Response_Time_Analysis_to_Support_Business_Process_of_the_NFC_Communication_in_Smartphone.pdf

WORD COUNT 2597
TIME SUBMITTED 30-MAR-2023 12:31AM
PAPER ID 98145257

Response Time Analysis to Support Business Process of the NFC Communication in Smartphone

[1]LN Harnaningrum, [2]Al Agus Subagyo
[1,2]STMIK AKAKOM, Jl. Raya Janti 143, Yogyakarta
ningrum@akakom.ac.id, alagus@akakom.ac.id

Keywords: NFC, mode, CE, mobile payment, smartphone.

Abstract: The development of wireless technology will reach the fifth generation (5G). If this condition occurs, then there will be many objects that can interconnect and exchange data. Embedded system is one area that will play many roles. One of them is the use of Near Field Communication (NFC). NFC is a short-range communication tool that has been used in many applications. NFC is one of the payment methods that will continue to be used by consumers. The development of this use must be accompanied by increasing trust. In practice, NFC has three modes: peer to peer, read / write and card emulation mode. In the state of card emulation mode, NFC mounted on a smartphone starts to bring up the Host Card Emulation which is launched on Android Kitkat 4.4. This condition allows the possibilies of interruptions or attacks. Then it needs to be examined the system that runs whether there is a gap or not. This study analyzed this with the response time parameters and the distance of the device. Card emulation conditions on NFC-enabled mobile with HCE show that communication can be done in combination with distance and the results show that distance does not affect response time. As long as it is still in the reader range, NFC-enabled mobile can still be read.

1 INTRODUCTION

NFC is a short-range electronic communication device. NFC can take the form of a tag card or be in a device, such as a smartphone. The development of smartphone utilization is increasing and for various purposes, encouraging the development of the use of facilities that are in smartphones as well. Utilization of NFC is developing for business, health, financial, social networking and others.

Emulation is one of the modes of NFC, usually called Card Emulation (CE). This mode uses ISO 1443 as a standard for the physical layer and the data link. An active NFC device operating in this mode appears on a remote external active device similar to a passive device. For example, a telephone that works in emulation mode can give itself as a contact or debit card. To make a payment, a user simply chooses a payment application, and brings the phone to a reader without contact. Therefore, we can design payment applications and tickets without contact on a mobile phone without changing the existing infrastructure.

CE mode is connected to the NFC controller of the device that is emulating. CE conditions are widely applied and used on NFC-enabled mobile devices. Mobile applications that use NFC as a means are mobile transaction applications. Typical CE applications, such as Google Wallet, involve the Graphical User Interface (GUI) application and the Java Card Applet. The user application runs on the Operating System (OS) device and is run by the main processing unit (ie CPU Host). In the Google Wallet example, the GUI application is used to enter a Personal Identification Number (PIN) code, to manage payments and to view transaction history. The Java Card applet is in SE and performs all NFC transactions. In addition, the SE is used to store sensitive information, such as credit card numbers or access tokens. SE communicates directly with the NFC reader interface via the NFC Controller. The NFC controller interacts with the NFC antenna and switches radio frequency communication to SE. Unit communications exchanged during a CE transaction on NFC are called Application Protocol Data Units (APDU) and are defined in the ISO / IEC standard. Although CE relies on SE for security-sensitive operations, several problems arise. SE has the same

978-1-7281-4519-4/19/$31.00 ©2019 IEEE

level of security as a contactless smartcard and consequently has the same disadvantages. The main problem is the existence of a relay attack. Relay attacks are Man-In-The-Middle exploits which extend the range of NFC communication, thus allowing attackers to interact with card readers, for example Merchant Point of Sales, using cards without contact from an unconscious user.

Host-based CE (hereinafter HCE) is a different approach to CE in smartphones that support NFC. HCE was introduced to be implemented in smartphones by Research In Motion (RIM) on the BlackBerry7 platform, followed by CyanogenMod8. Finally, in October 2013, Google included HCE on Android 4 KitKat. HCE is different from CE because SE is no longer involved in NFC transactions. The NFC controller directs the APDU directly to applications run by the CPU Host. As a result, developers must implement NFC transaction logic and smartcard emulation within the application itself, relying on the HCE low level API only. In addition, this application is also responsible for storing sensitive security data safely, such as access tokens. [1].

2 NFC IMPLEMENTATION ISSUES

The use of HCE facilitates the practicality of relay attacks in the application layer. The shift between Read and CE modes on the same smartphone device provides a great opportunity for attackers instead of using different intermediary devices. HCE has also been used in practical relay attack scenarios [2].
HCE relies on smartphone CPUs to process power and share power with other processes that are running. This results in a reading of the variable response time from the telephone. Response time variables were compared between HCE implementations compared with SE implementations. The findings are that there are significant variations in the timing of HCE implementation that can be questioned for their use in time critical applications, such as transportation tickets, and prevent the use of remote security measures to combat relay attacks. Significant variations in the average response time with the controlled CPU clock speed are also measured, then used to mimic the effect of loading. Continuation of these findings is how to consider additional smartphone platforms and SE, analysis of real world transportation performance and payment protocols [3].

Bayasin, et al [4] conducted a trial to get the response time for sending data with the APDU command. The result is a fairly fast response. The longest distance is 4 cm. This research can be developed for longer distance readings and tried with remote readers. This is to test the vulnerability of communication carried out by third parties. Meanwhile, Munch, et al [5] made an authentication test on HCE. The result is the validation time reduced from 1.2s to 0.2s. But it is necessary to enter the PIN twice. Need to find a way to overcome this. Pasquet, n.d. make a solution to two attacks and two solutions to protect the HCE Architecture. By using a token. Tokens are not very popular for smartphone users [6].

NFC communication for business transactions must be secure, because a high level of security will make users trust and use NFC more calmly. [7] created a secure protocol to deal with attacks. The proposed safe protocol does not accept transactions or the transaction will be terminated if it finds invalid certificates, inappropriate data and an interruption of attack. NFC is used as a means for student attendance transactions [8]. Students attend presence by using a camera and NFC to recognize attendance and record it to the system.
In addition to the issue of security protocols, things that need to be considered in NFC communication are NFC users' trust in anticollision. NFC can only be in an area that is strong enough of a similar signal. Thus, NFC can be read by an RFID reader, for example.
Research on NFC protocol authentication was conducted by [9]. The communication protocol is created on the NFC tag and NFC reader using four schemes. And as a result, this protocol can inhibit desynchronization. [10] use two anticollision protocols. The protocol is used to reduce collisions and identify tags efficiently. The results show better performance, which significantly reduces the communication delay and overhead for the tag reading process. Authentication is also done for the user. This protocol is used to overcome the problem of vulnerability and possible attackers [11].

3 MOBILE PAYMENT

Digital payments are growing and developing. Although long-distance e-commerce will probably still be the most widely paid payment, cellular payments have got a separate place and will continue

to increase over time. E-Wallet will also be an alternative payment that gets enough place from mobile payment users. Payments with E-Wallet are increasing. At the same time, with the increasing number of purchases made remotely, the loss of online payment fraud is increasing. As a result, cellular biometrics will gain popularity for providing extra protection against digital purchases. Payment using a debit card and credit card is also still a favorite payment system of customer choice. In the future, debit and credit cards will be increasingly used in smartphones with NFC facilities.

Smartcard for payment system and also for loyalty management, built customer loyalty [12]. Loyalty management design is made for two actors namely customer and seller. also benefited by being listed as a member of the seller.

Micropayment system is used to make payments and transactions become faster and more reliable, one of them is because the device is the customer's own and the security system has been guarded by encryption and inserting a pin. NFC technology is an easy and effective payment method. But users need high trust from service providers. The safety factor becomes a determining factor for users to decide to use NFC as a means of payment.

Transactions with NFC need to be secure and users can trust [13]. One of the security systems with NFC is to use the RTD-based transaction authentication method. With this authentication, the transaction can be trusted and there is no disruption because the transaction will not occur if there is no information about the RTD-based signature.

Studies on the future of payments by NFC have been carried out [14]. This study gives the result that NFC is a technology that will come for NFC payments. Although support from traders, including the provision of infrastructure, still needs to be fought for.

The m-Wallet comparison between Google and ISIS is done by [15]. This research shows that the two service providers are striving to create a solution for how to make cellular wallet payments immediately a method of payment everywhere. It still takes a long time and a long way to reach the expected scale, but Google and ISIS believe that with existing capabilities, this can be achieved.

4 ANALYSIS OF NFC COMMUNICATIONS

Smartcard is a part of smartphone, where a smartphone must have at least one smartcard reader. The communication protocol for smartcards (contact and contactless) is ISO7816. To communicate with the card, a reader can send an APDU command to the card, which will then be responded to with an APDU response. The APDU command is a byte array that has the structure shown in Figure 1. While the APDU response is shown in Figure 2.

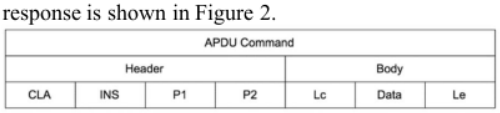

Figure 1. APDU Command Structure

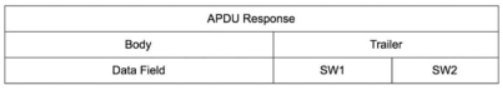

Figure 2. APDU Response Structure

When two smartphones communicate, there will be a command-response communication with the flow like Figure 3.

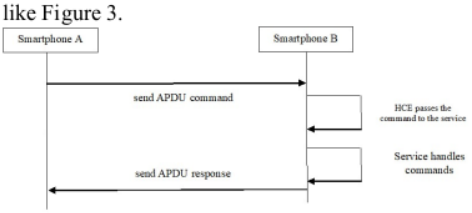

Figure 3. APDU command-response communication

An overview of the HCE and APDU systems will then be designed to be tested.

The trial of this study was conducted by calculating the response time of NFC enabled mobile to readings from the NFC reader. The experiments were carried out at different distances, namely 7 kinds of distances.

Table 1. Average Difference for Each Distance

Range	Response Time (ms)
0	106.000
1	108.273
2	104.900
3	110.000
4	110.000

5	106.200
6	111.000
7	105.818

The results of the difference in each distance (Table 1) shows the response time of NFC-enabled mobile when read by NFC reader. The farther the distance from the reader is not always directly proportional to the increase in response time. Even at the farthest distance, the fastest response time. This shows that the NFC reading is still going well as long as it is still within the reach of the reader. Zero distance test table, one and so on shows the distance with a difference of about 1 cm (0.5 cm error). While at a distance above the farthest distance NFC can not be read anymore. In this trial the command is performed to get the ID of the NFC-enabled mobile card.

5 CONCLUSIONS

The card emulation condition on NFC-enabled mobile with HCE shows that communication can be done in combination with distance and the results show that distance does not affect response time. As long as it is still in the reader range, NFC-enabled mobile can still be read.

REFERENCES

[1] Munch-Ellingsen, A, R. Karlsen, A. Andersen, and S. Akselsen, "*Two-factor authentication for android host card emulated contactless cards*," 2015 1st Conf. Mob. Secur. Serv. MOBISECSERV 2015, 2015.

[2] Cavdar, D and E. Tomur, "*A practical NFC relay attack on mobile devices using card emulation mode*," 2015 38th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2015 - Proc., no. May, pp. 1308–1312, 2015.

[3] Umar, *A*, Mayes, K, and K. Markantonakis, "*Performance variation in host-based card emulation compared to a hardware security element*," 2015 1st Conf. Mob. Secur. Serv. MOBISECSERV 2015, no. 2, 2015.

[4] Basyari, R.S, S. M. Nasution, and B. Dirgantara, "*Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield*," ICCEREC 2015 - Int. Conf. Control. Electron. Renew. Energy Commun., pp. 160–165, 2015.

[5] Pasquet, M, "*Fraud on Host Card Emulation Architecture*."

[6] Alattar, M and M. Achemlal, "*Host-based card emulation: Development, security, and ecosystem impact analysis,*" Proc. - 16th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2014, 11th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2014 6th Int. Symp. Cybersp. Saf. Secur., pp. 506–509, 2014.

[7] A. Asaduzzaman, S. Mazumder, and S. Salinas, "A Security-Aware Near Field Communication Architecture," *2017 Int. Conf. Networking, Syst. Secur.*, 2017.

[8] P. T. P. Subpratatsavee, W. Siriprom, and W. Sriboon, "Attendance System using NFC Technology and Embedded Camera Device on Mobile Phone," 2014, vol. 9, no. 3, pp. 227–229.

[9] K. Fan, P. Song, and Y. Yang, "ULMAP : Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G," vol. 2017, 2017.

[10] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tag-splitting: Adaptive collision arbitration protocols for RFID tag identification," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 6, pp. 763–775, 2007.

[11] V. Petrov, M. Komar, and Y. Koucheryavy, "A lightweight many-to-many authentication protocol for near field communications," *Proc. - Int. Conf. Netw. Protoc. ICNP*, 2013.

[12] F. Ferdianti, Y. Triyuswoyo, and D. A. R, "Utilization of Near Field Communication Technology for Loyalty Management," vol. 11, no. 3, pp. 617–624, 2013.

[13] S. Park and I. Lee, "Transaction Authentication Scheme based on Enhanced Signature RTD for NFC Payment Service Environments," *2016 Int. Conf. Platf. Technol. Serv.*, pp. 1–4, 2016.

[14] J. Ondrus and Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems An Assessment of NFC for Future Mobile Payment Systems," no. May 2014, 2007.

[15] J. Hedman, "Business Models for NFC based mobile payments," no. January, 2015.

Response_Time_Analysis_to_Support_Business_Process_of...

ORIGINALITY REPORT

16%
SIMILARITY INDEX

PRIMARY SOURCES

1	Armando, Alessandro, Alessio Merlo, and Luca Verderame. "Trusted host-based card emulation", 2015 International Conference on High Performance Computing & Simulation (HPCS), 2015. Crossref	189 words — 9%
2	ebin.pub Internet	34 words — 2%
3	Umar, Assad, Keith Mayes, and Konstantinos Markantonakis. "Performance variation in host-based card emulation compared to a hardware security element", 2015 First Conference on Mobile and Secure Services (MOBISECSERV), 2015. Crossref	32 words — 1%
4	D. Cavdar, E. Tomur. "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 Crossref	29 words — 1%
5	Jihoon Myung, Wonjun Lee, Jaideep Srivastava, Timothy K. Shih. "Tag-Splitting: Adaptive Collision Arbitration Protocols for RFID Tag Identification", IEEE Transactions on Parallel and Distributed Systems, 2007 Crossref	15 words — 1%

6	www.researchgate.net Internet	13 words — 1%
7	ufdcimages.uflib.ufl.edu Internet	12 words — 1%
8	www.semanticscholar.org Internet	12 words — 1%
9	core.ac.uk Internet	10 words — < 1%
10	Iakovos Gurulian, Konstantinos Markantonakis, Eibe Frank, Raja Naeem Akram. "Good Vibrations: Artificial Ambience-Based Relay Attack Detection", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018 Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF