SURVEY ON SECURITY THREATS AND SOLUTIONS FOR NEAR FIELD COMMUNICATION

Neeta B. Thorat[1], C. A. Laulkar[2]

[1]*Department of Computer Engineering, Sinhgad College of Engineering, Pune*
[2]*Department of Computer Engineering, Sinhgad College of Engineering, Pune*

Abstract

Near Field Communication is evolved from radio frequency Identification and it is a new trends now a days. NFC is combination of contactless identification and short range wireless technology. NFC is a new and innovative technology with futuristic uses. This can have many security problems. This paper surveys security threats for NFC and solutions over those security solutions. Firstly paper start with providing the brief overview of what is NFC and how it work and after that presents overview of security threats and addressing them. Finally, analyze the main security solutions proposed until date.

Keywords— *NFC security, Tag, NDEF, NFC-SEC*

----------***----------

1. INTRODUCTION

NFC is intended to create a close proximity communication between two devices. The NFC Forum [16] is established in 2004 and it is standardized by ISO/IEC in [16]. NFC bases on Radio-Frequency Identification (RFID) by supporting a two way communication. NFC can be utilized to create other connections, e.g. to establish a Bluetooth connection by touching NFC devices. In addition, NFC is applicable for contactless payment, sharing contacts or starting some application by touching a tag. NFC utilizes 13.56 MHz radio band and a typical communication range is few centimeters.

Near Field Communication is expected to be one of the most important trends nowadays. NFC is a set of standards for smart phones. NFC is a short range wireless communication technology which is evolved from Radio Frequency Identification (RFID). It is combination of existing contactless identification and interconnection technologies. It was jointly developed by Sony and NXP Semiconductors (formerly Philips). NFC uses the principle of magnetic induction coupling to create a 13.56MHz radio signal when two devices are within very close range (up to 10 cm/4 in.) of each other, So that, in NFC, the communication occurs when two NFC compatible devices are brought together less than ten centimeters, or simply by touching themselves

NFC itself does not contain protection against eavesdropping or message modifications. Consequently, if confidentiality or integrity is required appropriate controls have to exist in the higher layers, e.g. in the application. In NFC, physical features of RF signal offer some security, i.e. short range and direction of signals. In other words, it is assumed that user is able to notice if the attacker participates to the communication, which means that, for example, when the reader/writer mode is on, the card emulation mode cannot be used.

The following section introduces NFC technology and its operation modes. The III section gives security threats and defenses against it. The IV section explains other security problems related to tag and NFC devices. Section V explains the best solution for security in NFC. Finally we provide a conclusion in the ending section.

2. OPERATING MODES OF NFC

NFCs functionality is divided into three different modes: reader/writer, peer-to-peer and card emulation. Only one mode can be selected at a time.

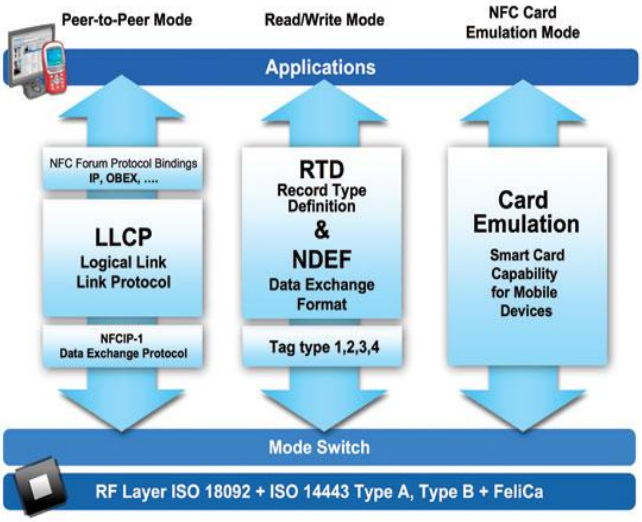

Fig 1: Modes of NFC.

2.1 Card Emulation

Smart-phone devices act like a contactless smart card when used in card emulation mode. This mode is used in NFC based payment and ticketing systems on smart-phones. ISO-14443 smartcard behavior is simulated by the NFC

controller of the smart-phone operating system. These mobile devices can be used in place of the typical smart cards used for payments or physical access control etc.

2.2 Reader/Writer

It allows the smart-phones to read data from NFC devices or smart cards containing RFID tags. The same phone can be used in writer mode as well where it is used to write tag information data on the blank and un-initialized tags. An NFC enabled smart device can read NFC tags, such as NFC smart poster tags.

2.3 Peer-To-Peer

Two devices can act as sender and receiver or active and passive device. Bidirectional communication takes place between two NFC enabled mobile phones to exchange information. The communication between the two devices takes place using the same channel in half duplex mode. NFC Data Exchange Format or NDEF is a standardized format which is used to store data on tags.

3. RELATED WORK

Security in short-range wireless networks is based on elements on various layers of communication. Confidentiality, authenticity and integrity are typically secured with cryptographic algorithms and security protocols on physical, link, network or application layers. Availability can be secured on the physical layer with spread spectrum technologies, e.g. frequency hopping and direct sequence spread spectrum, which makes radio signals more difficult to follow, intercept and jam[3]. In [14], Haselsteiner and Breitfuß show multiple attacks against NFC-based systems that rely on the lack of link level security of the NFC technology. The attacks range from eavesdropping to data modification, insertion, corruption, and Man-in-the-Middle attacks. In [12], Madlmayr et al. give an overview of security measures for NFC use cases and devices. They describe the possibility for NFC-based phishing attacks by simply modifying or replacing NFC-tags. Our work presented in this paper shows attacks that additional abuse vulnerabilities existing in NFC-devices.

4. SECURITY THREATS AND DEFENCES

4.1 Eavesdropping

Communicate between two devices over NFC channel can be intercepted or received by an attacker in the vicinity of the devices. The attacker can use bigger and powerful antennas than the mobile devices to receive the communication. This enables the attacker to eavesdrop an NFC Communication over greater distances. [14]

NFC does not have any specific or particular guard against the possibility of eavesdropping. It is pertinent to highlight that passive mode data transmission is comparatively difficult to be attacked upon than active mode communication. The use of passive mode only cannot be resorted to as many applications transmit data in active mode. Only solution to this type of vulnerability is to use a secure channel. The communication over NFC channel should be authentication based using the authentication and encryption schemes.

4.2 Data Corruption

The data corruption can be considered as denial of service if the attacker changes the data in an unrecognized format. The communication between the sender and receiver will be disturbed.. If the data stored on the tags or in the storage of the mobile devices is corrupted than it makes that particular tag to be useless and the mobile device would be required to get the data again. Another way to corrupt the data can be by transmission of the same or valid frequencies at the time when legitimate devices try to communicate with each other.[14] This sort of corruption can be performed by malicious software running on the same smart phone in background. This type of attack does not corrupt the original data but the data received at the receiver end is corrupted.

NFC devices are designed to be able to detect RF fields in which they communicate. If the devices can detect the strength of an RF field and the difference when there is some additional RF in the same field then it can effectively counter this type of threat. A higher amount of power than the typical power of the RF field is required to corrupt data being transmitted. The increased power should be easily detected by the NFC devices. These types of attacks are easily detectable and can be countered as well.

4.3 Data Modification

Moving forward from data corruption to data modification, where attacker changes the actual data with valid but incorrect data. The receiver in this case receives data manipulated by the attacker during its transmission. The attack requires expertise of the attacker in the field of wireless and radio communication where she can play and handle the amplitude modulations of the transmission.

Data modifications can be protected in a number of ways. Protection can be achieved by changing the Baud rate. Use of 106k Baud can stop modifications in active mode and make it impossible for an attacker to modify the data. But this implementation would require active mode be used at both ends to stop such vulnerability. This is practical but it increases the chances of eavesdropping manifolds. NFC devices are capable of checking the RF field before transmitting the data. The sending device needs to continuously monitor the RF field for possibility of such an attack and counter the effects of the attack. The best solution to defend against data modification attacks is to use a secure channel for transmission and reception of data.

4.4 Data Insertion

Rogue and unwanted data can be inserted in the form of messages by an attacker into the data while being exchanged between two devices. The success of attacker in this manipulation depends upon the duration of communication

and the response time of the receiving device. The attacker needs to respond to the devices before the legitimate device wants to establish its communication. If both devices, legitimate and the spoofed transmit at the same time then the data received at the receiver end would be corrupted.[6]

Data insertion by an attacker is possible when the answering device is slow to respond the first device. A possible countermeasure is possible if the answering device responds to the first device without a delay. The attacker does not get the window to insert malicious or manipulated data.

Another countermeasure to data insertion by attacker can be achieved if the second device which is at listening end, continuously listens and monitors the channel for its open time and start of a communication. The data insertion attempts by the attacker can be detected by the answering machine in this case. The best way to counter data insertion attack is by using a secure channel for the communication.

4.5 Man-in-Middle Attack

In Man-in-the-Middle Attack, third party tricks the two legitimate parties to be the other legitimate party and thus routing the communication between the two parties to go through the third party. After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.[14]

The distance at which the NFC devices operate is very short i.e. 10 cm. A Man-in-Middle attack is practically impossible to be carried out at such short distance. It is recommended that the communication mode for the NFC should be active-passive. Advice should be active and the other device should be in passive mode. The active device should monitor the RF field for any possible disturbance or attack scenario.digitally signed cards and readers. Therefore, we are going to use certificates management and asymmetric ciphered.

4.6 Relay Attack

In this attack the invader uses another communication channel (relay) as an intermediary to increase the range. The attacker needs no physical access to the device, but only an antenna and the relay in reading range. The other, perhaps more conspicuous, devices could be far away. This attack would compromise the secrecy of an NFC system.

4.7 High Distance Read

The attacker modifies an NFC device to increase its range so he can read tags from a safe distance. This is not easy, however. The attacker has to increase the energy of the high frequency field, use an optimized antenna and handle the increasing noise in the communication.

4.8 Social Engineering

In a communication medium where other devices can interact with the NFC device even contactless, is easy to use either a malignant card or a malignant reader to carry out unwanted operations. Solution: Only allow our NFC device interact with digitally signed cards and readers. Therefore, we are going to use certificates management and asymmetric ciphered.

5. OTHER SECURITY PROBLEMS RELATED TO NFC TAG & DEVICES

The attacks that can be performed on the NFC tag are as follows:

Destroy

This is the simplest attack which could be used. Afterwards the tag is not able to communicate any longer with an NFC device. It could be destroyed mechanically, for example by cutting the connection to its antenna. Another way to destroy the tag is an overpowered electrical field on the tag's working frequency, so that the electrical components would overload. Destroying The electrical circuits of the tag could also be done by placing the tag into a microwave oven. This attack would compromise the availability of an NFC system.

5.1 Remove

In this attack, the tag is removed from the carrier object. The motivation for this could be a thief, who wants to smuggle the carrier object through the security checks without recognition. This attack would compromise the availability of an NFC system.

5.2 Shield

This attack is only temporary and it could be done by placing the tag inside a metal box or a wrapping it in tinfoil. The inductive coupling is disturbed by high losses caused by eddy current induction inside the metal. This method could be used, for example, to pass automated toll checkpoints without recognition. The tag is not destroyed permanently. This attack would compromise the availability of an NFC system.

5.3 Clone

In this attack the original tag is read and an exact copy is created. The complexity of this attack depends on the tag. A read-only tag which stores only a simple numeric ID can be cloned very easily. There are also simple solutions possible where the ID can be changed. The reader can not decide if it is the original or the cloned tag. If some kind of certification is used, this attack would get more complex. This attack compromises the secrecy of an NFC system.

5.4 Falsify/Replace

This attack overwrites the data of a tag or physically replaces it. Overwriting can be done easily if the original tag is a writeable tag without any security measures (or these measures are broken). The aim of this attack is to falsify the original tag, e.g. for phishing purposes. This attack compromises the integrity of an NFC system.

5.5 Tracking

f a tag always uses the same unique ID for anti-collision (or is a simple read only tag with a numeric ID) an attacker could track the tag easily. If the tag is always carried by the user, his movements could be tracked. This attack compromises the secrecy of an NFC system.

5.6 Phishing:

Additionally to the technical issues there will also attackers try to mislead users by social engineering? The inhibition threshold of touching a tag or a reader with the mobile phone is probably much lower than making an intended connection with a wire. Thus phishing attacks could easily be performed by modifying or replacing tags.[12] This is a simple and inexpensive way to mislead the user. Using signatures on tags and transporters would be suitable way to overcome this issue.

5.7 Spoofing:

The tag data can be duplicated and transmitted to a reader. All read-only and r/w-transponder (without encryption)[12] are in danger; in addition, it cannot be detected by the reader device.

5.8 Skimming:

Unauthorized access of reading of tag data based on increase the reading distance of ISO 14443 with additional power to add additional noise to the load modulation side bands and increasing the antenna diameter to decrease the coupling factor.

5.9 Only one ID

Each tag has only one ID; which is used for identification and in the anti-collision algorithm. So it can be read and used by other card to supplant the owner's ID card. Solution: A random generation algorithm could be used to generate different IDs. This random 10 can be used in the anti-collision algorithm, so that real ID is just given when reader or tag is authenticated.

5.10 Privacy of the device contents

Malicious applications in our mobile could sniff the NFC index of applications existent in some cards (NXP in Mifare, JCOP, among others) and access to other resources of the cellular phone.[1]

Solution: We just allow access to application index to applications with a digital signature (for authentication that is not a malicious application), so we need to add digital certificates management to NFC devices. One more time, we are going to evaluate the cost of digital certificates management in NFC-powered devices.

5.11 Attacks on the NFC Device

An NFC device is often a complex and powerful device such as a mobile phone. Such devices are valuable to attackers and, thus, there is a high risk of attack. An example of an attack on the device is hacking into an application which uses the NFC interface. Attacks on NFC devices are performed either with the knowledge of the user i.e. the user is the attacker, or without the user's knowledge i.e. the hacker accesses the device through an internet connection.[1]

6. SOLUTION FOR SECURITY IN NFC

In this section we present the best solutions proposed so far to solve the security problems and threats associated with the use of NFC. The only solution to achieve security in NFC is the establishment of a secure channel over NFC. This can be done very easily, because the NFC link is not susceptible to the Man-in-the-Middle attack. Therefore, well known and easy to apply key agreement techniques without authentication can be used to provide a standard secure channel. This resistance against Man-in-the-Middle attacks makes NFC an ideal method for secure pairing of devices. Additionally, introduce NFC specific key agreement mechanism, which provides cheap and fast secure key agreement. Diffie-Hellmann key agreement protocol can be used in conjunction with RSA or Elliptic Curves to protect and authenticate the channel between two communicating devices. The arrangement can be augmented with use of symmetric key scheme like 3DES or AES. The arrangement can provide confidentiality, integrity and authentication.

NFC-SEC provide security standard for peer to peer communication of NFC. NFCIP layer does not provide any security for NFC. On top of NFCIP, NFC-SEC use to give security for NFC.NFC-SEC [9] defines a protocol stack that enables application independent encryption function on the data link layer. Security protocols of NFCIP-1 are standardized in ECMA 385 as NFC-SEC (NFC Security) and ECMA 386 as NFC-SEC-01.These security protocols are used in peer to-peer operating mode. NFC-SEC provides security standard for peer-to-peer NFC communication. Protocols that are included within NFC-SEC are defined to be used on top of NFCIP-1 protocol. NFC-SEC-01 specifies cryptographic mechanisms for key agreement, data encryption and integrity.

7. CONCLUSION

A list of threats has been derived and addressed. NFC by itself cannot provide protection against eavesdropping or data modifications. The only solution to achieve this is the establishment of a secure channel over NFC. This can be

done very easily, because the NFC link is not susceptible to the Man-in-the-Middle attack. Therefore, well known and easy to apply key agreement techniques without authentication can be used to provide a standard secure channel.

Also conclude that by using different IDs and digital certificates and due to use of secure element we can provide security to NFC tag and NFC devices

ACKNOWLEDGMENTS

I would like to thank my guide prof. C. A Laulkar, who guided me to conduct this survey, I would like to thank all the unseen authors of various articles on the Internet, helping me become aware of the research currently ongoing in this field and all my colleagues for providing help and support in my work.

REFERENCES

[1] Naveed Ashraf Chattha," NFC - Vulnerabilities and Defense", *IEEE Conference on Information Assurance and Cyber Security (CIACS)*, pp. 4799-5852, 2014 .

[2] Samia Bouzefrane, Amira F. Benkara Mostefa, Fatiha Houacine, Herv Cagnon,"Cloudlets Authentication in NFC-based Mobile Computing", *2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, pp. 978-1-4799-4425, 2014.I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[3] Antti Evestil, Jani Suomalainen2 and Reijo Savolal, "Security Risks in the Shortrange Communication of Ubiquitous Application", *The 8th IEEE International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 978-1-908320, 2013.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] Hasoo Eun, Hoonjung Lee, Heekuck Oh," Conditional Privacy Preserving Security Protocol for NFC Applications", *Consumer Electronics, IEEE Transactions on* , vol.59, no.1, Feb. 2013.

[5] Uwe Trottmann. " NFC - Possibilities and Risks", *Seminar FI & IITM WS2012/2013, doi: 10.2312/NET-2013-02-1 05 Network Architectures and Services*, February 2013.

[6] A. Lotito, D. Mazzocchi. " OPEN-NPP: An Open Source Library to Enable P2P over NFC", *in Proceedings of 4th International Workshop on Near Field Communication (NFC)*, pp. 57-62, 2012.

[7] Hsu-Chen Cheng,Wen-Wei Liao, Tian-Yow Chi, Siao-YunWei, " A Secure and Practical Key Management Mechanism for NFC Read-Write Mode", *ISBN ICACT* pp 13-16, 2011.

[8] Antonio J. Jara, Alberto F. Alcolea, Miguel A. Zamora, Antonio F. G. Skarmeta, "Evaluation of the security capabilities on NFC-powered devices", *ITG-Fachbericht 224 - RFID Systech* 2010.

[9] NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES, Jun 2010. ECMA-386 Standard (2nd Edition), *http://www.ecmainternational. org/publications/standards/Ecma-386.htm.*

[10] NFC-SEC: NFCIP-1 Security Services and Protocol, Jun 2010. ECMA-385 Standard (2nd Edition), *http://www.ecmainternational. org/publications/standards/Ecma-385.html.*

[11] C. Mulliner, " Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," *in Proc. International Conference on Reliability and Security*, pp. 695-700, 2009.

[12] G. Madlmayr, J. Langer, C. Kantner, J. Scharinger. " NFC Devices: Security and Privacy". *In Third International Conference on Availability, Reliability and Security*, pp7695-3102, 2008.

[13] NFC-SEC Whitepaper, Dec 2008. http://www.ecmainternational. org/activities/Communications/tc47-2008-089.pdf.

[14] E. Haselsteiner, K. Breitfu." Security inNear Field Communication(NFC)". *InWorkshop*onRFIDSecurity, 2006.

[15] Near Field Communication Interface and Protocol (NFCIP-1), Dec 2004.ECMA-340Standard(2ndEdition), *http://www.ecmainternational. org/publications/standards/Ecma-340.html*NFC Forum Specifications, http://www.nfc-forum.org/specs/