A survey on vulnerabilities in NFC devices, possible attacks and solutions

Chandini Shetty

Department of Computer Science and Engineering
University of California, Riverside

chandini.shetty@email.ucr.edu

Kiran Kumar G

Department of Computer Science and Engineering
University of California, Riverside

kiranriddle.kc29@gmail.com

***Abstract*—NFC is an upcoming short range technology that is widely being deployed for contactless payments. Most smartphones in the current market are shipping with NFC enabled- a dedicated hardware for storing the user's credit/debit information and loyalty programs. The goal behind this is to improve the user's ease of experience while paying for services/products at Point-of-Sale terminals without having to carry several cards. Recently ApplePay came out with NFC-based payment service option and enabling this in big retailers. NFC can also be used in peer-to-peer mode to support file transfers of small size- like user's exchanging contact information or pictures. Looking at these developments and increasing adoption of NFC, it becomes necessary to study the security framework of NFC hardware and protocols, due to the nature of the data that NFC handles. We need to closely examine the kind of security threats that NFC is susceptible to. In this survey, we carry out a study of the kinds of attacks that have been shown possible on NFC based applications & usage, and what solutions exist.**

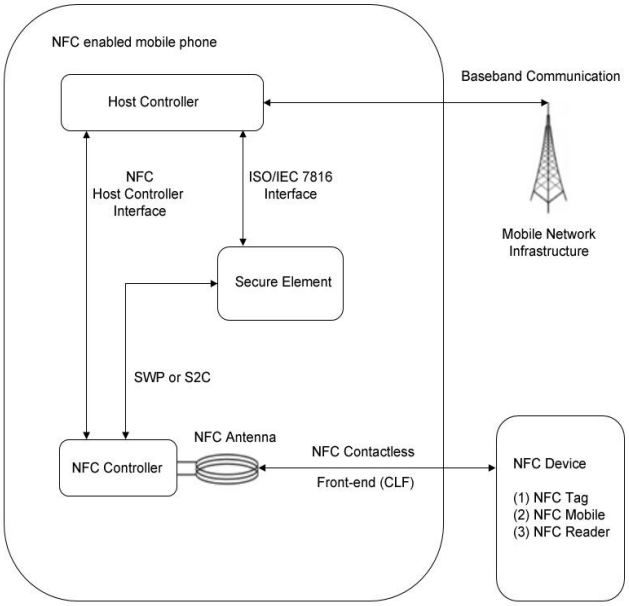
***Keywords*— NFC, Security.**

I. INTRODUCTION

NFC communication is being widely considered as a possibility for contactless payments and also achieving pairing ability between smartphones to do small transaction- like contact exchange. The main goal is to make the communication appear to user effortless by just tapping their smartphone against another NFC enabled devices. If the two devices are apart by a certain distance, then communication becomes impossible. The short range inherently ensures certain level of security and hence making it popular for financial transactions based applications. NFC standards states that the operating frequency of 13.56Mhz and based on data encoding scheme used (ASK/PSK) data rates of 106, 212 and 424 KBPS is achievable. Since NFC is a new technology, there are possible flaws in the design and vulnerabilities in the protocol, that could potentially decrease the adoption rate. Google Wallet which was one of the first popular NFC based application was demonstrated to have security vulnerabilities [8] by security firms which eventually led it to being not associated with NFC. Only the newer AndroidPay application which installs only on Android based phones, works with NFC with several fixes done for security.

In the next section, we briefly go over the architectural components of the NFC device [1] [3], with more focus on details that specific to security and are relevant to the discussion presented in future sections. Some additional protocol details like data exchange format, Link layer details related to data transmission are not covered for the sake if brevity.

A. NFC Architecture & Operation



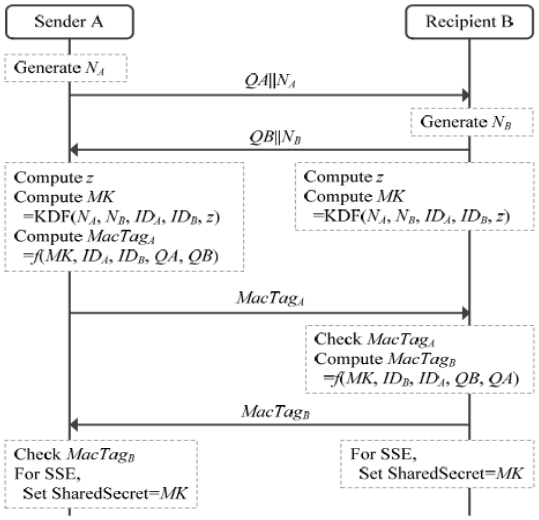
In a NFC setup, communication occurs over RF channel and happens through the magnetic induction between the antenna of the devices which decays with distance. On a smartphone, the NFC component mainly consists of a NFC contactless front end, a NFC antenna and a IC-NFC chip. A NFC reader is a device that can read the information from the smartphone, and transmit it securely to a connected server to complete verification of identity and authenticity.

In any NFC transaction, we distinguish between the two parties as an initiator and target. The initiator is usually the mobile phone, which generates a RF field and controls the transactions. A target can be a passive device (NFC Tag) or active device (mobile phone). If it's passive, then it has no energy source of its own and usually powered by the initiator.

B. NFC Secure element and NFC-SEC protocol:

One of the components of interest from security perspective in the NFC architecture is the Secure Element (SE) which stores and manages sensitive data like credit cards/PIN/ cryptographic keys. These are typically crypto chips, with a virtual machine (VM) running in secure mode. They cannot launch applications and can only respond to requests from upper layer applications. Any new application installation on the SE is managed by trusted entities. Access control to SE and possible vulnerabilities have not been widely studied and this is a possible area of further study. Only one study [7] showing the various scenarios under which the SE can subject to attacks -such as denial-of-service (DoS) and relay attacks - is explained briefly and at a high level. Hence we are unable to comment on the feasibility of such attacks or provide comparative analysis of this security aspect of NFC.

Another level of security already guaranteed in NFC is the NFC-SEC Protocol as defined by NFC standards [2] which provides protection from eavesdropping attacks and data modification. It requires usage of Elliptic Curve Cryptography – Diffie-Hellman scheme to generate shared secret key for encrypting all the data transmission. The secret key is then used in symmetric encryption protocol like DES. The schematic below from [8] describes the key exchange.



NOTATION

Notation	Description
$\|\|$	Concatenation symbol
N_X	Nonce of user X
ID_X	Random ID of user X for the activation of transport protocols
QX, QX', QX''	Compressed elliptic curve public key of user X
Q_X, Q'_X, Q''_X	Elliptic curve public key of user X
d_X	Elliptic curve private key of user X
G	Elliptic curve base point
KDF	Key derivation function
$MacTag_X$	Key verification tag received from X
MK	Shared secret key
z	Unsigned integer
r_X	Random integer generated by user X
PN	Pseudonym set
$Enc(k, m)$	Encrypt m with k
$Sig(k, m)$	Signature on m with k

C. NFC Modes of operation

Here we briefly go over how applications use NFC and three main ways in which it can operate.

1) Tag emulation mode:

A NFC Enabled phone can be used to tap against smart posters to launch the URL encoded in a NFC Tag or read product information which has NFC tags attached. A NFC tag is just a passive RFID tag and follows the standards specified by NFC forum. It contains data encoded in the NDEF format and has messages stored in binary format [NFC protocol cite]. An active NFC device generates the RF field which powers the tag and after this, the device can read or write from the tag. The tag itself has no power source and contains a very small memory capacity to encode information into it- say just enough to add a URL. Typically, NFC tags can be encoded any number of times until it is locked after which the data cannot be overwritten. However, attacks have been shown possible here by cloning the tags and also possible to change any unique ID information stored in the read-only memory by circumventing the authentication (challenge-response) present in these tags [10]. Newer NFC tags, although, come with built-in security features as 32-bit password authentication & detection of unauthorized copies [10]

2) Smartcard/Reader Mode:

In this mode, the NFC phone emulates a smartcard. A NFC reader cannot distinguish whether the device is smartphone or a smart card. The NFC reader directly communicates with Secure Element (SE) to obtain the stored credentials and verify.

3) Peer-to-Peer Mode:

In Peer-to-Peer (P2P) communication, two active mode NFC devices setup a communication link that is bidirectional and can transfer data- typically of smaller sizes like contact information or application specific. The RF interface is as per the NFCIP-1 specified in the NFC standards.

II. Types of Security Attacks

In this section we go over the various types of attacks and how they can be executed based the available studies that demonstrate these attacks in their work.

1) Eavesdropping: NFC with its short range of communication ensures certain level of security, especially at the physical layer. The perceived range of communication should be approximately 4-10 cm as per NFC standards published. However, researchers have showed that it is possible to carry out passive eavesdropping with special hardware [4]. The authors build a device of small form factor using readily available components- a small antenna, modulator and connect it via USB to a PC. The sniffer can eavesdrop for distances up to 250-300 cm for a range of smartphones. Also the possibility of eavesdropping attack increases when both the devices are in active mode, since RF power generated is quite high.

2) Tag based attacks: NFC tags are susceptible to attacks based on modification to the content stored on them. While content once written on the tag can be locked and prevented from being overwritten, this prevents the tag from being repurposed. The tag content can be manipulated by the attacker to point to a different URL and cause a malware to be downloaded when the user smartphone reads the tag. The URL is directly opened on the phone's browser and the user has no control once he taps the smartphone against a NFC tag. Another possibility is Denial-Of-service (DoS) attack where the originally embedded URL is changed or corrupted, and user is not able to make use of the intended service.

3) Relay attacks: In a relay attack, typically an attacker uses an alternative fast channel, to transfer the responses between two victim NFC devices (a reader and a target) thereby creating a NFC link between them even though they are separated by a distance. The attacker presents himself at a POS terminal with his NFC phone in card mode, and the NFC reader's response is transmitted by the attacker to a distant NFC enabled victim phone. The victim phone believes itself to be near a NFC reader responds back and this response is relayed to the NFC reader by the attacker. The lack of location based information, makes it difficult to detect the proximity between the devices making relay attacks a possibility.

4) Privacy based attacks: In any NFC transaction, where a user purchases products/good, in order to ensure security, key agreement has to occur and it follows the NFC-SEC protocol mentioned earlier. In the process of key agreement, a shared secret is generated using the user's public key in the first step. Malicious attackers who have managed to collect significant communication history over time, can start associating the public key with transactions and can build user profiles based on their buying habits. The ID to some extent anonymizes the user but not completely because a trusted third party should be able to track the user in case of a problem with the purchase. But any malicious attacker should not be able to associate the NFCID with associated user's real identity.

III. SOLUTIONS CURRENTLY AVAILABLE

Security measures in NFC has been studied widely and several solutions have been proposed. Some of them leverage existing solutions in the RFID and other wireless communications domain. Here we go over the solutions we have studied and try to reason out them.

A) Hardware Based solutions:

Many smartphones that have NFC chipset generate more RF power than they are typically designed to. This is shown by an experimental study carried out by researchers where they conclude that in active mode of communication, the NFC communication range is at least an order of magnitude more than intended. [4] Since the problem exist with the chip design, the paper looks at coming up with a hardware based solution non-invasive solution. The solution looks at attenuating the generated RF signal with the use of specialized hardware (nShield). A prototype is developed in which two looped antennas of different size are used- a larger antenna absorbs the RF energy and harvests while transmitting data to the initiator. The smaller antenna listens on all transmission outgoing from the initiator. This helps it to determine the RF power levels. An adjustable attenuator is multiplexed with the antenna load modulator and adaptive attenuation algorithm controls the attenuation levels. It is important to adjust the attenuation so that communication between the intended devices does not suffer. The algorithm piggybacks on the existing NFC device discovery mechanism to determine the RF power level and then does a Binary search algorithm to determine the optimum attenuation level. nShield also harvests the absorbed energy to keep itself powered and provide continued protection. The overall result is that the eavesdropping distance is significantly reduced to 30-50% from the original hence reducing the chances of the attack. While this appears to be overall effective in terms of thwarting attackers, the effect of this on NFC communications maybe significant. Also the attenuation determination algorithm could bring in some delay into the overall transaction in trying to adjust to the correct level.

Another hardware based solution looks specifically at protecting NFC devices from Tag based attacks. NFC interactions can sometimes be malicious. To jam these malicious interactions a jammer can be used. A typical RFID active jammer consumes a lot of power and thus requires an external power source and is also very big in size. Thus, NFC Guardian or EnGarde [5] for short, a hardware-based NFC security solution is proposed which is well-suited for the mobile phone form factor. The biggest advantage of EnGarde is its diminutive form factor. Firstly, EnGarde uses Passive NFC harvesting as the primary power source instead of batteries. Second, instead of generating an active jamming signal in the frequency domain, a passive jamming signal in the time domain generated using capacitive load modulation. EnGarde was designed in such a way that it achieves the following requirements:1. Protecting all modes of NFC 2. Transparently power. 3. No Impact on phone usability 4. Programmable rules 5. Fail safe. With a very small power consumption(6.4µW), EnGarde was able to generate the passive jamming signal to block the malicious NFC interactions. With selective URL blocking, the malicious content in NFC tags would be blocked from being accessed.

B) Software-based solution:

A Light weight security middleware [14] is yet another software approach for providing security in NFC devices from accessing malicious content in NFC tags or Smart posters. In this approach, the solution proposed was an Android service component that would run in the background as soon as the device boots up. When a NFC interaction is initiated by the device, this component is invoked. The middleware consists of 4 major components:1. Activity controller 2. White List 3. Black List 4. Crowd soured website reputation ratings

Once a tag is read by the device, the activity controller identifies NDEF record to be a URL and thus checks it against the 3 lists. The white list consists of all the safe websites; the black list consists of the malicious websites. The crowd source website reputation ratings provide an aggregated rating of websites which are helpful in determining whether the website is trust worthy. Based on the response, the content is either displayed in the browser, or block if the content was found to be malicious. Upon implementation with 100K websites in white list and 166K black listed websites, the middleware was found to be working as expected in blocking the malicious websites from being accessed. It was also found that the middleware was able to achieve this with a very small latency. Thus, the solution was quite effective in providing security against malicious content in NFC tags and Smart posters. Although this solution was intended for detecting malicious content in NFC tags, it could be extended for providing protection in other NFC modes such as peer-peer mode and tag emulation mode. This could potentially prevent eavesdropping and identity theft attacks.

C)Protocol -Modification based solution:

Under this category we studied how some papers propose solution to overcome threats by making changes to the existing protocols. For privacy related attacks that can occur after successful passive eavesdropping as described in previous section, certain changes to the NFC-SEC key agreement protocol is suggested by the work [6]. Specifically, it looks at using conditional privacy protection mechanisms that have been applied in other domains for similar attacks. Pseudonyms, which can be regularly generated by a trusted third party can issued for the NFC device to use in transactions instead of just using the user's public key as per the traditional NFC-SEC protocol. Pseudonyms, anonymize the user's public key and since it is generated by the trusted third party, which issued the public keys in the first place, provide an elegant alternative for privacy protection. The downside of this approach turns out to be that pseudonyms (like a set of 1000) end up consuming significant storage space on the small capacity chips.

Another solution explores the modification of an existing RFID based protocol and extend it to the NFC domain. Using third-party authentication platforms for NFC security authentication results in high cost and high power consumption. To overcome this problem, a Security authentication algorithm entirely based on a Hash function was proposed which is independent and does not reply on third party [15]. The approach for the solution to the problem was to transplant an authentication algorithm in RFID, then applying it to the NFC field after a wide range of optimization and improvement. There were three modifications suggested to the existing IHLAP algorithm in order apply it to NFC field. Firstly, the initiating mechanism to reduce the system error rate and save the power consumption of initiating device. Secondly, removing some key data to save the storage resources and thirdly, Optimization of Redundant Key. After the implementing the modifications to the algorithm, after thorough analysis it was found that the efficiency was improved and transmission channel rate was reduced. The system was still able to provide the same level of security. This scheme was able to provide protection against tracking, impersonating, replaying attacks and other MITM attacks.

For Relay attacks, this work [13] explores a probabilistic modelling based approach to demonstrate the feasibility of relay attacks and what channel parameters needs to be adjusted. The authors use PRISM- a probability model checker. The authors define a model of the NFC systems and the various states as a CTMC. The parameters are configurable and consists mainly of the -timeout period during transport (MAX_RWT), adversarial channel strength (denoted as DR_RCH)- in terms how fast it can relay data between two victim devices, quality of the channel (PKT_ERR) and volume of the data involved. By tweaking these parameters and running simulations, the paper shows what values of the described parameters are feasible to successfully thwart a relay attack. Strong adversaries (DR_RCH > 3Mbps) have a higher probability of performing a successful relay attack, which is above 60% for MAX_RWT > 4.5 sec. Even weaker adversaries with slower relay channels (DR_RCH = 0:7; 1 Mbps) exhibit a very high probability of successfully launching the relay attack when MAX_RWT is high. Similar experiments with high volume of data is done and shows similar trend. Overall the paper tries to show the effectiveness of thwarting relay attacks with right configurations of the protocol parameters.

IV. Security in Alternative NFC solutions

As a part of this survey, we also studied some the alternative solutions that have been proposed for achieving NFC communication where the smartphone device may not have NFC enabling hardware. VINCE [11] is a solution that looks at exploiting visible light (400 THz to 790 THz) to perform communication. It encodes information as different light intensities and displays on the smartphone screen. The NFC reader comprises of an array of light sensors which decode the information. To achieve reliable communication, the distance between the two devices needs to be very short. Because light waves are unidirectional, the transmission is free from attacks such as eavesdropping. The paper lists low-data rate and unreliable transmission in the presence of ambient light as the challenges for this form of communication. The authors develop signal conditioners and empirically derived model to compensate the variation in received light samples. Received communication undergoes a CRC check and upon failure, asks for retransmission via feedback channel. Overall the solution seems feasible from security perspective, with no NFC hardware required, but obviously cannot support the tag emulation mode of NFC. Hence it would be incompatible with applications that use NFC tags and not deliver the user the full benefit of ease of use.

An alternative approach that we studied was the use of acoustics to perform NFC. This particular solution Dhwani [12] looked at leveraging the mobile phone's speakers and microphone to act as sender/receiver of the NFC communication and achieve data rates of 2.4 KBPS. The user equipment does not even have to be smartphone based. The authors first study the characteristics of an acoustic channel like frequency selectivity and the noise levels typically experienced in realistic settings. Based on this they design a Software defined acoustic OFDM radio. To ensure security in this mode of communication, the authors use an information theoretic based approach by adding noise to channel which only the receiver can cancel out. This receiver based jamming technique called- JamSecure, ensures that an eavesdropper on the channel only hears noise and is not able to get any useful information. The receiver uses a set training sequence on the channel apriori and record the responses in a library which it uses to perform self-interference cancellation. Dhwani proves to be an innovative solution for NFC in low cost mobile equipment and promising security from eavesdropping attacks. The only downside that we observed that Dhwani does only peer-to-peer communication and offers no potential for supporting tag-based NFC.

V. Comparison of the Security Measures

In this section we try to compare and contrast the different solution that we discussed previously. Some of the works propose hardware based solutions like- EnGarde and nShield. These depend to some extent on the energy from the mobile phone to sustain themselves, and needs to be attached to the back of the mobile phone. Compared to this software based solution like the lightweight middleware solution that thwarts tag based attacks appear more feasible since they achieve similar level of security as hardware ones. But the Lightweight Security Middleware provides protection against malicious tag content but not in other NFC modes. Overall it appears that the most solutions try to target at fixing vulnerabilities in one particular mode only, while leaving the system open to other possible attacks. The NFC SEC protocol underwent few changes after researchers demonstrated the possible vulnerabilities that can easily be taken advantage of to launch an attack. [9]

VI. Conclusions

Upon thorough analysis of vulnerabilities in the NFC devices, it was clear that the NFC interactions are not completely secure and thus various attacks such as eavesdropping, identity theft etc. could be possible. To provide protection against such attacks various solutions have been put forward. Solutions such as Authentication algorithm, Security middleware and M-coupon protocol were software based and EnGarde, nSheild etc. were hardware based. Upon through analysis of these solutions, we found that the attacks that were previously feasible on NFC interactions are currently no longer possible due the implementation of the solutions. So, we concluded that the proposed solutions were effective in preventing the attacks and were able to make the NFC interaction much more secure and efficient.

Acknowledgment

We would like to thank our Prof. Srikanth V Krishnamurthy, for all the guidance and comments that have led us to complete this paper. We value the feedback that we have received over the duration of the course and presentations.

References

[1] NFC forum technical specifications. http://www.nfc-forum.org/specs/spec list/.

[2] ECMA International (2008). NFC-SEC, White Paper. Available at: http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf

[3] Survey on Near Field Communication Vedat Coskun *, Busra Ozdenizci and Kerem Ok NFC Lab-Istanbul, Department of Information Technologies, ISIK University, Istanbul, Turkey

[4] Ruogu Zhou, Guoliang Xing, nShield:A Noninvasive NFC Security System for Mobile Devices. *In MobiSys 2014*

[5] J. J. Gummeson, B. Priyantha, D. Ganesan, D. Thrasher,and P. Zhang. Engarde: protecting the mobile phone from malicious NFC interactions. In MobiSys 2013.

[6] Hasoo Eun ,Hoonjung Lee ; Heekuck Oh Conditional Privacy Preserving Security Protocol for NFC Applications IEEE Transactions on Consumer Electronics (Volume:59 , Issue: 1)

[7] Roland, M.; Langer, J.; Scharinger, J. Practical Attack Scenarios on Secure Element-Enabled Mobile Devices. In Proceedings of the 4th International Workshop on Near Field Communication, Helsinki, Finland, 13 March 2012

[8] S. Clark. http://www.nfcworld.com/2012/02/09/313079/researcherhacks-google-wallet-pin-on-rooted-android-phone/Feb

[9] C. Miller. Exploring the NFC attack surface. Proceedings of Blackhat, 2012.

[10] NXP: PN532 user manual. http://www.nxp.com/documents/user_manual/141520.pdf.

[11] Jianwei Niu Fei Gu ; Ruogu Zhou ; Guoliang Xing ; Wei Xiang In IEEE INFOCOM 2015

[12] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan.Dhwani: Secure peer-to-peer acoustic NFC. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM,2013

[13] Nikolaos Alexiou ; Stylianos Basagiannis ; Sophia Petridou, Security Analysis of NFC Relay Attacks using Probabilistic Model Checking International Wireless Communications and Mobile Computing Conference (IWCMC) 2014

[14] Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, Waqas Khalid Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters. 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications

[15] Zai-Jiao Zhuang, Jin Zhang, Wei-Dong Geng Analysis and Optimization to an NFC Security.Authentication Algorithm Based on Hash Functions 2014 International Conference on Wireless Communication and Sensor Network