ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

Prevention of Relay Attack Using NFC

Deepa S Pillai[1], S.Sathyalakshmi[2]

PG Scholar, Department of Computer Science & Engineering, Hindustan University, Padur, Chennai, India[1]

Professor, Department of Computer Science & Engineering, Hindustan University, Padur, Chennai, India[2]

ABSTRACT:Near Field Communication (NFC) is one of the emerging and promising technological developments for mobile phones and other contactless devices. NFC technologies allow two active devices embedded with chip transmit small pieces of data between each other via short range wireless connection and at low speed depending on the configurations. It offers low friction process because of the close range that the two NFC enabled devices can setup a connection. The combination of NFC with smart devices has led to development and range of NFC that includes data exchange, service discovery, connection, e-payment, and ticketing. With the help of a NFC enabled phone and card reader device, contactless card transaction can be performed. Security problems related to relay attack were analyzed and identified a proper solution to prevent the attack. In the proposed system, a Frame wait integer is used to check and verify data manipulation, by attaching the transacted data with a signed integer.

KEYWORDS: Relay Attack, Frame wait Integer, NFC electronic payment, RWD, Anticollision

I. INTRODUCTION

NFC is a short-range wireless communication technology and distance is around 4 inches. NFC technology operates in the range of 13.56 MHz frequency band and at a speed of 106Kbps to 424Kbps [4]. Combination of NFC with smart devices has led to development and range of NFC that includes data exchanges, service discovery, connections, e-payment, and ticketing,also replace credit cards in electronic payment. NFC is a set of standard for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually not more than a few inches. Communication is also possible between a NFC device and an unpowered NFC chip, called a "tag" [8]. NFC standard cover communications protocols and data exchange formatsbased on existing Radio-Frequency Identification (RFID) standards including ISO/IEC 14443 and Felica.

NFC offers a low-speed connection with simple setup, and used to bootstrap more capable wireless connections. NFC builds upon RFID systems by allowing two-way communication between endpoints. Earlier systems such as contactless smart cards were one-way only. The communication range of NFC is limited to a few centimeters; NFC alone does not ensure secure communications. NFC offers no protection against eaves dropping, data modification, and vulnerable to relay attack. Applications may use higher-layer cryptographic protocols to establish a secure channel.Noticeably, a considerable amount of increase in the number of research papers and activities concerning NFC technology.The current status of NFC research area is necessary to maintain the advancement of knowledge in NFC research and to identify the progress of NFC research [7].In fact, this intermediate level is introduced as NFC technology which is examined in terms of three major aspects; "Network and Communication" issuesuch as data aspect, new communication protocols, OTA transactions and the hardware issue dealing with "Tags, Antennae, Reader and Chip", "Privacy and Security" issuesuch as authentication, vulnerability, availability, confidentiality,authorization, integrity, non-repudiationwhich focus on developing design artifact rather than behavioral issue. This is positioned with pre-defined business related with to existing ecosystem, technology infrastructure, and applications.

It has been suggested that NFC systems are particularly vulnerable to relay attacks, and the attacker's proxy device could even be implemented using off-the-shelf NFC enabled devices. This project describes how a relay attack can be

implemented against systems using legitimate peer-to-peer NFC communication by developing and installing suitable MIDlets on the attacker's own NFC enabled phones. It does not need to access secure program memory nor use any code signing, and can use publically available APIs. Some of the countermeasures could be applied to prevent relay attacks on contactless applications using passive NFC on mobile phones [14].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

II. RELATED WORK

Security threats related to NFC card transaction particularly relay attack is in the scope of this project. Various mode of communication in NFC like peer-to-peer mode, active-passive mode etc. have been deeply analyzed. Studies have been done to develop Standards and Technical Reports for Near Field Communication Systems, for the realization of simple wireless communication between close coupled devices.In the current scenario the market share of smart phone users are increasing in an exponential rate. Out of the various services available in the smart phone, NFC is one of the most predominant features. But still the number of smart phone users who were using the capabilities of NFC is on the low side due to severe security implications. There were very less number of studies undergoing in this field for maintaining security in card transactions, preserving privacy information, etc. by utilizing the features of NFC.The opportunity to learn about a new area of technology not covered in lectures was appealing. Increased usage in NFC enabled smartphones and the potential of them being used as mobile wallets for doing all merchant transactions, replacing the traditional physical card swiping system inspired me to research further on this. As with all emerging technologies related to monetary transactions, the possible cases of security breaches through various forms of attacks and vulnerabilities further increased my quest to research further on this.Propose and design a NFC based card transaction system by preserving the authenticity of the transactions using the best available security measures. The system would incorporate the following services:

- The Merchant Terminal which interfaces with the secured data stored in the NFC device using an NFC card reader.
- A merchant Portal which enables the merchant to maintain his inventory of stocks and transactions.
- Suitable solutions to prevent the security threats in NFC like relay attack using Signed Frame Wait Integer (FWI).

III. LITERATURE SURVEY

The integration of NFC technology into mobile devices offers many reliable applications; specifically payment, ticketing, loyalty services, identification, access control, content distribution, smart advertising, peer-to-peer data/money transfers, and set-up services. NFC has become an attractive research area for many academics due to its exploding growth and its promising applications and related services. A total number of 5 different paper and methodologies have been studied.

Sl. no	Title of the Paper	Author	Objectives	Technology/Protocol used	Advantages	Disadvantages
1	Using NFC Phones for Proving Credentials	GergelyAlpar ,Roel	Secure authentication can be obtained by anonymous credentials	Tap2 Technology	Smart cards are ideal means for construction of privacy.	The smart card is assumed to be tamper-resistant
2	Improvements to NFC Mobile Transaction and Authentication Protocol	Muhammad QasimSaeed	Payment through mobile device using GSM	Chen's protocol	Compatible with existing GSM network	M-commerce is insufficient
3	Remote relay attack on RFID access control systems using NFC enabled devices	Wouter van Dullink Pieter Westein	Despite the use of cryptology used in access control	RFID Technology	SwissKnife solutions which claims to solve every security	Propagation delay of data is more

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

			systems			
4	An Overview of VeryIDX – A Privacy-Preserving Digital Identity ManagementSystem for Mobile Devices	Federica Paci, Elisa Bertino, Sam Kerr, Anna Squicciarini, Jungha Woo	Identity attributes that are send over WI-FI or 3G networks	VeryIDX system	A multi-factor identity attribute verification approach for mobile devices	J2ME environment considered is a little outdated in the current windows and android phone market.
5	An Indoor Interactive NFC Navigation System for Android Smartphones	Jing Hang Choo, Soon Nyean Cheong, Yee Lien Lee, and SzeHouTeh	An indoor navigation system using NFC technology	I2 Navi system	A simple, low-cost and reliable indoor navigation	System is designed only on one platform(Andr oid platform)

Table 1.1: Literature survey

IV. **PROPOSED SYSTEM**

A relay attack is one type of hacking technique. An attacker relays verbatim a message from the sender to a valid receiver of the message. Relay attacks are forecast to get more and more common with the increasing number of contactless devices. Several counter measures to avoid relay attack by using NFC technology. Various possibilities of security threats have been analyzed and identified a potential threat related to card transaction using NFC.
Security problems related to relay attacks were analyzed and identified a proper solution to prevent attack. In this solution frame wait integer is used to check and verify data manipulation, by attaching the transacted data with a signed integer.

ADVANTAGES OF PROPOSED SYSTEM

- Electronic payments can be done using contactless transactions by making use of NFC enabled devices.
- E-bills can be generated and stored in the initiating NFC enabled phone, thus making paper less.
- Increased portability of carrying single device for various transactions.

A. *Three pass Authentication Sequence*

E) The RWD (Read Write Device) specifies the sector to be accessed and chooses key A or B.

b) The card reads the secret key and the access conditions from the sector trailer. Then the card sends a random number as the challenge to the RWD (pass one).

c) The RWD calculates the response using the secret key and additional input. The response, together with a random challenge from the RWD, is then transmitted to the card (pass two).

d) The card verifies the response of the RWD by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).

e) The RWD verifies the response of the card by comparing it to its own challenge.
After transmission of the first random challenge the communication between card and RWD is encrypted.

E. *Relay Attack Prevention using Three Pass Authentication*

In a peer to peer communication using NFC chances of relay attack is on a higher probability. To prevent such vulnerabilities three pass authentication protocol is implemented using the Elliptic Curve Diffie-Hellman version.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

- Can do key exchange analogous to D-H
- Users select a suitable curve Eq(a,b)
- Select base point G=(x1,y1),With large order n s.t.nG=O
- A & B select private keys nA<n, nB<n
- Compute public keys: PA=nAG, PB=nBG
- Compute shared key: K=nAPB, K=nBPA, Same since K=nAnBG
- Attacker would need to find k, hard

➢ ECC Encryption and Decryption:

- Must first encode any message M as a point on the elliptic curve Pm
- Select suitable curve & point G as in D-H
- Each user chooses private key nA<n
- Computes public key PA=nAG

- To encrypt Pm : Cm={kG, Pm+kPb}, k random

- Decrypt Cm compute: Pm+kPb–nB(kG) = Pm+k(nBG)–nB(kG) = Pm

E. *Anticollision*

An intelligent anticollision function allows operating more than one card in the field simultaneously. The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.

D. Anticollision Loop

In the anticollision loop the serial number of a card is read. If there are several cards in the operating range of the RWD, they can be distinguished by their unique serial numbers and one can be selected (select card) for further transactions. The unselected cards return to the standby mode and wait for a new request command.

E.*Communication FROM the tag*

Data output from the tag is sent as a single contiguous frame.

S	b1	b2	b3	b4	b5	b6	b7	b8	P	b1	b2	b3	b4	b5	b6	b7	b8	P	b1	b2---b8	P	E

Fig 1.1: Data Frame

The 8-bits of each data byte (together with each byte's parity bit) are concatenated into this single frame.
The overall frame format is the "Standard Frame" as specified for the type A variant in the ISO/IEC 14443-3:2001€ standard.
S = 'start of frame' followed by one or more bytes (with least significant bit first in each byte).
Each byte is followed by a P (parity bit) where the number of 1's is odd in (b1 to b8, P).
E = 'end of frame' (after last byte's parity bit).

F.Basic Architecture

NFC enabled smart reader software is installed in the PC of the merchant outlet. A card reader is connected via USB to the terminal laptop.
Merchant portal software is running in the terminal where the card reader is attached. Once the merchant logged in to the portal he should be able to see all the transactions and should be able to maintain his inventory of stocks based on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

the transactions. Suitable algorithms have been implemented to prevent various security threats like relay attacks. Bank gateway emulator is used and a mobile wallet/mifare tag module is used to store the secured card data.
Electronic payments can be done using contactless transactions by making use of NFC enabled devices. E-bills can be generated and stored in the initiating NFC enabled phone, thus making paper less.

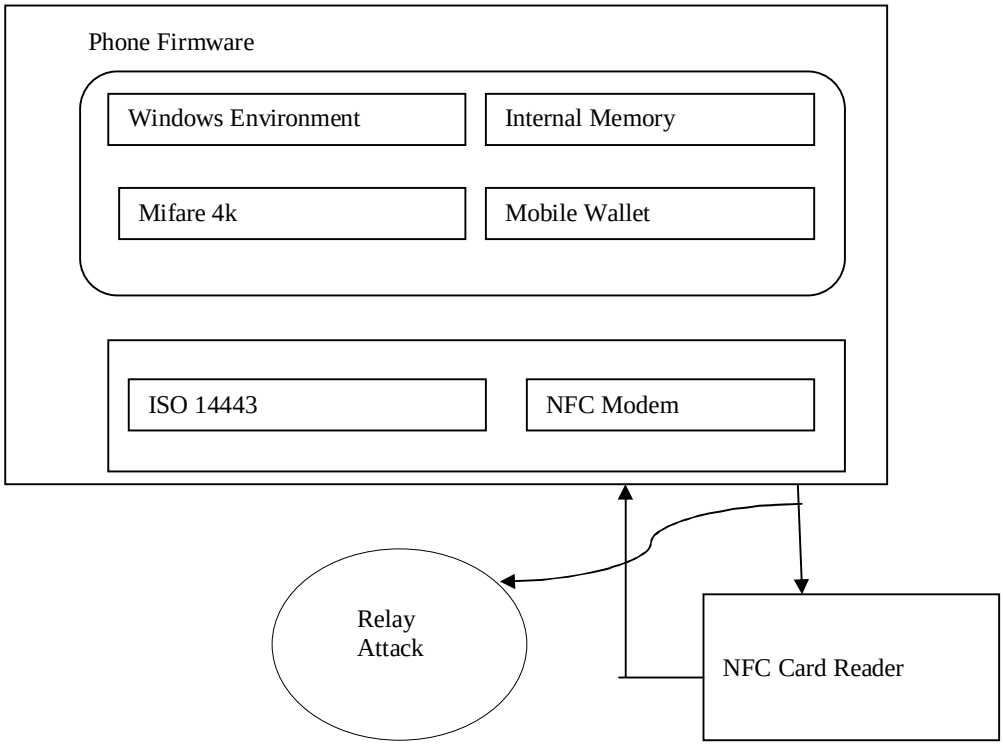
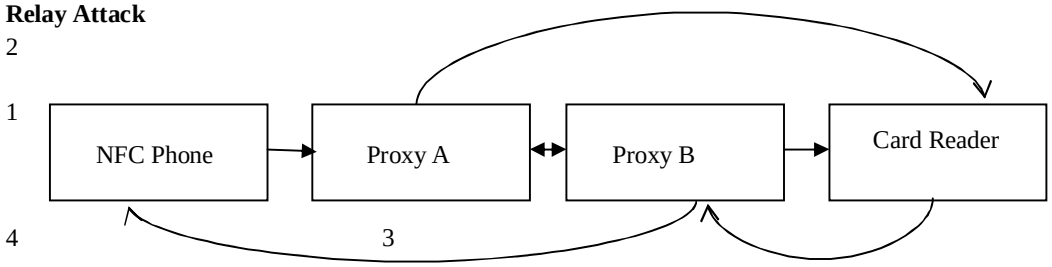


Fig 1.2: Basic Architecture

Relay Attack



1.Phone exchanges the command with proxy A.
2.Command from Proxy A is transferred to proxy B and card reader or other phone.
3.Card reader will sent message to proxy B.(the response of command message was transferred by card reader to proxy A via proxy B)
4.Proxy B will send to phone A.
This way an attack is performed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

- So to prevent this attack we introduce a counter measure as signing of FWI in the standard protocol data unit.
- The FWI is an unsigned integer, so signing this would result in moresecurity.

G. Relay Attack Implementation

The relay attack against two NFC enabled mobile phones operating in peer-to-peer mode and participating in a legitimate transaction. Phone A intends to interact with Phone-B to perform a legitimate peer-to-peer transaction. The attacker introduces two additional mobile phones into the transaction setup, namely Proxy-A and Proxy-B, to relay the communications between Phone-A and Phone-B [9].

1)Phone-A and Proxy-B
The role of Proxy-B, as name suggests, is to represent Phone-B and to relay communications to and from Phone-A. On phone-A, a MIDlet was implemented (3 kilobyte in size) that utilized the JSR 257 extensions API to realize NFC peer-to-peer communications. Phone-A is designed to switch between "reading" and "writing" modes as required [9].
On Proxy-B, a MIDlet was implemented (14 kilobyte in size) that utilized the JSR extensions for NFC peer-to-peer and JSR 82 API for IEEE 802.15(Bluetooth) communications. By default, Proxy-B was configured in "reading" mode and also supports "writing" mode. The NFC platform of Phone-A and Proxy-B supported the active peer-to-peer mode of operations for both Target and Initiator. Hence these devices performed "reading" and "writing" in active mode.

2)Phone-B and Proxy-A
Phone-B and Proxy-A were realized on two Nokia NFC mobile phones, based on FPI platform. Proxy-A represented Phone-A in the transaction and relayed messages with Proxy-B. Similar to Phone-A, on Phone-B a MIDlet was implemented (3 Kilobyte in size) that utilized JSR 257 extensions API to realize NFC peer-to-peer communications. Phone-B is designed to switch between "reading" and "writing" modes as required [9].

V. EVALUTION AND RESULTS

The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered provided one knows the relevant key and the current access condition allows the operation.

Access Bits Valid Commands Block Description
C13 C23 C33read, write □□3 sector trailer
C12 C22 C32 read, write, increment, decrement, transfer, restore □□2 data block
C11 C21 C31read, write, increment, decrement, transfer, restore □□1 data block
C10 C20 C30 read, write, increment, decrement, transfer, restore □□0 data block

TYPICAL TRANSACTION TIME:

Identification and selection procedure	4ms
Authentication Procedure	2ms
Memory Operations	2.5 ms-Read block, 6.0ms-write block

The value blocks have a fixed data format which permits error detection and correction and a backup management

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

VI. CONCLUSION

With recent release of various terminals equipped with NFC(Near Field Communication), electronic payment market using NFC is expected to be activated. Near field communication (NFC) is a set of standards for smartphones and proximity, usually no more than a few inches.With recent endeavors of practitioners and academics concerning the use of Near Field Communication (NFC), one can expect a bright future of NFC along with business opportunities. With the development of more and innovative NFC enabled applications for standards and policies is increased. Strategy for diffusion and adoption of NFC systems and economy of NFC systems need to be considered while developing new service that includes the costs of designing, developing, controlling and updating such system. NFC is a set of short-range wireless technology, typically requiring a distance of 10 cm or less. Also several security countermeasures are discussed to prevent relay attack using NFC Some counter measures take more time and complex algorithms used. So to prevent the relay attack, introduced another method is signing of FWT.

ACKNOWLEDGMENT

First and foremost I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work. It's a matter of pride and privilege for me to express my deep gratitude to the management of HITS for providing me the necessary facilities and support. I am highly elated in expressing my sincere and abundant respect to the Vice Chancellor Dr.S.Ramachandran for giving me this opportunity to bring out and implement my ideas in this project. I wish to express my heartfelt gratitude to Dr.E.R.Naganathan, Head of the Department, Department of Computer Science and Engineering for much of his valuable support encouragement in carrying out this work. I would like to thank my internal guide Mrs.S.Sathyalakshmi, Professor, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work. I would like to thank all the technical and teaching staff of the Computer Science and Engineering Department, who extended directly or indirectly all support. Last, but not the least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

REFERENCES

[1] Busraozdenizci, Mehmet Aydin,VedatCoskun,kerem ok," NFC Research Framework: A Literature Review and Future Research Directions", Information Technologies Department, ISIK University, Istanbul ,Turkey ,April 2010.
[2] Busra,Mehmet,"NFC Research Frame work: A Literature Review And Future Research Directions", Published in 14th IBIMa Conference,23-24 June 2010.
[3] Ernst Haselsteiner and klemensBreitfub,"Security in Near Field Communication (NFC)", May 2011
[4] Eun.H, Lee.H, Son.J, Kim.S, and Oh.H, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-389, Janaury. 2012.
[5] Federica Paci, Elisa Bertino, Sam Kerr, Anna Squicciarini, Jungha Woo," An Overview of VeryIDX – A Privacy-Preserving Digital Identity ManagementSystem for Mobile Devices",Journal of Software, vol.4 september 2009.
[6] Felipe Meneguzzi, BalajeeKannan Katia Sycara Carnegie Mellon University, Pittsburgh, USA,"Predictive Indoor Navigation using Commercial Smart-phones",Journal of software May 2011.
[7] GergelyAlpar,LejlaBatina and RoelVerdult,"Using NFC Phones for proving Credentials",TNO Information and Communication Technology, Near Field Communication,International Workshop on,0:77-82,2011
[8] Gerhard Hancke," A practical relay attack on ISO 14443 Proximity Cards",University of Cambridge,February.2010.
[9] Jing Hang Choo, Soon Nyean Cheong, Yee Lien Lee, and SzeHou ,"I2 Navi: An Indoor Interactive NFC Navigation System for Android Smartphones", Information and Communication Technology, February, 2012.
[10] Lawrence Muriira.M and Nimrod Kibua,"Near Field Communication (NFC)
Technology:The Future Money Service", International Journal of computing and ICT Research,vol.6,issue1,pp.380-385,June 2012
[11] Lishoy Francis, Gerhard Hancke,Keith Mayes, "Practical NFC Peer-to-peer Relay attack using Mobile phones, Information Security Group,November.2009.
[12] Lishoy Francis, Gerhard Hancke,KeithMayes,KonstantinosMarkantonakis," Practical Relay Attack on Contactless Transactions by using NFC Mobile phone", Security Group, London, August 2010.
[13] Muhammad QasimSaeed,"Improvements to NFC Mobile Transaction and Authentication Protocol",IEEE Computer Society,2009.
[14] ShafeqRahman and jane Coughlan," An Efficient Mobile Payment System Based on NFC Technology",World Academy of Sciene, Engineering and Technology 78, pp.1695-1698, 2013
[15] Teo J.C.M, Ngoh.L.H, and Guo.H, "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks," Proceedings of the 2009 International Conference on Advanced Information Networking and Applications (AINA 2009), pp. 675-682, May 2009.
[16] VassillisKostakos&Eamonn O'Neill," NFC on mobile phones;issues,lessons and future research",Department of Computer scince,University of Bath,April 2012.
[17] Wolfgang Issovits and Michael Hutter," Weakness of the ISO/IEC 14443 Protocol Regarding Relay Attacks", IEEE International Conference on RFID-Technologies and Applications,2011
[18] Wouter van Dullink Pieter Westein," Remote relay attack on RFID access control systems using NFC enabled devices", February, 2013.