UNIVERSITI PUTRA MALAYSIA

A RELAY ATTACK FOR HOST-BASED CARD EMULATION (HCE) USING NFC-ENABLED DEVICE FOR MOBILE PAYMENT

HAFIZAH BINTI CHE HASAN

FSKTM 2018 47

A RELAY ATTACK FOR HOST-BASED CARD EMULATION (HCE) USING NFC-ENABLED DEVICE FOR MOBILE PAYMENT

By:

HAFIZAH BINTI CHE HASAN

Thesis submitted to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in fulfillment of the requirements for the Master of Information Security

JUNE 2018

COPYRIGHT PAGE

DEDICATIONS

This thesis is dedicated to:

The sake of Allah, my Creator and my Master,

My messenger, Mohammed (May Allah bless and grant him), who taught us the purpose of life,

My great parents who never stop giving of themselves in countless ways,

My dearest husband, who remains willing to engage with the struggle, and ensuing discomfort,

My beloved family and friends, who encourage and support me…

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Information Security

A RELAY ATTACK FOR HOST-BASED CARD EMULATION (HCE) USING NFC-ENABLED DEVICE FOR MOBILE PAYMENT

By
HAFIZAH BINTI CHE HASAN
JUNE 2018

Supervisor: Assoc. Prof. Dr. Nor Fazlida Mohd Sani
Faculty: Faculty of Computer Science and Information Technology

Near field communication (NFC) is a family of radio frequency identification (RFID) that used wireless communication and it becomes more popular nowadays. It has been used in many different systems such as contactless payment processing, access control, passport identification, etc. With a card emulation mode, NFC technology is able to emulate the smartcard such as a credit card and save it in mobile phone. Therefore, the physical credit card is no longer needed in order to perform the electronic transaction. However, NFC is susceptible to some attacks such as data fabrication and eavesdropping. Thus, the mobile payment that used the NFC technology is also at risk. NFC is also particularly vulnerable to a relay attack. A relay attack is a type of Man-In-The-Middle attack that extends the range of NFC communication. It is therefore allows an attacker to interact with a Point of Sales (PoS) using the contactless card and perform electronic transaction without a user knowledge. Attacker starts an interaction with a card reader

(PoS terminal) and victim's device through an Internet or Bluetooth connection. One type of NFC approach, which is host card emulation (HCE) approach makes a relay attacks in NFC communication becomes easier, as it could interact with PoS directly without the need to interact with Secure Element (SE) as hardware on the device. One of the objectives of this research is to identify security problem of a relay attack for HCE approach in NFC-enabled device. Thus, a proof of concept has been built and tested in a lab environment to prove that a HCE approach is susceptible to the relay attack. The result from this research shows that HCE implementation approach is susceptible to relay attack. An overview of security issues in NFC communication, the relay attack process in detail, discussion of testing result, and some mitigation techniques towards the relay attack for HCE approach on NFC-enabled device are the elements that have been discussed in this project.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
Sebagai memenuhi keperluan untuk Ijazah Sarjana Keselamatan Maklumat

SERANGAN GEGANTI KE ATAS EMULASI KAD BERASASKAN HOS (HCE) MENGGUNAKAN PERANTI BERASASKAN NFC UNTUK PEMBAYARAN MUDAH ALIH

Oleh

HAFIZAH BINTI CHE HASAN
JUNE 2018

Penyelia: Prof. Madya Dr. Nor Fazlida Mohd Sani
Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Komunikasi bidang berhampiran (NFC) adalah sejenis teknologi daripada keluarga identiti frekuensi radio (RFID) yang menggunakan komunikasi tanpa wayar dan ia menjadi semakin popular pada masa kini. Ia telah digunakan dalam banyak sistem yang berbeza seperti pemprosesan pembayaran tanpa sentuh, kawalan akses, pengenalan pasport, dan sebagainya. Dengan mod emulasi kad, teknologi NFC dapat menyimpan data kad pintar seperti kad kredit di dalam telefon bimbit. Justeru, kad kredit fizikal tidak lagi diperlukan untuk melakukan transaksi elektronik. Walau bagaimanapun, NFC terdedah kepada beberapa serangan seperti fabrikasi data dan pendengaran tanpa keizinan. Oleh itu, pembayaran mudah alih yang menggunakan teknologi NFC adalah berisiko. NFC juga terdedah kepada serangan geganti. Serangan geganti adalah sejenis serangan orang tengah yang mampu memanjangkan julat komunikasi NFC. Oleh itu, ia membolehkan penyerang berinteraksi dengan pusat jualan (PoS) yang menggunakan kad tanpa sentuh dengan jarak yang lebih jauh dan melakukan transaksi elektronik tanpa pengetahuan pengguna. Penyerang memulakan interaksi dengan pembaca kad (terminal PoS) dan peranti mangsa melalui Internet atau sambungan Bluetooth. Satu jenis pendekatan NFC, yang dikenali sebagai pendekatan emulasi kad berasaskan hos (HCE) membuatkan serangan geganti dalam komunikasi NFC menjadi lebih mudah, kerana ia dapat berinteraksi dengan PoS secara langsung tanpa perlu berinteraksi dengan Elemen Selamat (SE) yang mana ia merupakan perkakasan pada peranti. Salah satu objektif penyelidikan ini adalah untuk mengenal pasti masalah keselamatan serangan geganti untuk pendekatan HCE dalam peranti NFC. Oleh itu, bukti konsep ini telah dibangunkan dan diuji dalam persekitaran makmal untuk membuktikan bahawa pendekatan HCE adalah terdedah kepada serangan geganti. Hasil daripada kajian ini menunjukkan bahawa pendekatan pelaksanaan HCE sememangnya terdedah kepada serangan geganti. Gambaran keseluruhan mengenai isu keselamatan dalam komunikasi NFC, perician proses serangan geganti, dan beberapa teknik yang boleh mengatasi serangan geganti ke atas pendekatan HCE pada peranti NFC adalah elemen-elemen yang telah dibincangkan di dalam projek ini.

ACKNOWLEDGEMENT

I feel grateful and thanks Allah SWT because of His bless and mercy. During this period, I am able to learn so many new things especially related to security in Information Technology. First of all, I would like to dedicate this appreciation to my beloved husband, En Ahmad Kamil Ismail, my parent Tuan Haji Che Hasan Jusoh and Puan Hajjah Siti Lina Daud, and also my mother in law, Puan Hajjah Faridah Abu Bakar who always give me endless moral support and encouragement. My appreciation also goes to my supervisor, Assoc. Prof. Dr. Nor Fazlida Mohd Sani who always patient in helping me and giving guidelines for improvements. I am very thankful towards his effort and sharing of knowledge to support me until the end of this project. Not to be forgotten, thanks to my fellow friends who are not tired of giving opinion and constructive comments that able to improve my project. May Allah bless all of you.

APPROVAL FORM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master Information Security. The members of the Supervisory Committee were as follows:

ASSOC. PROF. DR NOR FAZLIDA BT MOHD SANI
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)

Date: June 2018

DECLARATION FORM

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work
- Quotations, illustrations and citations have been duly referenced
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions
- Intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia (UPM)
- Written permission must be obtained from supervisor and Deputy Vice-Chancellor (Research and Innovation) before thesis is published in book form
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity was upheld as according to Rule 59 in Rules 2003 (Revision 2013-2014). The thesis has undergone plagiarism detection software

Signature: ________________________ Date: __________________

Name and Matric No.: HAFIZAH BINTI CHE HASAN (GS 47583)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

CHAPTER 1

INTRODUCTION

As for the introduction, this chapter will initially discussed the research background and highlight the problem statement. Apart from that, the research objectives, research scope and research schedule also has been provided in this chapter. Besides that, this chapter also has a brief description of thesis structure.

1.1 RESEARCH BACKGROUND

Wireless communications are well-established, and it's revolution offers multiple new business opportunities for companies across many industries. Radio Frequency Identification (RFID), bluetooth and Near Field Communication (NFC) are wireless standards and technology that been widely used today.

RFID is the wireless technology that commonly used for inventory tracking and supply chain applications. RFID tags can be read with a special handheld reader at a range of up to 100 meters. RFID typically only supports one-way communication.

Bluetooth has been designed specifically to replace data cables. Most bluetooth devices support two-way communication. Like RFID, these bluetooth devices can communicate within a range of about 10 meters. Nowadays, bluetooth is built into most mobile phones and many consumer electronics devices.

NFC is another wireless standard that performs functions similar to RFID and Bluetooth. Same as bluetooth technology, it is a short-range wireless communication technology that supports two-way communication between devices. When the two NFC are touched and matched, a peer-to-peer connection between these devices is established and both can send and receive information (ISO/IEC 14443 A&B, 2011; JIS-X 6319-4, 2005) (Cavallari, Adami, & Tornieri, 2015). However, for greater security and control, NFC works within a close range of a couple of inches. NFC is built into over 1 billion devices, including smartphone and tablets.

There are two (2) types of communication in NFC; passive and active. Active device has its own power source. It can act as either a reader or a tag, depends on how they are programmed. A passive device has no power source of its own, and it gain power via magnetic point from the reader while its been communicated. An example of passive device is a NFC chip embedded in a credit card which can be brought into the range of a credit card payment terminal. This payment terminal is an active device. Touching the credit card close into the payment terminal would activate the NFC inside the card, power it and begin a data exchange process between them.

However, the range of NFC communication is extremely limited. The combination of these 2 properties; a limitation of communication and the ability to communicate with a low power, makes NFC suitable for credit card communication. (Jensen, Gouda, & Qiu, 2016)

Since NFC supports two-way communication, it can allow contactless transactions (similar to contactless EMV cards) and other data exchange between electronic devices. In addition, NFC offers something that bluetooth does not: card emulation mode. It lets the NFC-enabled device act like a contactless smart card to make over-the-counter payments with just a tap, instead of cash or credit/debit cards. These NFC enabled devices have NFC controllers bonded on the motherboard. Then dedicated APIs will connected with NFC kiosks to provide NFC facilities as a reader and card emulator. (Urien, 2014)

A payments system in the world has been evolving for time to time, migrating from cash to a greater use of credit and debit cards. Although cash is still in use along with a bank accounts, Europay, MasterCard, and Visa (EMV) chip cards (credit and debit) and mobile payment are gaining more popularity as it is more convenient to use. Beside that, the security aspect for these payment methods are also being considered by the payment provider.

There are five primary models for mobile payments (International Telecommunication Union, 2013) are; 1) Mobile wallets, 2) Card-based payments, 3) Carrier billing, 4) Contactless payments using Near Field Communication (NFC), and 5) Direct transfers using bank accounts. This research will focus on type 4 of mobile payment model which is payment that uses NFC communication.

The mobile payment that uses NFC communication involves some parties including a mobile phone manufacturer, telecom operators, carriers, financiers, service providers, shops and trust services (Feng, Hwang, & Syu, 2016). Usually, user is required to provide a secure PIN or password in order to approve the transaction using this payment method (Ganapathi, Pramod, Rakesh, & R, 2012).

The function of the NFC is initiated by Google in Android 2.3. NFC-enabled devices can operate in three (3) different modes which are: reader/writer mode, peer-to-peer (P2P) mode and card emulation mode. (Basyari, Nasution, & Dirgantara, 2015).

In reader/writer mode, an NFC device comports as a reader for NFC tags. It detects a tag immediately in close proximity by using collision avoidance mechanism. Once the device and tag are connected, the NFC device can either read data from or write data to the detected tag. In this mode, NFC communication is established between two devices, one device acts as NFC reader/writer and the other one behaves as a passive NFC tag (Ganapathi et al., 2012).

In P2P mode, two NFC enabled devices can connect and exchange information between each other. P2P mode complies with ISO/IEC 18092 specifications to enable bidirectional data transfer (Alliance, 2014). By using this mode, the two NFC enabled device can perform some activities such as exchange photos, contact and also perform money transfer. In this mode, a device is in active states when sending data, and it switches into passive states when receiving a data. An example of technology that is using P2P mode is Android Beam technology.

In card emulation mode, an NFC device behaves like a contactless smart card and complies with ISO/IEC 14443 standard and FeliCa specification (Alliance, 2014). In this mode, a smartcard (e.g: credit card, debit card, transit card and access card) can be replicated by a separate chip on NFC device, called secure element smart card as depicted in Figure 1.1. This device then can connect to NFC reader which therefore enables contactless payment (Ganapathi et al., 2012). Many SIM cards that have been provided by the telecom operator have the secure element to devices that have NFC technology (Basyari et al., 2015).

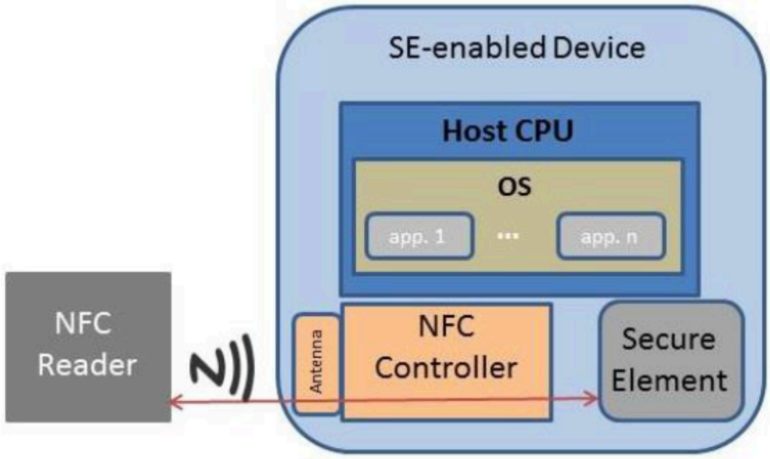

Figure 1.1: Card Emulation with secure element (Alattar & Achemlal, 2014)

Android OS 4.4 introduce Host-based Card Emulation (HCE) that replace card emulation with secure element mode. This mode allows a smart card to be emulated by android application and communicate directly with any NFC reader without going through the secure element as depicted in Figure 1.2 below. The data then will be forwarded to the host CPU directly (an android application need to be in running mode at this time), instead of routing the NFC protocol frames to a secure element (Basyari et al., 2015).

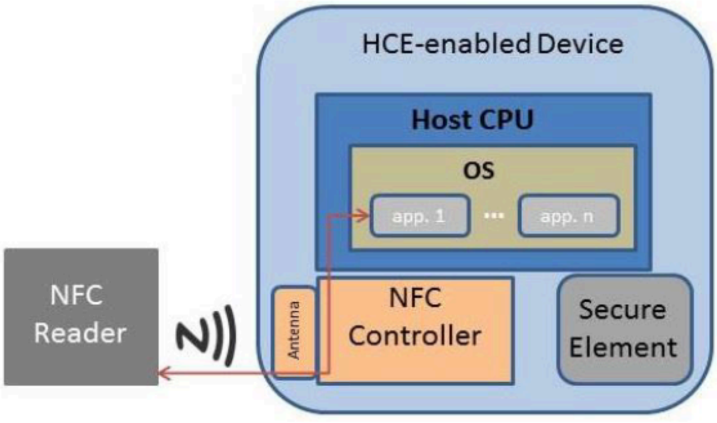

Figure 1.2: Host Card Emulation (Alattar & Achemlal, 2014)

The goal of HCE approach is to introduce a basic framework for simple card emulation that will increase end-user familiarity with NFC through additional services and also encourages new developers and service providers to roll-out new NFC services to the market (SimAlliance, 2014).

1.2 PROBLEM STATEMENT

This HCE technology still immature and might be vulnerable to security attacks. Besides eavesdropping and data fabrication attack, the NFC suffers for relay attack. Thus, the HCE is also at risk for these kind of attacks. Futhermore, a contactless credit card protocol that is used for mobile payment is also vulnerable to relay attacks. This attack aim to to perform unauthorised transaction. With the combination of these security risks in NFC and card protocol, its would provide the HCE implementation a higher risk in order to provide a secure payment.

1.3 RESEARCH OBJECTIVE

The purpose of this research is to identify security problem of a relay attack for HCE approach implementation in NFC-enabled device in providing secure mobile payment. A security testing will be conducted in this research to investigate the potential limitations of this approach. The research then will review a potential solution in order to mitigate the security problem in the HCE approach.

1.4 RESEARCH SCOPE & LIMITATION

This research focuses on relay attack as a security problem for mobile payment using HCE approach. In order to perform security testing, there is a security tool has been identified. However, as NFC is short-range wireless communication, this research require additional hardware to increase the range of communication. As the hardware is quite expensive, thus this research will only focus on software and application based attack.

1.5 THESIS STRUCTURE

The structure of this thesis consists of six chapters including Introduction, Literature Review, Research Methodology, Project Implementation, Result and Discussion and last chapter is Conclusion.

Chapter 1 is briefly explaining the introduction of background study of the related subject towards this project. Besides that, this chapter also consist problem statement, research objective, research scope & limitation research result expectation and thesis structure. Research objectives are derived from problem statement and expected to achieve at the end of this project.

Research scope and limitation highlight the scope of this project while research schedule is to ensure this project is on the right track according to schedule stated.

Chapter 2 is a list of literature review for this project. A literature review is a source of research article and journal that being used to give more understanding about related topic. This chapter is important as it is to ensure this project is possible to be done and to avoid any duplication of previous work (research gap). Besides, this chapter act as knowledge resource that helps to do improvement, tips, proof of concept based on previous research. This is able to help to increase the success rate for this project.

Chapter 3 explains a methodology that being used to develop this research project. A methodology is one of essential elements in every project as it will ensure the project is properly plans and can be executed smoothly. In this chapter also explained the framework that being used in this project.

Chapter 4 is a project development and implementation. In this chapter, the approach used is being explained in detail. Besides, the design and the functionalities of the approach also are highlighted. This chapter provides overall and process flow chart for this project. All the detail according to the implementation of the approach also can be found in this chapter.

Chapter 5 is a explaining the result. In this chapter, all the result and finding related to this project are explained that includes an evaluation of the result and the discussion.

Chapter 6 is the chapter of conclusion for this project. Besides, there is also suggestion for future enhancements that can be done. This chapter also concludes the whole project, result and the achievement while doing this project.

REFERENCES

Alattar, M., & Achemlal, M. (2014). Host-based card emulation: Development, security, and ecosystem impact analysis. *Proceedings - 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Security*, 506–509. https://doi.org/10.1109/HPCC.2014.85

Alliance, S. C. (2014). Host card emulation (HCE) 101. *A Smart Card Alliance Mobile and NFC Council White Paper.*, (August).

Basyari, R. S., Nasution, S. M., & Dirgantara, B. (2015). Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield. *ICCEREC 2015 - International Conference on Control, Electronics, Renewable Energy and Communications*, 160–165. https://doi.org/10.1109/ICCEREC.2015.7337036

Cavallari, M., Adami, L., & Tornieri, F. (2015). Organisational aspects and anatomy of an attack on NFC/HCE mobile payment systems. *ICEIS 2015 - 17th International Conference on Enterprise Information Systems, Proceedings*, *2*(Mi), 685–700. https://doi.org/10.5220/0005477506850700

Cavdar, D., & Tomur, E. (2015). A practical NFC relay attack on mobile devices using card emulation mode. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, (May), 1308–1312. https://doi.org/10.1109/MIPRO.2015.7160477

Chattha, N. A. (2014). NFC &amp;#x2014; Vulnerabilities and defense. *2014 Conference on Information Assurance and Cyber Security (CIACS)*, (1), 35–38. https://doi.org/10.1109/CIACS.2014.6861328

de Reuver, M., & Ondrus, J. (2017). When technological superiority is not enough: The struggle to impose the SIM card as the NFC Secure Element for mobile payment platforms. *Telecommunications Policy*, *41*(4), 253–262. https://doi.org/10.1016/j.telpol.2017.01.004

Feng, T., Hwang, M., & Syu, L. (2016). An Authentication Protocol for Lightweight NFC Mobile Sensors Payment, *27*(4), 723–732. https://doi.org/10.15388/Informatica.2016.108

Ganapathi, K., Pramod, B. K., Rakesh, C. M., & R, S. N. (2012). Near Field Communication – Applications and Performance Studies, 1–10.

International Telecommunication Union. (2013). The Mobile Money

Revolution. Part 1: NFC Mobile Payments. *ITU-T Technology Watch Report*, (May), 22. https://doi.org/1

Janssen, T. (2013). HCE security implications, analyzing the security aspects of HCE, 9.

Jensen, O., Gouda, M., & Qiu, L. (2016). A secure credit card protocol over NFC. *Proceedings of the 17th International Conference on Distributed Computing and Networking - ICDCN '16*, 1–9. https://doi.org/10.1145/2833312.2833319

Kayande, D., Rebello, E., Sharma, S., & Tandel, M. (2017). Overview of a payment solution for NFC-Enabled Mobile phones. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. https://doi.org/10.1109/ICTBIG.2016.7892685

Mayes, K. E., Markantonakis, K., Francis, L., & Hancke, G. (n.d.). 1 Introduction 2 Security Elements within the NFC Architecture, 1–7.

Merlo, A., Lorrai, L., & Verderame, L. (2016). Efficient Trusted Host-based Card Emulation on TEE-enabled Android Devices, 454–459.

Ozdenizci, B., Coskun, V., Ok, K., & Karlidere, T. (2015). A Secure Communication Model for HCE based NFC Services, (August), 19–22.

Pandy, S., Crowe, M., & Russell, B. (2016). Understanding the Role of Host Card Emulation in Mobile Wallets. *Federal Reserve Bank Of Boston*, 1–7.

Pannifer, A. S., Clark, D., & Birch, D. (2014). HCE and SIM Secure Element : It ′ s not black and white, 1–12.

Pasquet, M. (n.d.). Fraud on Host Card Emulation Architecture.

SimAlliance. (2014). Secure Element Deployment & Host Card Emulation, 1–13.

Street, N. G., Lafaye, W., Street, N. G., Lafaye, W., Street, N. G., Lafaye, W., … Lafaye, W. (2017). A Countermeasure against Relay A ack in NFC Payment. https://doi.org/10.1145/3018896.3025144

Umar, A., & Mayes, K. (2017). Trusted Execution Environment and Host Card Emulation. *Smart Cards, Tokens, Security and Applications*, 497–519. https://doi.org/10.1007/978-3-319-50500-8_18

Umar, A., Mayes, K., & Markantonakis, K. (2015). Performance variation in host-based card emulation compared to a hardware security element. *2015 1st Conference on Mobile and Secure Services, MOBISECSERV 2015*, (2). https://doi.org/10.1109/MOBISECSERV.2015.7072872

Urien, P. (2014). Cloud of secure elements: An infrastructure for the trust of mobile NFC services. *International Conference on Wireless and Mobile Computing, Networking and Communications*, 213–218. https://doi.org/10.1109/WiMOB.2014.6962173

Verderame, L. (2015). Trusted Host-based Card Emulation, 221–228.