SECURITY IN NFC-BASED APPLICATION:ANALYSIS OF ITS THREATS AND COUNTERMEASURE

BY

NOUR ELHOUDA TABET

A dissertation submitted in fulfilment of the requirement for the degree of Master of Information Technology

Kulliyyah of Information and Communication Technology
International Islamic UniversityMalaysia

SEPTEMBER 2013

ABSTRACT

Near Field Communication (NFC) is a recent technology that has been rapidly implemented in different areas in the market. NFC is a wireless communication technology that enables fast and low cost transaction to be conducted. This technology is based on RFID technology which has been in the market for over a decade. However, NFC comes to serve the areas where RFID failed to do so; areas that requires short range and a quick transaction. NFC has been already implemented in various fields including payment systems, access control systems, monitoring systems, ticketing systems, and many more. However, NFC technology is very recent in comparison to the other wireless technologies. This fact highlights the importance of carrying further studies that investigates the readiness of NFC technology as a service enabler, specifically in low risk tolerance systems such as payment systems. Google wallet is one of the first movers toward implementing NFC into a payment system called Google wallet. Yet, attackers could not resist the temptation of breaking such a new technology. Relay attack was introduced as one of the main threats that have been exploited by attackers. This research studies the security threats and gaps in NFC-based systems, and examines the feasibility of several countermeasures such as setting a time constraint, applying Distance-bounding protocol, and the possibility of procedural improvement.

خلاصة البحث

تقنية التواصل عن قرب و التي تعرف بالNFC تعتبر من أحدث التقنيات التي انتشر استخدامها خلال فترة زمنية قصيرة في عدة مجالات. تقنية الNFC هي إحدى تفنيات الشبكة اللاسلكية و اللتي تسمح بنقل المعلومات بصورة سريعة و غير مكلفة. تقنية الNFCمبنية على أساسيا تقنية ترددات الراديو و التي تعرف بRFID. تقنية الـ NFC أتت لتخدم المجالات التي لم تتمكن تقنية الRFID من خدمتها، كالمجالات التي تتطلب نقل معلومات خلال فترة زمنية قصيرة و بين مسافات محدودة. الى يومنا هذا، تم تطبيق و استخدام تقنية الNFC في عدة مجالات منها البرامج المالية، برامج المراقبة، برامج المحاسبة المالية، و غيرها من البرامج و المجالات. بغض النظر عن المجالات التي تخدمها تقنية الـ NFC فإن هذه التقنية لا تزال حديثة بالمقارنة مع التقنيات الأخري. هذا الواقع يفرض على الباحثين و الخبراء البحث في هذا المجال و التحقق من استعدادية هذه التقنية أن تخدم في مجالات عديدة، خاصة مجالات الدفع الإلكتروني. محفظة قوقل (Google Wallet) هي من أوائل المحاولات لاستخدام تقنية الNFC في مجال الدفع الإلكتروني. في المقابل، لم يستطع الهاكرز منع انفسم من اختراق حواجز هذه التقنة الحديثة. تم التعريف عن هجوم التتابع (Relay Attack)كأحد أهم المخاطر التي تم التعرف عليها ضد تقنية الـ NFC. هذا البحث يدرس المخاطر الأمنية في مجال تقنية الـ NFC، و يختبر بعض سبل المقاومة ضد هذه المخاطر و جدوى استخدامها في توفير حماية ضد الاختراقات الأمنية. من هذه الوسائل التي يتضمنها البحث فرض قيد زمني محدد، تطبيق بروتوكول احاطة المسافة، و امكانية تطوير و تحسين سير اجراءات و خطوات البرامج المتضمنة لتقنية الNFC.

APPROVAL PAGE

I certify that I have supervised and read this study and in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for degree of Master of Information Technology.

……………………………………
Media Anugerah Ayu
Supervisor

I certify that I have read this study and in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for degree of Master of Information Technology.

……………………………………
Akram Zaki
Internal Examiner

This dissertation was submitted to the Department of Information Systems and is accepted as fulfilment of the requirement for degree of Master of Information Technology.

……………………………………
Mior Nazri Mior Nasir
Head, Department of Information Systems

This dissertation was submitted to the Kulliyyah of Information and Communication Technology and is accepted as fulfilment of the requirement for degree of Master of Information Technology.

…...............……………………..........
Tengku Mohd Tengku Sembok
Dean, Kulliyyah of Information and Communication Technology

DECLARATION

I hereby declare that this dissertation is the result of my own investigation, except where otherwise stated. I also declare that it has not been previously or currently submitted as a whole for any other degrees at IIUM or other institutions.

Nour Elhouda Tabet

Signature …………………………… Date: …………………….

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

SECURITY IN NFC-BASED APPLICATION:
ANALYSIS OF ITS THREATS AND COUNTERMEASURE

Affirmed by Nour Elhouda Tabet

………………………… ……………………
Signature Date

ACKNOWLEDGEMENTS

Foremost, I am grateful to the Almighty God for establishing me to complete this dissertation. I would like to express my sincere gratitude to my advisor Assoc. Prof. Dr. Media Anugerah Ayu for the continuous support of my research, for her patience, motivation, enthusiasm, and immense knowledge. Allah's SWT blessing and then her guidance helped me throughout the difficulties of this research and the process of writing of this dissertation. There are no words that can express her greatness as a supervisor, as well as a mentor to me. She has pushed me to achieve what I have not considered to be possible in the past. She opened my eyes toward the bright future that ambition and hard work could bring to our generation. She is by far, one of the best lecturers, supervisors, and mentors I have been introduced to. Besides, my sincere gratitude goes to the dearest person to my heart, my mother, for her patience, her prayers, her love and support throughout the journey, and for having to cope with the stress I went through as if it is her own. My gratitude also goes to my beloved father Nouar Tabet for his full support in all means, and for being the role model I take in pursuing my higher education and carrying the urge of ambition toward a brighter future. I would like to also thank my siblings for their ongoing support and their unceasing encouragement. I also place on record, my sincere gratitude to my lab-mates Bro. Ahmad Faridi, Bro. Barroon Isma'eel Ahmad, Sis. Siti Aisyah Binti Ismail, and Sis. Aqqiela Zuhra for sharing their knowledge, time, and all the resources they could in helping me toward completing my dissertation successfully. one and all who, directly or indirectly, have lent their helping hand in this dissertation.

TABLE OF CONTENTS

Abstract ii
Abstract in Arabic iii
Approval Page iv
Declaration Page v
Declaration of Copyright Page vi
Acknowledgements vii
List of Tables x
List of Figures xi
List of Abbreviations xii

CHAPTER 1: INTRODUCTION 1
1.1 Introduction 1
1.2 Background of Study 3
1.3 Problem Statement 4
1.4 Research Questions 4
1.5 Research Objectives 5
1.6 Significance of the Study 5
1.7 Limitations 5
1.8 Organization of the Dissertation 6
1.9 Chapter Summary 6

CHAPTER 2: LITERATURE REVIEW 7
2.1 Introduction 7
2.2 RFID Technology 7
2.3 NFC Technology 8
2.4 NFC Operating Mode 8
2.4.1 Card Emulation Mode 9
2.4.2 Reader/Writer Mode 10
2.4.3 Peer-To-Peer Mode 11
2.5 Mobile-Based Payment Systems 11
2.6 NFC-Enabled Ecosystems 13
2.6.1 NFC-Based Attendance System 14
2.6.2 Smart Poster 15
2.6.3 Google Wallet 16
2.7 NFC Possible Attacks 18
2.7.1 Eavesdropping 20
2.7.2 Data Corruption, Modification or Insertion 20
2.7.3 Man-In-The-Middle (MITM) Attack 21
2.7.4 Relay 21
2.8 NFC Security Countermeasures 24
2.9 NFC Secure Communication Channel 26

CHAPTER 3: METHODOLOGY 28
3.1 Introduction 28
3.2 Research Design 28
3.2.1 Problem Identification 29
3.2.2 Formulating Hypothesis 30
3.2.3 Designing Experiment 31
3.2.4 Data Collection 37
3.2.5 Data Analysis 37
3.2.6 Conclusion 37

CHAPTER 4: NFC SECURITY THREATS: RELAY ATTACK 39
4.1 Introduction 39
4.2 NFC-Based Systems Threats and Security Gaps 39
4.2.1 Security Threats: Relay Attack 39
4.2.2 Security Gaps 41

CHAPTER 5: NFC SECURITY COUNTERMEASURES 45
5.1 Introduction 45
5.2 Setting Time Constraint 45
5.2.1 Experimental Results 46
5.2.3 Discussion of Findings 48
5.3 Distance Bounding Protocol 50
5.4 Procedural Improvement 54
5.6 Chapter Summary 58

CHAPTER 6: CONCLUSION 59
6.1 Conclusion 59
6.2 Reliability of Concept 60
6.3 Limitation 60
6.4 Suggestion for Future Work 61

REFERENCES 62

APPENDIX 1 65
APPENDIX 2 **.. 67**

LIST OF TABLES

Table No.		Page No.
2.1	Summary of Mobile Based Payment Technologies	12
2.2	NFC-Enabled Systems	14
3.1	Definition of Experiment Variables	32
3.2	Design of Experiment	34
3.3	Experiment Set of Devices and Applications	36
5.1	Result from Expirement with Model 1	47
5.2	Result from Expirement with Model 2	48
5.3	Relay attack detection based on position	52
5.4	Security Mechanisms Impact on NFC Characteristics	57

LIST OF FIGURE

Figure No.		Page No.
2.1	NFC card emulation mode	9
2.2	NFC reader/writer mode	10
2.3	NFC Peer-to-Peer mode	11
2.4	Framework for security areas in NFC payment system	18
2.5	Practical relay setup using NFC mobile phones Frsancis (2011)	23
2.6	Miller Coding Imhontu (2010)	25
2.7	Manchester Coding Imhontu (2010)	25
3.1	Research Stages	29
3.2	RTT for an NFC-based transaction	33
3.3	Practical NFC peer-to-peer relay attack setup	35
4.1	Framework for security areas in NFC payment system	41
4.2	Gaps in the current NFC security framework	42
4.3	NFC-based payment process flow	43
5.1	NFC-based payment communication	51
5.2	NFC-based relay attack setup in payment communication	51
5.3	NFC-based relay attack process flow	56

LIST OF ABBREVIATION

NFC	Near Field Communications
POS	Point of Sales
SE	Secure Element
TSM	Trusted Service Manager
CC	Credit Card
OTA	Over the Air
APDU	Application Protocol Data Unit
R-APDU	Response Application Protocol Data Unit
C-APDU	Command Application Protocol Data Unit
INTEG	Intelligent Research Group

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Near Field Communication (NFC) has been a new trend that many try to implement into their products and services. NFC is a short-range radio technology that enables communication between devices by either touching each other, or holding the devices close together. NFC wireless communication interface requires about 10cm working distance only Filipe (2011). The implication of this technology into banks, smartcards as well as mobile devices has been growing daily. The design of this technology differs according to its usage. The NFC interface can operate in several modes which are distinguished by the type of the device; whether it generates its RF field,or retrieve the power from the RF field generated by another device. However, this technology is driven from the idea of transferring data in a wireless medium. This idea gives the advantage of easy share to NFC. Hence, it would be a well accepted technology between users from different areas Filipe (2011).

Today, there are hundreds of millions of people who use contactless techniques in payment and ticketing cards Imhontu (2010), simply because of the increase of the number using the system, such as public transports. In big cities such as Hong Kong, Tokyo and London, the public transport system has been growing since late 1990s. Today, each of these cities has designed sort of NFC implementation plan.

The transportation system is just one of the main fields that NFC servesImhontu (2010). NFC provides services such as contactless transactions, data transferincluding calendar synchronization or electronic business cards,as well as access to online digital content. All of these services require some level of information; the user must have sort of an account or a profile that allows him to interact with the NFC device. The presence of information creates a level of threat according to type of information used in the NFC service. Take for an example, in transportation systems, the NFC card or device used has the information of the balance that the user has. Is can also provide the information of the last destination the user was at. In another NFC application such as payment smartcard, there is more information in it such as the user ID, account information and so on. In the second example the information stored within the NFC environment is much more sensitive than the data in the transportation system. This is important to focus on in order to highlight the threats that NFC technology could face Imhontu (2010), Filipe (2011).

The wireless nature of NFC technology makes it most likelythreatened by wireless network threats such as eavesdropping, spoofing, and others. The common attacks that been highlighted are lack of encryption that could lead to man-in-the-middle (MITM) eavesdropping, spoofing and corruption attacks, the ability to spoof Universal Resource Indicators (URI) from 'smart' posters used for NFC-enabled advertising, and defects in current NFC handsets.Storm (2011)

This research study focuses on investigating the level of security in NFC-based systems, and confirming the readiness of NFC technology to serve in several areas with different level of risk tolerance. It also examine the adaption of countermeasures in order to protect against the vulnerabilities and threats that NFC-based systems are imposed to, and confirms the feasibility and applicability of these countermeasures.

1.2 BACKGROUND OF STUDY

There have been many developments in the field of security over the years. Yet, with every new technology there are a set of new threats, new vulnerabilities, and concerns that should be studied in order to overcome them. The NFC technology itself has its own security concerns. It is not only the technology that needs to be studied, but also the services that come with the technology. For example, one of the services NFC offers is smart poster. For smart poster services, the interaction does not require a high level of sensitive information, so when studying the security threats it does not cover all aspects of sensitive data security. On the other hand, in transaction such as credit card payment using NFC enabled device, the security measures taken should be at the highest level. This highlights the fact that, the only way to ensure the security and privacy of NFC enabled services is to study all types of services offered by NFC, along with the devices as well as the environment that this services are carried out on. Collin Mulliner (2011) is one of the few who studied the NFC security threats. Mulliner is a mobile devices security researcher at Fraunhofer Institute for Secure Information Technology (SIT), Division for Secure Mobile Systems, as well as a member of the trifinite group which is a group of people interested in mobile and wireless security.

The minimum work that has been carried out in comparison with the rapid development of NFC-based systems is alarming. The speed of NFC growth in the market exceeded the speed of the research works required to examine the readiness of NFC to serve in systems with low risk tolerance. This dissertation is motivated by the recent development of the field of NFC systems.

1.3 PROBLEM STATEMENT

With the growing of the possible services that can be offered by NFC technology, using NFC has a promising expansion around the globe. Yet, besides being new into the market, one of the main factors that are holding NFCfrom rapid expansion is people's trust. The security level of NFC has not yet reaches a convincing level. It is yet to convince people to move from their comfort secure zone to the new NFC zone. Security becomes the top priority concern especially in services such as payment transaction. In order to gain the users trust, assumptions are not enough, there should be measures taken into consideration in order to secure the NFC based transactions.

In the recent years, there have been many studies that focuses on security threats and vulnerabilities in NFC systems.Mulliner (2008), Imhontu (2010),Francis (2011), Coskum (2012), and Roland (2013), the finding of these researches varies, but they all agree on one fact, that is NFC did not yet reach the security level required for it to be used in financial transaction around the globe. Relay attack is highlighted to be one of the most practical attacks that can be performed on NFC-based payment systems. Roland (2013) highlighted the recent improvements that were done by Google wallet to overcome the threats and vulnerabilities.

1.4 RESEARCH QUESTIONS

1- What are the security threats in NFC technology?

2- What are the measures taken toward higher NFC security level?

3- What method can be used to ensure NFC security?

4- How does this method strengthen the NFC security?

1.5 RESEARCH OBJECTIVES

1- To investigate the vulnerabilities of NFC.

2- To measure the level of each threat and the consequence of it.

3- To highlight the measures that should be taken toward secure NFC implementation.

4- To measure the impact of implementing some security methods into NFC.

1.6 SIGNIFICANCE OF THE STUDY

NFC technology is a new topic in today's market. Yet, the main factor limiting the spreading of NFC application is the security measures, especially in areas such as financial transactions. This study focuses on

- Measuring the threat levels in the NFC technology.
- Applying some security measures, and
- Testing the results in order to identify whether these measure increase the security level or not.

This research paper highlights the level of vulnerability and investigates the possible solution to improve the security level in the NFC-based payment systems.

1.7 LIMITATIONS

The study limited by the resources available for conducting the study. NFC based systems are not yet widely spread. This study is conducted in Malaysia, where the NFC has not yet been implemented in many fields. Also, the structure of the NFC devices as well as systems are not shared publicly, many manufacturers prefer to keep the details unknown. This limits the studies to be performed on all NFC based systems. Finally, the time constraint limits this study to be carried outin a wider area and application.

1.8 ORGANIZATION OF THE DISSERTATION

This study is carried out in International Islamic University Malaysia. The research will be based on the available tools, using personal handset, and gadgets that are owned by the Intelligent Environment Research Group (INTEG) Lab.

1.9 CHAPTER SUMMARY

Near Field Communication is a technology with a promising future. Yet, in order to get the market to move toward the implementation of NFC into their systems, there should be higher security measure, and stronger NFC security model.This chapter introduces NFC technology, and the work intended to be carried out in order to examine the current security level of the NFC-based systems. This research will also investigate the effect of implementingseveral security measures into NFC- based systems, and the factors influencing the adaption of these measures.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

The implementation of NFC technology into applications and services has been expanding. The main objective of this implementation is to enhance the current service level, offer new services, and provide the market with more opportunities and higher competitive advantages. Service providers saw NFC technology as potential service enabler. With the suggested abilities of NFC such as short-range communication, NFC appears to be the solution to many problems, one being the problem of carrying many items in a person's belonging**.**NFC technology hasopened the door fordifferent types of services depending on the operating mode that it is designedCoskun (2012). The concern now is to which level is NFC technology suitable. In some sectors such as the financial sector, implementing new technologies needs to be critically reviewed before it is implemented. On the other hand, basic implementation of NFC technology such as in smart posters might need a less level of criticality. The type of service that is enabled by NFC technology depends on the operating mode of the NFC tag.Imhontu (2010).

2.2 RFID TECHNOLOGY

Radio frequency identification RFID technology is one of the most used contactless transmission technology. RFID contains of two main components which are the reader; which is an antenna that is able to detect and read information from the RFID tag; and the transponder which is referred to as the tagImhontu (2010).. The transponder is a microchip that is attached to an antenna. The RFID tag allows a range of applications categorized by the tag's power source; whether it is active or passive.

2.3 NFC TECHNOLOGY

The technology of RFID was not capable to serve all types of applications, especially those that require fast and short distance transmission. That was the reason behind looking for a new technology such a NFC. NFC enabled devices contain a silicon chip that has the NFC system's antenna, analog modulator/demodulator for sending the receiving signals, and a digital circuitry.Imhontu(2010).The chip also contains RF-level detector that recognizes the NFC radio fields and convert them into 13.56MHz signals, and card-mode detector recognize the type of then tag detected. In order to transmit the energy and the data from one device to another, NFC uses a magnetic inductive coupling that is generated by the inductive antenna. In a scenario of a passive device, the power is generated by another active device and carried out by the magnetic field, while the passive device will absorb the energy in order to communicate with the other deviceCoskun (2012). This characteristic allows NFC devices to operate in different modes.

2.4NFC OPERATING MODE

There are three modes that NFC operates in; emulation mode, reader/writer mode, and peer- to-peer mode. The difference between these modes is in how to access the data and where is it kept. "In card emulation mode, the data resides in an NFC enabled mobile phone and external NFC devices access this data. In reader/writer mode, data resides in NFC tags or compatible RFID tags. NFC mobile phones or NFC readers are able to write data to these tags as well as reading data from those tags. While in peer-to-peer mode, two NFC-enabled mobile devices pair with each other." Kerem, (2011)

2.4.1 Card Emulation Mode

Card emulation mode gives NFC tags the ability of storing information. This characteristic will allow the user to eliminate the need of carrying many items. Some applications that use this mode are payment application Coskun (2012), and electronic key application Kerem (2011). NFC enabled payment application allows the user to pay using a mobile phone instead of paying using cash or credit cards. This eliminates the need to carry cash or credit and debit cards. The e-key application is one of the most common uses of NFC technology in card emulation mode.User's mobile device will act as a key to access hotel room, the user house, or any place that the NFC tag has been assigned to access. This is done by installing the e-key into the mobile device through an SMS or any other way. E-key application also allows the user to check-out using NFC technology. From this, we could say that besides the elimination of the need to carry cash or credit debit cards, NFC technology also eliminates the need to carry physical keys. Enabling physical access using NFC enforces a level of access control. Besides physical access and checking-in and out from hotels, an attendance system (Kerem, 2011)is another example for using NFC technology in access control.

Figure 2.1 NFC card emulation mode

2.4.2 Reader/Writer Mode

The secondNFC operating mode is the reader/writer mode where most NFC enabled applications operates under this mode.In this mode, data resides in NFC tags or compatible RFID tags. Smart posters are one of the applications of NFC in reader/writer mode. The idea of smart posters is to provide the user with the ability of reading the content of the poster by downloading it to an NFC-enabled mobile device. By downloading the poster data, the user can walk away from the poster without the need to write poster information manually, or even stand in front of the poster in order to finish reading the information and remembering it. Smart posters save users effort and time, as well as giving the application user the sense of mobility when collecting the information or performing tasks on the application. Shopping from home application Coskun (2012), Kerem (2011), is another example for applications that uses the reader/writer operating mode.In this application, the clients can shop while sitting at home using market’s NFC-tag equipped shopping binder and their mobile phones.

A similar service is offering patients the ability of uploading their medical information using NFC technology from their homes. Furthermore, people can also order their meals from their homesKerem (2011), Coskun (2012).. All these applications, whether it is already implemented or proposed only, aims to limiting human effort and providing the users with a comfortable and mobile experience.

Figure 2.2 NFC reader/writer mode

2.4.3 Peer-To-Peer Mode

Moving to peer-to-peep mode, we find fewer applications developed under this mode. The main use of this mode is for data transfer between devices. Coskun (2012), Kerem (2011).A single touch between NFC-enabled devices allows exchanging business cards, pictures, video or audio contents, and many other file types are designed in this mode.

Figure 2.3 NFC Peer-to-Peer mode

2.5 MOBILE-BASED PAYMENT SYSTEMS

There have been many technologies designed to serve mobile payment systems. Thecontinues development in the payment systems aims to improve the transaction process,maximize the security level, and create a simple payment method in order to satisfy the customers' requirements. The following table is a summary of these technologies.

Table 2.1: Summary of Mobile Based Payment Technologies

Technology	**Description**
Short Message Service (SMS)	- Store-and-forward technology - Nokia enabled users to pay using (SMS) text messages for soft drinks in Finnish vending machines in 1997
Unstructured Supplementary Service Data (USSD)	- Session oriented, transaction oriented technology. - USSD information is sent directly from a sender's mobile to an application platform handling the USSD service, McKitterick
General Packet Radio Service (GRPS)	- GPRS Mobile Payment System based on RFID is composed of Mobile Terminals, Communication Network, Mobile Payment Platform (MPP), Banks and Certificate Authority, Weib (2010)
3G (Third-generation)	- Packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps),
Wireless Application Protocol (WAP)	- WAP based sites offer a familiar form-based interface, and security can be implemented effectively. - Services require hosting a WAP gateway. Banerjee1 (2011)