A Practical NFC Relay Attack on Mobile Devices Using Card Emulation Mode

D. Cavdar* and E.Tomur **
* Middle East Technical University, Ankara, Turkey
** İzmir Institute of Technology, Izmir, Turkey
dcavdar@metu.edu.tr, emrahtomur@iyte.edu.tr

Abstract - In this study, a practical card-emulated relay attack is implemented on Near Field Communication (NFC) equipped mobile devices. NFC is a promising communication technology which is also used in smart mobile devices. As an effective and flexible communication technology, NFC is frequently used in innovative solutions nowadays such as payments, access control etc. Because of the nature of these transactions, security is a critical issue that should be considered in system design and development phases. Although inherited from Radio Frequency Identification (RFID) technology, NFC security needs, requirements and solutions differ in terms of its usage areas and solutions. Based on these parameters, security precautions in communication layer of RFID technology do not prevent relay attacks occurred in the application layer NFC solutions. This study is conducted to prove relay attack practicability with using only mobile phones for relaying credentials instead of RFID based smart cards in an access control application. The Host Card Emulation (HCE) mode also eases relay attacks in NFC communication. The study explains the conceptual description of proposed relay attack, development and operating logic of mobile applications working based on card emulation mode and server software and also data communication basics between modules and web services descriptions.

***Keywords*- NFC, Relay Attack, Mobile, Card Emulation**

I. INTRODUCTION

Daily communication devices such as computers, mobile phones etc. have evolved in the last decades in terms of both size and functionality. Although they are small in size, they became very capable devices in terms of performing complex and critical processes. This state is defined as the third era of computing [1] and named "Ubiquitous Computing" or "Pervasive Computing". In this stage, standard computer perception changes both in appearance and logic.

In the last decade, the communication and life style of people have completely changed. People have started to use smart mobile devices for their daily routines such as mailing, dealing with documents, entertaining etc. As a result, production and sales of smart mobile devices, mobile operating systems, mobile marketing and mobile solutions have extremely increased. According to the research conducted by Collins, there are 7.3 billion mobile devices in the world which exceeds world population. These numbers also show the impacts of mobile ecosystem.

Near Field Communication (NFC) technology is one of the communication conveniences that emerge from mobility tendency and device interaction concept. The main function of NFC is to establish connection between two mobile devices or NFC tags and reader. Data exchange or access requests can be easily performed with this concept. NFC enabled smart mobile devices are used in daily applications and create smart solutions. For example; NFC technology is used for contactless payments which are also the most popular NFC applications, loyalty couponing, transport systems (bus, train etc.), data exchange, gaming, location based services and access control systems.

This paper has five sections: After introduction, Section 2 explains Near Field Communication basics and Section 3 includes literature review about the study. Relay attack is described in Section 4 and finally Section 5 concludes the paper with summary and possible future works of this study.

II. NEAR FIELD COMMUNICATION

With the invention of mobile phones, the intent was to enable making voice calls via wireless instead of using traditional wired phones. After Second Generation (2G) GSM technology, mobile phones have been equipped with not only to perform voice but also to send/receive text messages and also to have internet experience capabilities. In addition to standard cellular network connection over base stations, mobile devices have started to establish connection to other electronic devices for data exchange and interaction. The infrared technology was used in first wireless communication trials, then Bluetooth and Wi-Fi wireless technologies have been developed for connection between interactive mobile devices.

1) Basics of NFC

After the studies of hardware developments, Near Field Communication (NFC) technology was introduced in 2002 by Philips and Nokia [3]. In 2004, NFC Forum was established in order to foster cooperation and standardization by Nokia, Microsoft,

This study is supported by the Scientific and Technological Research Council of Turkey under 2211 program.

Sony, and Philips. In early 2010s, NFC Forum has started to introduce NFC standards such as: Logical Link Control Protocol (LLCP) Specification, NFC Data Exchange Format (NDEF) Specification and NFC Record Type Definition (RTD) Specification etc. Then, mobile device manufacturers have been influenced from these developments and started to produce smart NFC products which are NFC enabled mobile devices, tags and readers. Finally, NFC became a standardized short range, easy to use and set up, flexible and stable communication technology.

NFC provides short range (up to a few centimeters) wireless communication between two electronic devices. In order to establish communication, at least one active (energy provider) device should initiate communication process. NFC enabled mobile devices and NFC readers such as contactless payment readers are active devices, whereas NFC tags and NFC posters are passive devices.

NFC operates in 13.56 MHz High Frequency (HF) unlicensed frequency band that is available to all manufacturers with range of up to 4 cm. Data transfer rates of NFC are 106, 216 and up to 424 Kbps which is higher than RFID data transfer rates, however much lower than 3G and Wi-Fi rates. The reason of that is the main purpose of NFC operations is not transfer high volume data to destination.

2) Operating modes of NFC

NFC devices interact via three different modes according to application types and needs. This flexibility creates a customizable environment for developers and manufacturers.

a) Peer-to-Peer Mode

In Peer-to-Peer mode, two active NFC enabled mobile phones interact with each other in two directional data exchange paradigm. Firstly, one mobile device initiates communication set-up process using request-response mechanism, and other mobile device replies its response. The connection is established according to Logical Link Control Protocol Specification (LLCP) created by NFC Forum and data exchange is performed based on Simple NDEF Exchange Protocol (SNEP) protocol basics. The data, picture, URL exchange operations between two mobile devices use this mode of operation.

b) Reader/Writer Mode

Active mobile devices can both read and write passive NFC tags in Reader/Writer mode. Similar to RFID cards, NFC cards respond to requested data sent from initializer mobile device or write demanded data. Passive NFC tags are operated according to NDEF and RTD message format standards. Location based services, information tags or smart posters use this operation mode.

c) Card Emulation Mode

In this mode, two active NFC devices which are mobile device and reader are used. The mobile devices act as smart card based on ISO/IEC 14443 Type A, Type B and FeliCa standards in the application. When mobile phone gets close to reader, similar to RFID applications, reader initiates interaction and reaches mobile phone's NFC module and Secure Element if available. Payment and Access Control applications use this mode for granting access.

III. Related Work

The Near Field Communication (NFC) technology is relatively a new technology which is introduced within the current decade [4]. The first versions of related standards have been released in last five years by NFC Forum and ISO [5], also device manufacturers have started to develop more NFC devices after these developments.

After mobile payment systems have been launched especially after Google Wallet solution, the popularity of NFC has increased. As a result of this popularity, trials of practical attacks on mobile payments were conducted in research [6], [7] and [8]. These studies demonstrate the applicability of security problems in mobile payment domain.

The implementations of NFC relay attack examples were conducted successfully in [6] and [7]. A mobile application installed on mobile device is used in attack; however, no security precautions are discussed in the study [9]. In the studies [6], [8] and [10], ISO/14443 based RFID cards were exposed to relay attack and successfully relayed. As countermeasures, protocols of distance bounding and Frame Waiting Time were offered in [6] and [8], however, they cannot provide sufficient precautions for attacks.

In the ISO/14443 standard, Frame Waiting Time (FWT) is defined for standard smart card and reader communication. FWT variable defines maximum response time after the end of the reader's data. FWT is defined as $(256 \cdot 16/ fcarrier) \times 2^{FWI}$, where FWI is a value from 0 (FWT = 300 μs) to 14 (FWT = 5 s) with a default of 4 (FWT = 4.8 ms). The control of this variable was offered in the literature for avoiding relay attack in [6] and [8]. This variable can be modified by attacker or some additional readers may be placed between reader and card in order to overcome this variable. However, the main reason of its unsuitability is that mobile devices are used in the proposed model instead of smart cards and when a relay attack occurred, only NFC based mobile phones

communicate with each other. There is no timing limitation between two NFC based mobile phone communications, because two devices are active not like in the ISO/14443 based passive cards. This problem should be solved with application layer security methods.

Location based control is also offered as another countermeasure in the studies [8] and [11]. Distance-bounding protocols use FWT values for calculating round trip time and finally comment on requester's location. As it is mentioned, using FWT is not a suitable solution for avoiding relay attacks especially where NFC enabled mobile device are used. These studies also show the significance of this research, because, it proves relay attack practicability with using only mobile phones for relaying credentials instead of RFID based smart cards and any other intermediate devices.

IV. RELAY ATTACK

In addition to other security threats such as eavesdropping, data modifications etc. in the short range wireless communication, relay attacks are frequently used for performing interventions.

Attacker captures and forwards relayed message to proxy device and this device delivers the message as if the real owner in a typical scenario. Similar to relay attacks, man in the middle attacks also influence wireless medium, however, the method and also purpose of relay attacks have completely changed. These attacks are frequently used in ISO/IEC14443 based passive smart card communication environment. Since these cards are used in critical payment and access control systems, relay attacks in this environment result in important security threats. For example; in the research [7], ISO/IEC14443 based smart contactless credit card is successfully relayed over proxy devices. In this application, relay mobile phone records debit card data in reader mode and forwards this data to another phone via wireless communication such as Wi-Fi or Bluetooth. Proxy NFC based mobile devices send credentials to reader as the real owner in card emulation mode. If the reader cannot detect the fake sender, relay attack is completed successfully. This activity flow is illustrated in Fig. 1.

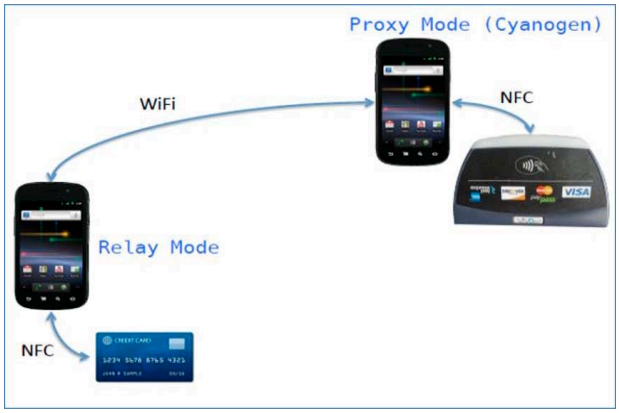

Figure 1. Typical Relay Attack scenario using contactless credit cards.

In the literature, NFC enabled mobile phones are generally used for relaying smart cards, in other words mobile phones read and send the data only. Credit cards, debit cards, and even electronic passports are used in relay attack experiences, however, in the access control systems proposal; mobile devices are used in card emulation mode instead of using smart cards. On the other hand, smart cards are limited and just reply the requested data

A. Host Card Emulation Mode (HCE)

NFC devices basically operate in three different implementation modes, Reader/Writer, Peer-to-Peer and Card Emulation mode. Although three modes are specified, developers could use only two of them, Reader/Writer and Peer-to-Peer in Android operating system because of Google policies. Only Google Wallet [12] application could use this operation mode for its transactions. With release of Android 4.4 (API Level 20), developers have started to use Host Card Emulation Mode [13] in their solutions and users have started to use their mobile phones like smart cards. We have also moved to that operation mode in our system because of its functionality and flexibility compared to its other modes.

The use of HCE in solutions also eases the practicability of relay attacks in the applications. Shifting between Reader and Card Emulation modes on same mobile device provides great chance to relay attackers instead of using different intermediate devices. HCE has also been used in practical relay attack scenario of the study.

B. Implementation

The relay attack setup in this study shows differences in transaction methods and relaying medium. As it is illustrated in Fig 3, the high level components of NFC based access control systems are NFC Enabled mobile device, NFC reader, access control panel and central server.

The general activity flow of NFC based access control system begins with controlling whether NFC unit of the mobile device is active or not. If NFC is enabled, user registers to the system with his/her mobile operator number, username etc. using application that is installed on the device. Once user is registered to the system, central server activates his/her account and sends activation key to authenticated mobile device. The activation key is checked based on predefined parameters. After registration process is completed successfully, user can now send access requests with his/her user name, password and expiration time of key parameters.

After getting key from the server using JSON based web services infrastructure, user can now send authentication requests to NFC reader with acquired key. At that time, relay phone can interfere NFC communication between reader and mobile phone. Relay phone can read the key that stored in the real mobile phone by getting close to phone in reader operation mode. In other words, relay phone imitates the NFC reader. If requester cannot identify the real

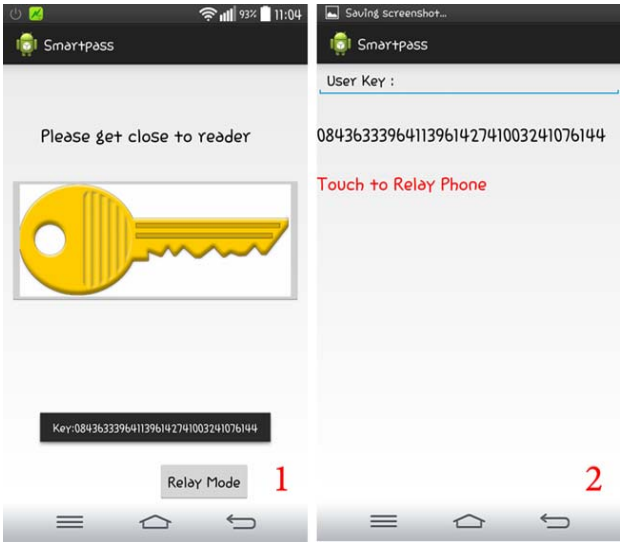

Figure 2. Screenshots of mobile application

NFC reader, relay phone gets the user key from real owner with operating peer-to-peer mode.

In order to complete the attack successively, relay phone should send access request to NFC reader with the key that captured from real phone. In order to do that, relay phone shifts its operating mode to Host Card Emulation Mode, by doing this; it now acts as a smart card and sends requests. These processes are illustrated in Figure 4. After these transactions, NFC reader gets the key and forwards to the server. Because of the validity of the key, unauthorized attempt can access to resource.

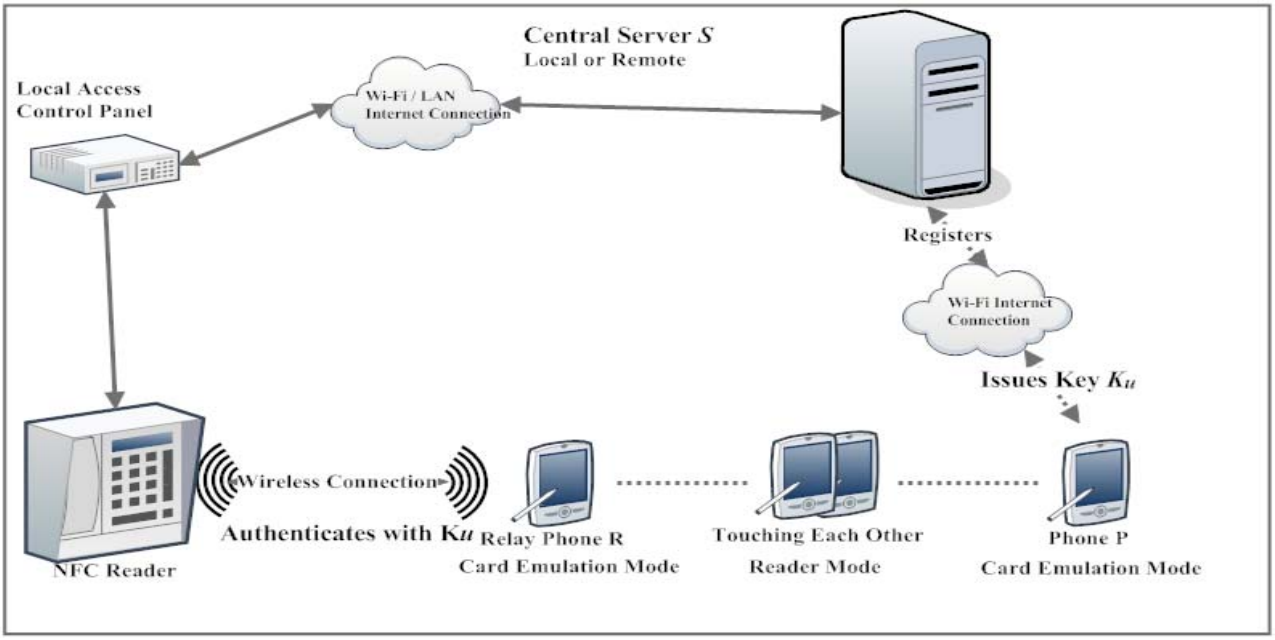

Figure 3. NFC Relay Attack scenario for access control system

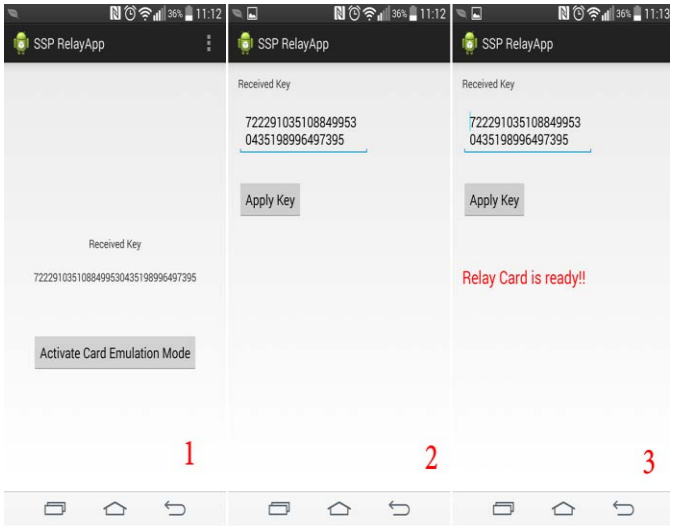

Figure 4. Screenshots of relay application

The whole process is illustrated in Figure 3. In the attack environment, relay phone has no wireless connection to server; therefore any key exchange occurred between server and relay phone. It captured the key from user mobile device using peer-to-peer operating mode and then changed its mode to card emulation mode. After this change, it created a virtual smart card using captured key from user device and requested access. NFC reader, access control panel and central server could not realize the relayed mobile device and attack is successively performed.

In a typical relay attack scenario which is also illustrated in the Figure 1, at least two mobile devices are used for relaying credentials. However, in this study, only one mobile device performs attack with the help of ability of switching operating modes of NFC. This is the main originality of the study. Also this convenience provides flexibility to attackers, because, in this kind of environments, attackers do not need to place between devices physically at the same time. Once he captures the credentials from real phone in reader mode, then he can use them another time after switching NFC mode to card emulation mode. Critical part of this type of relay attacks is whether relayed sender mobile device is detected or not by reader during authentication.

V. CONCLUSION & FUTURE WORK

Practical and successful relay attack scenario on mobile device using card emulation mode and its implementation steps are described in this study. NFC is a relatively new and popular wireless communication technology especially on mobile devices and used in critical solutions frequently. As well as its functionality, it is exposed to the relay attacks. Because of inheritance from RFID standards, the proposed precautions of communication layer such as defining FWI for transactions between receiver and transmitter do not prevent relay attacks in NFC environment. The study proves NFC communication security gap in access control systems using mobile devices. This type of relay attacks occur in the application layer, therefore, the real-time precautions that work on this layer and able to detect real sender should be developed for prevention as a future work.

REFERENCES

[1] Mark Weiser, “The computer for the 21st Century”. Scientific American. Vol. 265, No. 3, 1991, pp.66 -75.

[2] Romen, G. Presentation, 2010, NFC and the NFC Forum

[3] NFC forum, accessed from http://nfc-forum.org/ on January 2, 2014

[4] NFC forum, accessed from http://nfc-forum.org/our-work/specifications-and-application-documents/ on January 2, 2014

[5] NFC Forum. NFC data exchange format (NDEF). Technical specification, version 1.0. 2006

[6] Vounter van Dullink, Wouter, and Pieter Westein. "Remote relay attack on RFID access control systems using NFC enabled devices." 2013. unpublished.

[7] Hancke, Gerhard P. "A practical relay attack on ISO 14443 proximity cards." Technical report, University of Cambridge Computer Laboratory, 2005: 1-13.

[8] Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones," Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. To appear in The 2012 Workshop on RFID and IoT Security (RFIDsec 2012 Asia), November 8 - 9, 2012, Taipei, Taiwan

[9] Zhao Wang, Zhigang Xu, Wei Xin, and Zhong Chen. 2012. Implementation and Analysis of a Practical NFC Relay Attack Example. In Proceedings of the 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC '12).

[10] Master thesis, Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment Henning Siitonen Kortvedt, May 17, 2010 Der Technischen Universit At Munchen

[11] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. 2010. Practical NFC peer-to-peer relay attack using mobile phones. In Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues (RFIDSec'10

[12] Google Inc. accessed from https://www.google.com/wallet/ on January 15, 2015

[13] Google Inc. accessed from https://developer.android.com/ guide/topics/ connectivity/nfc/hce.html on January 15, 2015