, 2013.

GALITZ, W.O.,**The essential guide to user interface design: an introduction to GUI design principles and techniques**, John Wiley & Sons, Inc., 3rd ed., 2007.

IGOE, T, JEPSON, B., BEGINNING.**NFC: near field communication with Arduino, Android, Phonegap**, O'Reilly Media, Inc., pp.11–15, 2014.

MADLMAYR, G., LANGER J., KANTNER. C., SCHARINGER, J.,**NFC Devices: Security and Privacy, Third International Conference on Availability, Reliability and Security**, ARES 08. 2008.

MATOS, AV Development**of an application prototype for a device with the Android operating system for the management of an event by a producer.**Federal Technological University of Paraná, 2012. Dissertation (Postgraduate course for Specialization in Java Technology). Available at: http://repositorio.roca.utfpr.edu. br/jspui/bitstream/1/830/1/CT_JAVA_VII_2012_19.PDF. Accessed on June 17th. 2022.

NFC-FORUM.**NFC and Contactless Technologies.**Available at: http://nfc-forum.org/what-is-nfc/about-the-technology/. Accessed on June 15th. 2022.

ORGANIZATION, IS**International standard ISO/IEC 14443.**Technical Specification. 2003, p.18

POURGHOMI, P., SAEED, MQ, GUINEA, G. Secure**Cloud-based NFC Mobile Payment Protocol.**Available at https://eprint.iacr.org/2014/538.pdf. Accessed on October 25, 2022.

ROLAND, M.,**Software Card Emulation in NFC-enabled Mobile Phones:**Great Advantage or Security Nightmare? Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 2012.

SCHNEIR, B.,**Applied Cryptography**, 2nd ed., Mountain View, p.14-15, 1996.

VISA, pay.**Wave for Mobile**, Available at: https//www.developer.visa.com/paywavemobile. Accessed on 20 June. 2022.