Summary of NFC and providing a method to improve security at NFC

Omid movagharIslamic Azad University, Tabriz,Iran

Abstract—For the first time, the idea of NFC introduced in 2004. In fact, this technology developed for smart phones and the similar devices to define a simple communication. The devices equipped with NFC technology can act as contactless smart cards; also they are able to read and write the data. Electronic payments are one of the most important applications of the NFC. This article classifies the applications and the problems ofthe NFC technology,thenproposes and examines a new way to improve the security of electronic payments.

Index Terms— Bluetooth، Mobile payment،near field communication، RFID.

1 Introduction

The NFC or Near-Field Communication is a kind of short range wireless communication and a set of standards designated for small and portable devices to create radio communications. This provides a standard coverage for the information exchange and the communication between devices. This is based on radio frequencies (RFID)and is used for data exchange at a distance less than 10 cm, in frequency band of 13.56 MHz with a speed of 424 Kbits/s.Low energy consumption and its proper relative security are two important achievements of this technology. If someone wants to infiltrate your device through NFC or interfere the connection of your device with another devicehe/she should be very close to your device which is almost impossible to do it without your suspicion. NFC can transmit data in two different states; active and passive. An active device is capable of producing its own radio frequency (RF) and sending it to the environment. In contrast, a passive one does not have the ability to produce these waves and uses the waves produced by the opposite device. Always, in NFC communication one side is considered as the initiator and the other side as the target; the initiator propagates the short range radio frequencies and creates energy in the target, leading to formation of a kind of command in the target. For development of the NFC technology, several features are considered. Over the air technology (OTA) that enables the system to operate without any prerequisite and Secure Element (SE) that is the prerequisite to save the high value information and provides a secure environment for concurrent (synchronous) connection of smart card with the NFC services. Fast development and high potential of this technology cause many software's and services make use of it, such as electronic payments, identification, access control, smart advertisements, cash or data transfer, etc. Also, by activating the NFC on your mobile phone, you can easily do a lot of everyday tasks very simply. For example, only by taking your phone near the printer, you can transfer the photos and print them.

2 NFCApplications

NFC is more than anything related to "mobile wallet". An idea that replace your cash and credit cards with your smart phone.Google Wallet is an example of that. You can save your information in Google Wallet and get a "virtual bank(credit) card", then you can pay all your purchases and expenses. Below are some of the most important applications:

2.1 Mobile payment:

Taxi or ticket payment through NFC-capable mobile phone
Payment for goods through mobile phone with NFC capability in stores equipped with contactless card readersStore coupons on a NFC-capable mobile phone

2.2 Identification, access control and electronic key saving

- Secure access to building
- Secure access to PC
- Secure access to ATM
- Locking the car doors

2.3 Data transfer among NFC units

- Print the photo by approaching the camera to the printer

2.4 Access to digital information

- Read the smart advertising posters info
- Get maps from related posters
- Record the location such as parking

For NFC to be publicly accepted, all categories and roles,as summarized in table 1, must do their job correctly. They areamong the factors affecting NFC's success which must have an integrated and coordinated performance.

Table 1. Effective factors in success 1

category	roles
NFC chip market	Designs and manufactures the chips for NFC, such as NXP.
Secure element manufacturer	Produces the secure elements for NFC payments.
Mobile phone manufacturer	The companies producing mobile phones.
Service managers	Provide suitable platforms for network operators and mobile users
Producers of mobile operating system	The companies producing the mobile operating systems
Application developers	They develop the applications like payment application, such as Google Wallet.
Customers	Customers are the main point in accepting this technology. To adapt the customer's needs with the features of this technology makes it easy to accept this technology.

3 Comparison between Bluetooth and NFC

Bluetooth and NFC are very short range technologies in cellphone device and both are considered as wireless communication. The NFC has a higher speed than the standard Bluetooth. The Bluetooth is a wireless communication protocol for connection of devices to each other that despite the lower speed than Wi-Fi makes it much easier to connect devices and is usually preferred in direct connection between two of them. Considering the fact that almost all smartphones support the Bluetooth, this technology has become a default way for wireless connection of speakers, headphones and other accessories to smartphones. Except for smartphones, the Bluetooth can be found on other electronic devices like printers, remote devices and personal computers. Among the radio communications available on smartphones the NFC and the Bluetooth have a shorter range, the first one several centimeters and the latter several meters. The NFC technology is better for e-payments and the Bluetooth for file transfer. The NFC's operating frequency (13.56 MHz) is much lower than that of the Bluetooth (2.5 GHz). Owing to this difference, the Bluetooth can support the fast transfers in several meters away. But the NFC with its short range has attracted the attention of many companies including Google, Microsoft and companies providing credit cards toward the e-Wallet payments. If you have information about antennasyou know that each of them works with a certainoperating frequency.The wavelength corresponding to the operating frequency of the NFC is 22 m which means that a half-wavelength antenna suitable for receiving and sending via NFC should be 11 meters long [12].It is clear that the NFC antennas of the smart phones can't be that large. On the other hand, if there is no antenna there is no connection and digital wallet will not be meaningful.

Table 2. Comparison of NFC and Bluetooth 1

Properties	**NFC**	**Bluetooth**
RANGE	Several centimeters	Several meters
Type of network	point to point	**WPAN**
Frequency	13.65 MHz	2.5 GHz
Energy consumption	Low	High (Since it uses more waves)
BIT RATE	424KBIT/S	2.1MBIT/S
Installation time	Less than 0.1 s	Less than 6 s
Standard	ISO/IEC	BLUETOOTH SIG

4 Security and Issues

Since NFC technology is a wireless standard it is clear that the security issues regarding that will be of great importance. This technology is inherently worrying because it can transmit sensitive data through waves and this data can be accessed illegally during transmission. Interestingly enough, the NFC protocol itself has kind of security protection against data eavesdropping. The measures taken by the NFC Forum are limited to the physical aspects of this protocol.For example, the maximum range of the NFC whentransferring data between two devices is 4 inches, so it will be very difficult to

eavesdrop or unauthorized (illegal) access to data within this small area.

4.1 Different kinds of security on NFC

Two main parts of the NFC security are:

- **Security of data analysis in NFC tags:**Inread / write mode these attacks play a very important role as long as the NFC tags are the main elements. The way to dealing with them is to use appropriate encryption techniques.
- **Security in Secure Elements (SE):**If thesecurity of these elements is not taken into account, the applications of the host controller may run without informing the user or malware applications within the host controller or the secure elements can use other data stored on the device.

4.2 Secure Element in NFC

To replace the normal smart card with NFC technology the most important factor to be considered is the system security. To solve this problem, the additional elements are added to the NFC as "secure element". A secure element is a combination of hardware, software, interfaces and protocols stored onthe NFC mobile and makes secure storage possible. The secure element provides the security and secure storage for NFC-capable devices and applications and includes the followings:

- Embedded hardware: An item that is embedded inside a mobile phone and is customizable by the user.
- SMC (secure memory card): Are made by memory and smart card elements.
- UICC (universal integrated circuit card): Secure SIM cards that protect personal information from users.

4.3 Different kinds of security threats

NFC platforms are still prone to attacks. There are different security threats in this technology. The most important of them are listed in Table 3 along with coping strategies.

Eavesdropping: Since the NFC system works through waves, the eavesdropping is a reasonable attack that does it by powerful antennas and signal amplifying. This attack influences the confidentiality of the NFC system.

Altering and destroying the information: The attacker manipulate (alter) the message by signal modulation

AddingInformation: If the device waits for response for a long time the attacker can send its information. This attack affects the accuracy of NFC system information.

Man-in-the-middle attack: In this attack, the third person is as an interface between the device and the NFC system or replaces them.

Security issues regarding NFC tags should be checked in a limited range, usually a few centimeters. Of course, receiving the signals by the attackers in the range of one meter or more, depending on the kind of the signal, is possible.

Strategies for dealing with threats	Type of threat
Secure channel	eavesdropping
Making the ability to recognize the power consumption	Destroying information
Permanent controlling the radio field, Secure channel	Altering the information
Send responses to the recipient without interruption,	Adding information
Failure to launch this attack due to its features	Man-in-the-middle attack

Table 3. Different types of treats and the strategies to dealing with them

5 NFCin e-payments

Nowadays, with science and technology advances, we are gradually moving toward a magnificent evolution in various fields. One of the things we are going to talk about that is obvious changes in e-payments.With the help of new NFC technologywhich is developing in many countries, it is possible to make significant measures about payments without bills (banknotes) and remote payments. Of course this can lead to the significant savings in a variety of costs, most notably in paper consumption for banknotes as well as time. Since NFC is a communication interface, the NFC-equipped devices provide a variety of communication modes that can be categorized into three main groups [17, 18]:

Read / Write operation mode: In this mode, the mobile phone or any similar NFC-equipped device is able to read a RFID tag or write the data on it. First, by sending signals to the

NFC tag, two mobile phones start communication with it, then read the NFC tag by sending commands to it.
Peer-to-peer operation mode: In this mode, two NFC devices will exchange information between themselves by creating a radio link. The peer-to-peer interfaces use the NFCIP protocol which is capable of "request-response model" between two active devices. In this mode, NFC mobile phones can exchange any kind of information such as business cards, digital photos, etc.
Smart card emulator mode: When a NFC-enabled device changes to this mode can act as a smart card. In this operation mode, the card reader device can't distinguish between the (contactless) smart card and the NFC device. This communication method is based on the ISO 14443 standard originally developed for contactless smart cards and is suitable for e-payment and ticket-related applications. The advantages of each method are summarized in the table 4:

Table 4. various communication modes 1

Read / Write operation mode	Peer-to-peer operation mode	card emulator operation mode
Increased mobility	Simplicity of exchange information	Access control
Ease of implementation	pair with most devices	physical element simulation

In e-payments, it's enough the client close its NFC-equipped device to a payment terminal to show the amount of payment on it. The only thing to do is to press the confirm key or the pay button.

6 Proposed work

In this section a customer's behavior pattern recognition system is proposed to enhance the security in e-payment systems.
This model includes three phases:
Create normal profile: This phase involves saving all the information needed from each person and creating a normal customer profile.
Detection of behavioral abnormalities: In this phase a model is constructed that shows the normal and acceptable use of the system, then it finds any mismatch with the reference model in the current data and detects it as abnormal behavior. This phase is based on the sum of similarity coefficients.
Combination of the results: Each of the customers' criteria stored in their normal profile is checked individually by sum of similarity coefficients method. To achieve the final result, the results of each criterionmust be combined, then the decision is made on the normality or abnormality of the customer's behavior. If the authentication process detects an unauthorized user, access to services is blocked. Appropriate selection of features that reflects customer behavior will have a significant impact on the reduction of errors. This approach is based on Behavior Theory presented by Bandura in 1986.
The Parameters should be selected in such a way as to be measurable and as far as possible express the features and characteristics of an individual. Some of these parameters are:

- The time allocated to the user's electronic payment
- Number of Transactions and Payments
- Places and environments used,in terms of the days and hours of a week

In this method, using the input data set, the user's normal profile is formed then the similarity coefficient is calculated for each criterion, then the results are combined together and the final result is obtained.
In this process the values of the set of parameters are obtained bymonitoring the user's behavior. Finally, behavior of the user is compared with its normal profile, then existence ofany abnormality is investigated.

If the user's normal profile matches its behavior it is accepted; otherwise it is recognized as unauthorized user.

7 Conclusion

In this article NFC technology and related issues were briefly reviewed. Regarding the materials presented in this study, it can be concluded that the NFC technology has great potential for facilitating the daily routine of human activities. This has led various financial institutions and companies to invest in. With increasing development of this technology in daily life of people, in the near future we will see its more usage and applications. Nevertheless many improvements have been made in this area, this technology still needs more efforts about its security. Ultimately, this technology has been able to meet many of the expectations in spite of some security problems it faced.

References

[1] Pampattiwar, S. (2012). Literature Survey on NFC, Applications and Controller. International Journal of Scientific & Engineering Research, 3(2), 1.

[2] Coskun, V., Ozdenizci, B., & Ok, K. (2015). The survey on near field communication. Sensors, 15(6), 13348-13405.

[3] Strommer, E., Jurvansuu, M., Tuikka, T., Ylisaukko-oja, A., Rapakko, H., &Vesterinen, J. (2012, March). NFC-enabled wireless charging. In Near Field Communication (NFC), 2012 4th International Workshop on (pp. 36-41). IEEE.

[4] Ok, K., Coskun, V., Aydin, M. N., &Ozdenizci, B. (2010, November). Current benefits and future directions of NFC services. In Education and Management Technology (ICEMT), 2010 International Conference on (pp. 334-338). IEEE.

[5] Van Damme, G., Wouters, K., &Preneel, B. (2009). Practical experiences with NFC security on mobile phones. Proceedings of the RFIDSec, 9, 27.

[6] Kumar, N., Raj, M., Agarwala, N., Sharma, P., &Vineeth, N. Survey on NFC and RFID Technology.

[7] Ghag, O., &Hegde, S. (2012). A comprehensive study of google wallet as an NFC application. International Journal of Computer Applications, 58(16).

[8] Ozdenizci, B., Alsadi, M., Ok, K., &Coskun, V. (2013). Classification of NFC Applications in Diverse Service Domains. International Journal of Computer and Communication Engineering, 2(5), 614.

[9] Pourghomi, P., &Ghinea, G. (2012, December). Challenges of managing secure elements within the NFC ecosystem. In Internet Technology And Secured Transactions, 2012 International Conference for (pp. 720-725). IEEE.

[10] Madlmayr, G., Langer, J., &Scharinger, J. (2008, July). Managing an NFC ecosystem. In Mobile Business, 2008. ICMB'08. 7th International Conference on (pp. 95-101). IEEE.

[11] Sharma, V., Gusain, P., & Kumar, P. (2013). Near field communication. Department of Computer Science & Engineering Tula's Institute, The Engineering and Management College, Dehradun, Uttarakhand, 248001.

[12] Brown, T. W. C., &Diakos, T. (2011, April). On the design of NFC antennas for contactless payment applications. In Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on (pp. 44-47). IEEE.

[13] Chhabra, N. (2013). Comparative Analysis of Different Wireless Technologies. International Journal Of Scientific Research In Network Security & Communication, 1(5), 3-4.

[14] Madlmayr, G., Langer, J., Kantner, C., &Scharinger, J. (2008, March). NFC devices: Security and privacy. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on (pp. 642-647). IEEE.

[15] Reveilhac, M., &Pasquet, M. (2009, February). Promising secure element alternatives for NFC technology. In Near Field Communication, 2009. NFC'09. First International Workshop on (pp. 75-80). IEEE.

[16] Haselsteiner, E., &Breitfuß, K. (2006, July). Security in near field communication (NFC). In Workshop on RFID security (pp. 12-14).

[17] Ghosh, S., Goswami, J., Kumar, A., &Majumder, A. (2015, May). Issues in NFC as a form of contactless communication: A comprehensive survey. In Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on (pp. 245-252). IEEE.

[18] Roland, M. (2012, June). Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare. In Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (pp. 1-6).

[19] Mazhelis, O., Puuronen, S., &Raento, M. (2006). Evaluating classifiers for mobile-masquerader detection. Security and Privacy in Dynamic Environments, 271-283.

[20] Khan, S. S., & Madden, M. G. (2009, August). A survey of recent trends in one class classification. In Irish Conference on Artificial Intelligence and Cognitive Science (pp. 188-197). Springer Berlin Heidelberg.

[21] Joe, I. (2004). Internet-based device communication protocol with the client/server role exchange. Information Networking. Networking Technologies for Broadband and Mobile Networks, 1005-1014.

[22] Madureira, A. (2017). Factors that hinder the success of SIM-based mobile NFC service deployments. Telematics and Informatics, 34(1), 133-150.

[23] Badra, M., &Badra, R. B. (2016). A lightweight security protocol for nfc-based mobile payments. Procedia Computer Science, 83, 705-711.

Omid Movaghar: Master of Science in Software Engineering ,Azad University of Tabriz, In 2017, I graduated with a Masters degree ,I participated in the International Conference in Istanbul, Turkey, as the Department of Engineering and Research Technology

Email: omidmovaghar.g@gmail.com