An NFC Relay Attack with Off-the-shelf Hardware and Software

Thomas Bocek, Christian Killer, Christos Tsiaras, Burkhard Stiller

An NFC Relay Attack with Off-the-shelf Hardware and Software

Thomas Bocek, Christian Killer, Christos Tsiaras, Burkhard Stiller

University of Zürich UZH, Communication Systems Group CSG
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
Email: tsiaras|bocek|stiller@ifi.uzh.ch, christian.killer@uzh.ch

Abstract Passive Near Field Communication (NFC) devices, such as contactless smart cards, use NFC to communicate with other devices without any physical connection or an internal battery source, deriving power inductively via the radio field generated by the NFC reader device. Today, many Point-of-Sale (PoS) terminals, credit cards, and also mobile devices are NFC-capable and facilitate contactless payments. Although the communication range is typically limited to a few centimeters, NFC attacks exist that exploit such contactless communication channels.
This paper focuses on NFC relay attacks and shows that a practical relay attack on public transport PoS terminals, using off-the-shelf mobile devices and hardware, is feasible. Finally, countermeasures are discussed with the main finding that currently the best countermeasure against relay attacks is to physically shield an NFC device.

Keywords: NFC, Relay Attacks, Countermeasures, Credit Card

1 Introduction

Near Field Communication (NFC) technology is defined as a standardized wireless communication technology, which operates in the High Frequency (HF) band at 13,56 MHz. NFC devices do not necessarily need a battery in place to operate. Passive NFC devices, such as contactless smart cards, can operate deriving power inductively from the magnetic field generated by the NFC reader.

Europay, Mastercard, and Visa (EMV), is a protocol for smart card payments around the world [4]. The Point-of-Sales (PoS) exchanges EMV protocol messages with the chip on the smart card, while selected data is secured with a cryptographic Message Authentication Code (MAC) using symmetric encryption in the online mode, and asymmetric encryption in the offline mode (without access to a network). In the online mode, the key is known to the card issuer, so the identity of the card can be verified. Originally, EMV was designed to fight against the threat of magnetic stripe card fraud and the effort to establish a worldwide standard for chip-based payment-cards and PoS. While the deployment of EMV progressed, and the use of chip-based transactions increased, fraud incidents including magnetic stripe card fraud decreased. However, fraudulent card-not

present transactions (especially card transactions over the Internet, phone, or fax) increased as well [24,26]. The widespread distribution of EMV-compliant payment-cards, immediately raised the question if security issues have to be further investigated. Prior research showed that the EMV protocol has major vulnerabilities that can be exploited [11,23,22]. Today, new PoS terminals, credit cards, and mobile devices are NFC-capable and designed according to the EMV contactless standard. Thus, many security sensitive applications, such as payment applications and electronic passports, already use contactless technologies [25].

One type of attack with NFC and Radio-frequency Identification (RFID) is the relay attack. This type of attacks in RFID communications is known for years, but still EMV-compliant PoS terminals are at least partially vulnerable. With relay attacks, the physical presence of the credit card near a PoS is not necessary anymore. This could disrupt security and privacy assumptions, mainly due to the fact that most of these contactless smart cards are based on the International Organisation for Standardization (ISO)/International Electronical Commission (IEC) 14443 standard and are intended to operate only over a distance of around 10 cm. With a relay attack, the distance assumption of 10 cm does not hold anymore. As an example, a credit card can be physically in the US, while in Germany, with relaying, this card can be used to pay for a public transport ticket using a contactless PoS terminal. Furthermore, in some countries, small amounts can be charged from the credit card via NFC without any user intervention or credential usage.

This paper shows the feasibility and proof-of-concept of relay attacks with off-the-shelf software and hardware by implementing a practical relay attack on EMV-compliant PoS machines for public transportation. It shows that its still feasible to exploit this known vulnerability. Furthermore, a discussion follows about countermeasures and its effectiveness.

The remainder of this paper is structured as follows. Related work is discussed in Section 2, followed by a generic NFC relay attack architecture in Section 3. While Section 4 presents technical details about the implementation of this work, Section 5 proposes possible countermeasures to prevent NFC relay attacks. Finally, Section 6 summarizes this paper and draws conclusions.

2 Related Work

Various EMV protocol attacks have been reported in the literature. After an overview over the EMV authentication methods, downgrading, yes-card, wedging, pre-replay, and relay attacks are presented in the following.

There are three different authentication methods for EMV cards, Static Data Authentication (SDA), Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA) [3]. Weaknesses have been found for all these card authentication methods. Cards using SDA are vulnerable to the “yes-card” attack, where an attacker can copy the static data. Then, the attacker can use the copied card to conduct valid, statically signed transactions. As a result, DDA improved this by signing dynamic data with a card-unique asymmetric Rivest, Shamir and

Adleman (RSA) key. CDA combines DDA, the signing of changing transaction data, with the use of an application cryptogram (AC) generated by the card.

All these authentication methods improve the security of contactless transactions. There are three main Cardholder Verification Methods (CVM) which are supported by EMV. There is an online and offline Personal Identification Number (PIN) verification, or the use of signatures (which is used for magnetic-stripe cards). Usually, for low amount transactions, no additional CVM is used. Prior research showed that the payment terminal itself can be forced to fall back to old Cardholder Verification methods (CVM), such as downgrading a full EMV credit card to perform an EMV magnetic-stripe transaction [26]. If such an attack is possible, all of the new authentication methods are rendered useless.

Another critical issue concerning EMV is the EMV PIN verification "wedge" vulnerability. This vulnerability allows an attacker to use stolen cards without knowing the correct PIN. To do so, the attacker uses a man-in-the-middle attack, where the stolen card will accept any PIN entered, for both offline and online transactions [23].

Prior research presented a proof-of-concept for the so-called Pre-Replay attack [11]. An attacker can use a tampered terminal to collect card details. Later on, the attacker can replay the data collected at a terminal of the same type that data were harvested on. The collected card details include the PIN and an Authorization Request Cryptogram (ARQC). These ARQCs are responses from the card, when presented with an Unpredictable Number (UN) by the PoS terminal. The flaw is that some PoS terminals generate predictable numbers instead of a random number. The protocol design flaw is that the terminal generates the number and the issuer relies on its random generation. Thus, for this attack to succeed, the attacker must compromise the terminal equipment and then harvest ARQCs, to be able to carry out indistinguishable transactions to the issuer.

Relay attacks on ISO/IEC 14443 Type A-based smartcards are introduced in [18] and [16]. The Radio Frequency (RF) communication was relayed up to a distance of 50 m. This work illustrates how the attacker can use commercially available tools. Moreover, it highlights the potential security implications for current contactless applications. Practical and generic relay attacks were implemented, only using two NFC-enabled mobile phones and software applications. It has been shown that many EMV-compliant systems still seem to be vulnerable [13,14]. Previous work has also shown that an extension of the classic relay attack is possible [20]. Such an extension could mean an increase of the distance between the reader device and the genuine card. The additional distance varies between 40 cm to 50 cm and the extra cost is less than 100 $. More precisely, a potential attacker could discreetly access a foreign card from about 50 cm far away. This is a fivefold increase in distance compared to the distance of a ISO 14443 contactless smart card transaction. Additionally, EMV transactions have a common structure. Thus, if a transaction is recorded and the static and redundant data, which is the same for every transaction, are omitted in the relayed communication, a relay attack transaction can be optimized.

Besides mobile payment, relay attacks in other scenarios, such as ticketing systems, have been successfully demonstrated as well as reported in [15].

This paper shows that while the relay attack vulnerability is well known and has been reported in many papers and articles before, its still exploitable as of today with off-the-shelf hard and software.

3 Background and Architecture

The relay attack presented in this paper applies to ISO/IEC 14443 smart cards of operation mode type A. These smart cards are passive and the inductively coupled RFID transponders have a transceiving range of up to 10 cm. The reading device is called Proximity Coupling Device (PCD) and the card is referred to as Proximity Integrated Circuit Card (PICC). In a typical usage scenario, the PICC interacts directly with a PCD.

For a relay attack, further devices are necessary. In addition, as shown in Figure 1, two NFC devices (tablets) and at least one IEEE 802.11 wireless network (Wifi) are used. This enlarges the transceiving range up to the Wifi range to about 100 m. For larger ranges two Wifi devices connected to the Internet are required as shown in Figure 2. In both cases, one NFC device is in a proxy mode that will relay the NFC traffic from the PCD (PoS) via Wifi and back, the other NFC devices is in relay mode that will relay the NFC traffic from Wifi to the PICC (credit card) and back. The Wifi network establishes a tunnel for the traffic between the two NFC devices in proxy mode respectively in relay mode. An attacker needs to place one NFC device on the contactless payment terminal, while placing the other NFC device close to the victim's NFC credit-card.

In consequence, the physical presence of the PICC is no longer required. This work here assumes that the delay occurring is below 1.5 s and, therefore, the attack is possible [11].

3.1 EMV Contactless Transaction

EMV Contactless [4] is the standard for contactless PICCs. The contact chips, for both contact and contactless PICCs, are usually based on the ISO/IEC 7816 standard and the "contactless integrated circuit" is designed according to ISO/IEC 14443.

Comparing ISO/IEC 7816 and ISO/IEC 14443 to the Open Systems Interconnection model (OSI model), in contact based systems, the ISO/IEC 7816-3 [8] standard specifies layer 1 (Physical), 2 (Data link), and 4 (Transport). In contactless systems, these three layers are specified in ISO/IEC 14443-2 [5], ISO/IEC 14443-3 [6], and ISO/IEC 14443-4 [7]. Even though the contact and contactless standards differ in various aspects (*e.g.* transport protocols, anti-collision, activation, bit transfer and power supply), the communication protocol as on OSI layer 7 (Application) is the same as specified in ISO/IEC 7816-4 [9] for contact based systems. Further, the transaction protocol supports the use of so-called Application Protocol Data Units (APDU).

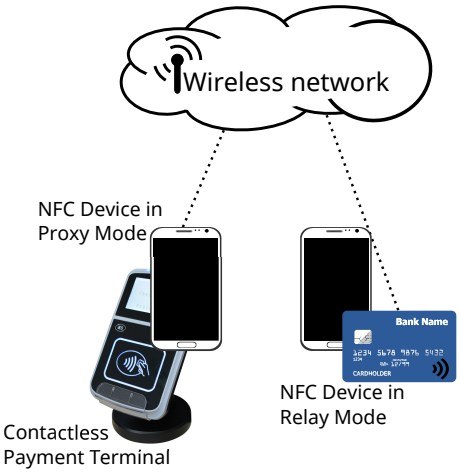

Figure 1. Setup 1: Simple Relay Attack Setup

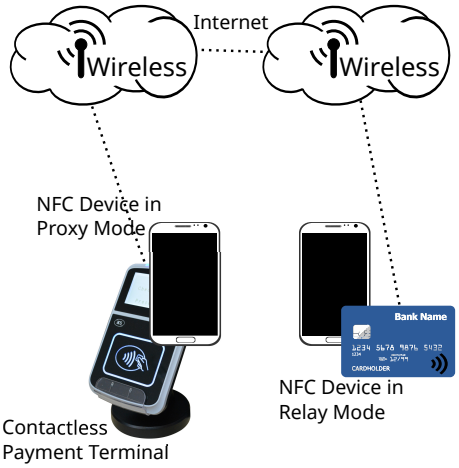

Figure 2. Setup 2: Internet Relay Attack Setup

Before the APDU-based protocol can be started, PCD and PICC need to have the same configuration. First of all, the PCD polls for new PICCs by sending out a REQA. After that, PICCs that have not been activated yet, synchronously answer with their Answer-to-Request (ATQA). The PCD is now notified that a new PICC is available and, therefore, initiates the anti-collision procedure by starting a binary search tree algorithm and enumerating all PICCs based on their Unique Identifier (UID). If the anti-collision was successful, these PICCs send a Select Acknowledge (SAK), which indicates whether the card supports the standard data transmission of ISO/IEC 14443-4 or not. If supported, the PCD sends a request to answer the select (RATS) as a command and expects an answer to reset (ATS) as a response. The RATS contains parameters, such as the frame size the PCD can receive. In return, the ATS contains information about the chip's operating system. Now the PCD and PICC reached the same configuration. Hence, from there on the communication between PCD and PICC is always conducted in the form of APDU command-response pairs.

3.2 Visa Smart Debit/Credit (qVSDC) Protocol

Visa's payWave transactions are using the quick Visa Smart Debit/Credit (qVSDC) protocol as shown in Figure 3, which is slightly more compressed than the MasterCard PayPass protocol. The main difference between the two protocols is that Visa transactions omit using the GENERATE AC command. The functionality is brought together in the GET PROCESSING OPTIONS (GPO) (message #5 in Figure 3) request, because the card will respond to the GPO by calculating the Application Cryptogram (AC) and sign the data in the next response (message #6 in Figure 3). The different steps in a Visa contactless transaction can be divided into 8 steps [13].

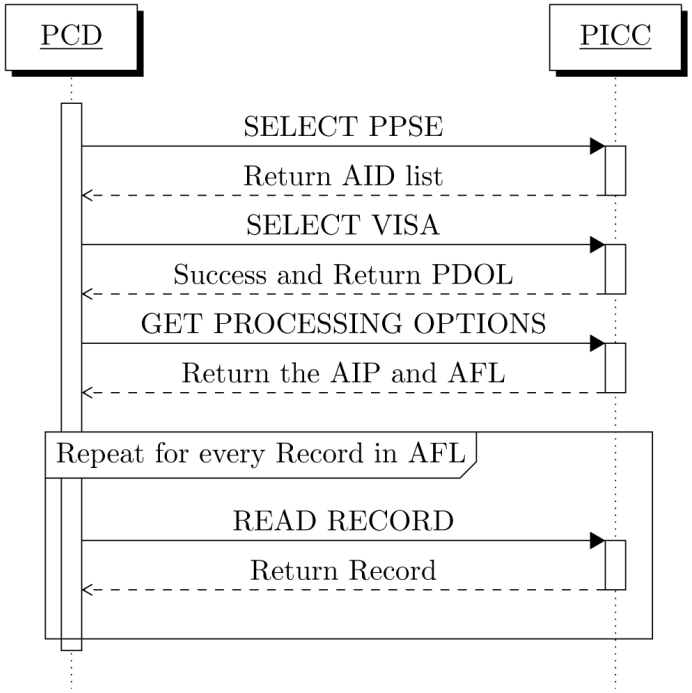

Figure 3. EMV Contactless Transaction Sequence Diagram.

1st Message PCD → PICC: Command: `SELECT PPSE`
The PCD selects the Proximity Payment System Environment (PPSE).

2nd Message PICC → PCD: The PICC responds with the file control information template (FCI) which is list of the supported EMV applications, so-called Application Identifiers (AID) also combined with a priority indicator for every AID.

3rd Message PCD → PICC: Command: `SELECT VISA`
The PCD then selects the AID with the highest priority which it is supporting.

4th Message PICC → PCD: The PICC responds if the application was selected successfully. The response also contains the File Control Information (FCI) template with application details, such as the Processing Options Data Object List (PDOL) with all those fields (*e.g.* Amount, Terminal Country Code, Terminal verification Results, Transaction Date/Type and the Unpredictable Number) needed by the PCD for the next step.

5th Message PCD → PICC: Command: `GET PROCESSING OPTIONS`
Following the application selection, the PCD requests processing options. In essence, the PCD responds with the PDOL related data encoded according to the PICC's previous PDOL received in the 4th message.

6th Message PICC → PCD: The card responds with the Application Interchange Profile (AIP) and Application File Locator (AFL). The AFL is used by the terminal to read the data records from the PICC. These records contain a variety of information, such as the Primary Account Number (PAN), the expiry date, and more (except for the Card Verification Value (CCV)). The AFL also indicates, if any of the data will be provided for the Authentication Process. As a result, the card is in control, which files can be read.

7th Message PCD → PICC: Command: READ RECORD
The PCD requests the records according to the AFL and the PICC follows these requests with the according responses. Which data is being read exactly depends on how the issuer configure the card.

8th Message PICC → PCD: The PICC returns the records requested.

4 Implementation

For this work here, the NFCProxy [10] was selected to carry out the relay attack. The hardware requirements - as discussed above - are 2 NFC devices and one or more Wifi devices. Two commercially available off-the-shelf NFC-enabled mobile tablets were used. The NFCProxy requires a certain versions (9.1 and 10.1) of CyanogenMod [1]. The installation of those versions is mandatory, because the NFCProxy requires certain features for handling Host Card Emulation (HCE), which was removed in some Android versions. However, on never devices, these relay attacks work without installing a custom ROM [27]. To install CyanogenMod on a mobile device, the device needs to be rooted and unlocked. Furthermore, these HCE extensions require the NXP PN544 NFC Controller, which is used on many commercially available devices. To carry out the relay attack, the setup as shown in Figure 1 with a portable IEEE 802.11 b/g/n wireless router was used, which was powered on with a mobile power source.

4.1 Hardware/Software Specification

The following hardware and software was used to carry out the relay attack.

- 2 Tablets; brand/model: ASUS Nexus 7v1, CyanogenMod 10.1 operating system
- Wireless Router; brand/model: Alfa Network Hornet-UB, chip set: Atheros AR9331 SoC, 2.4 GHz, 802.11 b/g/n
- Credit-Card; brand: VISA, model: Visa Card Classic, payWave limit: 40 CHF
- NFCProxy [10], version 0.1.2

4.2 Relay Attack Proof-of-Concept

The relay attack implementation was tested as described in [12] at two different public transport PoS terminals that were capable of handling contactless transactions. The attacker placed one Android device (proxy mode) on the PoS terminal

and the other Android device (relay mode) next to an NFC credit card of the victim. Two relay attacks at two different terminals were video recorded and can be seen in a proof of concept (PoC) video as shown in Figure 4. Note that for this attack purely the feasibility of the attack was targeted at, as the only purpose was to show and indicate vulnerabilities. At no times at all the public transportation authority was faced with fraud or any misuse of services obtained.

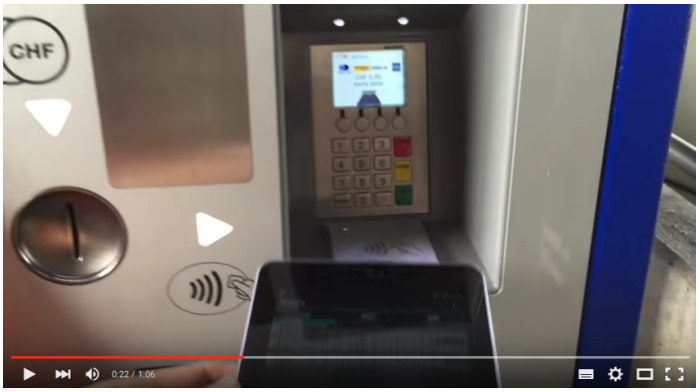

Figure 4. Proof-of-Concept [21]

4.3 Protocol Details

The Visa payWave logs that were recorded during the PoC implementation follow the protocol as described is Section 3. As a card authentication method, the offline CDA was used, following the Visa payWave Contactless EMV standards. In general, CDA verifies the card by generating an RSA signature on individual transaction data and additionally verifying using an AC generated by the card. For this reason, the message #5 as above also included an Unpredictable Number (UN). The card is expected to return a Signed Dynamic Application Data (SDAD) and an application cryptogram in message #6. SDAD is a dynamic signature generated by the card and validated by the reader during fast Dynamic Data Authentication (fDDA) processing. As the name implies, fDDA is faster than the standard DDA due to the fact that it utilizes a pre-defined list of data elements for authentication.

As indicated in Figure 3, messages #7 and #8 are repeated for every record in the AFL. Therefore, the PCD starts to read data records (message #7) from the PICC. The first response (message #8) contains an Issuer Public Key Certificate (IPK), which is certified by a Certification Authority (CA). Further, the response contains more data, such as the Certification authority public key index (to identify the CA public key) and also an Issuer Public Key Exponent, which is used for verification of the SDAD and the IPK. In return, the PCD requests

another data record with the message #7. In the second response of the card (message #8), the PAN, the expiration date, the issuer code, and the ICC Public Key Certificate is returned. If everything was accepted by the POS terminal, the transaction was successful.

Although, a successful relay attack was carried out on public transport PoS terminals, no fraudulent transactions were issued. At any point in time, equipment and credit cards were used belonging to a single person. All purchased tickets over the NFC relay were paid in full by the authors.

5 Countermeasures

To carry out this relay attack as presented above, an attacker does not have to decrypt any of the data, thus, there is no formal breaking of keying material or credentials involved. Hence, providing sufficient protection against such relay attacks is difficult, because the attack cannot be prevented by application-level cryptography [17]. Therefore, to supplement existing security mechanisms, additional countermeasures are required. These countermeasures have to focus according to today's knowledge on the essential and key aspects of the relay attack: (1) the added time delay and (2) any unnoticed access to the card [18].

Countermeasures can be classified into two key categories: either (1) the card is protected or (2) the system itself is [20]. The most simple, effective, and cost-efficient form to protect the card is to shield the chip (*e.g.,* wrapping card in metal foil) and, thus, prevent almost certainly any unwanted remote activation. Additionally, the following selection of further possible countermeasure include (a) additional verifications, (b) time measurements, and (c) distance bounding.

5.1 Additional Verification

Relay attacks could be prevented by introducing secondary authentication procedures (*e.g.,* password or biometrics). However, such additional verification countermeasures demand additional (typically unwanted - due to practicality reasons) user-interactions, which eliminates the convenience emerging from the use of the contactless smart cards. Another drawback that could arise is the resulting increase in transaction time, which might not be acceptable in every application anymore. Recent approaches in combining credit card and smartphone with NFC introducing an additional secure elemement could solve the problem *e.g.,* by asking the user on the smartphone if a transaction should be carried out. Once a vendor is known with a previously approved transaction, further transcation with this vendor could be carried out again without any user interaction. Thus, making the relay attack much more difficult, without loosing the convenience and keeping the transaction times low.

5.2 Time Measurement

A valid and genuine contactless transaction has a certain time duration, depending on the specific PICC and PCD setup. Typically, relaying this communication

results in a delayed transaction and, therefore, takes more time. Because these POS terminals would need to serve a variety [11] of contactless cards, setting a time limit could easily lead to valid transactions being rejected (false positive).

Theoretically, if an accurate response time is recorded for every PICC and PCD combination, it would be possible to implement a maximum time duration for a transaction as presented in this work [28]. The implementation of such a time measurement challenge-response protocol makes a relay attacks more difficult, but wold not be able to prevent them in full [26].

In contrary, prior research also concluded that the time variance observed on dynamic messages between various cards was even larger than the overhead by the relay [14]. Thus, simply using an overall time limit on static or dynamic data authentication (*e.g.,* using the GENERATE AC message response in MasterCard PayPass or the GET PROCESSING OPTIONS message response in Visas PayWave) cannot be used as an efficient countermeasure against relay attacks due to different chips on cards, resulting in very different processing time.

The relay attacks in the PoC video [21] lasted between 671 ms and 2050 ms and those were accepted either way. Yet, the EMV Contactless standard allows for up to 500 ms of total time per transaction (*e.g.,* for Visa [2]). Prior research could also observe an equal behavior [14]. Transactions would be accepted even though the transaction took longer than 500 ms. Therefore, when performing a relay attack, the genuine card could be anywhere in the world and timing constraints are not sufficient on their own to provide a suitable protection against relay attacks.

5.3 Distance Bounding

Distance bounding protocols define countermeasure against relay attacks. In essence, a cryptographic distance bounding protocols enables the PCD to compute a maximum distance between the PCD and the PICC. Distance bounding protocols assume that the PICC and the PCD share a secret and measure thereafter the time it takes to exchange a number of bits. Combining the time measurement at the level of nano seconds and the knowledge of the speed of light, the distance can be estimated within an accuracy of a few meters. However, it would still be possible to perform a relay attack with specialized hardware that is able to relay communication close to the speed of light. However, such specialized hardware is very expensive today, resulting in a poor risk/reward ratio [14].

Distance bounding mechanisms have to be implemented into the physical communication layer, because all mechanisms above the physical layer, such as collision-avoidance, result in a fatal inaccuracy of the time measurement [19,28]. This inaccuracy could be prevented using a dedicated and fast RF communication channel. Despite the aforementioned inaccuracy, distance bounding protocols are today and theoretically the best countermeasure against relay attacks.

A simplified distance bounding protocol has been proposed in [14]. The proposed PaySafe protocol is EMV-compliant and, therefore, uses existing fields within EMV (*e.g.,* Unpredictable Number and the ICC Dynamic Number). The main approach of PaySafe is to improve the protocol in such way, that time

measurements can be used as an efficient countermeasure. For this reason, the protocol splits up the challenge and response command from the generation of the signed authentication and cryptogram. The PaySafe protocol also initiates the contactless transaction with the application selection. Now, before the PICC sends its PDOL (message #4 in Figure 3) to the reader, the PICC generates a nonce it temporarily stores. Then the PCD sends a timed GET PROCESSING OPTIONS request to the PICC (message #5 in Figure 3). The PICC immediately responses with the nonce generated in the previous step. This response does not need any computation and, therefore, the variance in the time it takes is very low. If the message was relayed, an additional overhead would be introduced and the PCD can easily detect such a deviation. The suggested upper bound for the respective time out is at 80 ms. Thus, the PaySafe protocol would stop relay attacks using mobile phones or off-the-shelf USB NFC readers.

6 Summary and Conclusions

This paper discussed security issues concerning the EMV protocol. Furthermore, the approach undertaken takes a deeper look at a practical path to relay attacks. As the approach was focused on public transportation PoS machines, it serves as an example only, which did not fraud any public or private body throughout the experiments. Thus, the PoC shows a successful relay attack over an IEEE 802.11 Wireless network, using two commercially available tablets, publicly available Software, and a Visa payWave credit-card.

Even though the EMV specification defines 500 ms as the maximum duration for a transaction, the transactions in those experiments have taken up to 2060 ms and were accepted! Similar behavior has been observed in prior research [14].

Possible countermeasures against relay attacks include additional verification mechanisms, which could prevent the attack by adding security, but giving away convenience emerging from the usage of contactless cards. Time measurement cannot be efficiently deployed due to the variance in dynamic messages and the possibility to cache static messages. Distance bounding requires stable performance and predictable time accuracy of those communication channels in use and in compliance with ISO/IEC 14443 systems. The PaySafe protocol is a simplified distance bounding protocol that is EMV-compliant.

Even though relay attacks have been a quite prominent research topic, the EMV-compliant payment systems in place today are still partially vulnerable. While effective countermeasures are theoretically available, they are not deployed everywhere yet. Since other cards use EMV as well, these cards are vulnerable too [14]. The ease to intercept and relay a full transaction shows that these systems need to be hardened against relay attacks, as currently the only effective defense strategy is to shield the chip as show in Figure 5.

In general, there are further attack scenarios possible, *e.g.*, an attacker with his NFC device in relay mode, can stay at a PoS equipped with a contactless reader. A second attacker with his NFC device in proxy mode and an additional antenna can stay in a crowded place and try to activate foreign cards and relay

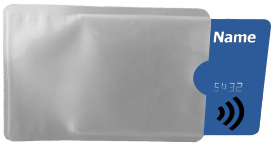

Figure 5. NFC/RFID Card Protection

the APDUs back and forth (cf. setup 2 in Figure 2). However, such an attack does not scale well and the pay-off is not as high compared to the card-not-present fraudulent activities.

Explicit Note: This work performed did proof as its key and only objective the feasibility of this type of reply attack on public Point-of-Sales (PoS) terminals. Since this and only purpose was driven by research motivations on IT system security this work only shows, demonstrates as a proof-of-concept, and indicates technical vulnerabilities. At no times at all the publicly accessible PoS was faced or threatened with any fraud or any misuse of services obtained.

Acknowledgments: This work was partially supported by the FLAMINGO project funded under the EU FP7 Program (Contract No. FP7-2012-ICT-318488).

References

1. CyanogenMod. http://www.cyanogenmod.org, [online; accessed Jan-2016]
2. EMV Contactless Specifications for Payment - Systems Book C-3 - Kernel 3 (Visa)
3. EMV Key Management - Explained. https://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-emv_key_management.pdf, [online; accessed Jan-2016]
4. EMVCo. http://www.emvco.com, [online; accessed Jan-2016]
5. ISO/IEC 14443-2:2010 - Identification cards - Contactless integrated circuit cards - Proximity cards, Part 2: Radio frequency power and signal interface, 2010
6. ISO/IEC 14443-3:2011 - Identification cards - Contactless integrated circuit cards - Proximity cards, Part 3: Initialization and anticollision, 2011
7. ISO/IEC 14443-4:2008 - Identification cards - Contactless integrated circuit cards - Proximity cards, Part 4: Transmission protocol, 2008
8. ISO/IEC 7816-3:2006 - Identification cards - Integrated circuit cards, Part 3: Cards with contacts - Electrical interface and transmission protocols, 2006
9. ISO/IEC 7816-4:2013 - Identification cards - Integrated circuit cards, Part 4: Organization, security and commands for interchange, 2013
10. NFCProxy. http://sourceforge.net/projects/nfcproxy/, [online; accessed Jan-2016]
11. M.Bond, O.Choudary, S.J.Murdoch, S.P.Skorobogatov, R.J.Anderson: Chip and Skim: Cloning EMV Cards with the Pre-play Attack. IEEE Symposium on Security and Privacy (SP 2014). San Jose, CA, USA (May 2014)
12. J.van den Breekel: NFC Hacking: The Easy Way, DEF CON 2012, Las Vegas, Nevada, USA (July 2012)

13. J.van den Breekel: Relaying EMV Contactless Transactions using Off-The-Shelf Android Devices, BlackHat Asia, Singapore, (March 2015)
14. T.Chothia, F.D.Garcia, J.de Ruiter, J.van den Breekel, M.Thompson: Relay Cost Bounding for Contactless EMV Payments. 19th International Conference on Financial Cryptography and Data Security. Puerto Rico (Jan 2015)
15. X.Chu: Relay attacks of NFC smart cards. Master Thesis, NTNU Trondheim, Norwegian University of Science and Technology, Department of Telematics (Jun 2014)
16. L.Francis, G.Hancke, K.Mayes, K.Markantonakis: Practical NFC Peer-to-peer Relay Attack Using Mobile Phones. 6th International Conference on Radio Frequency Identification: Security and Privacy Issues. RFIDSec'10, Istanbul, Turkey (Jun 2010)
17. G.P.Hancke, K.E.Mayes, K.Markantonakis: Confidence in Smart Token Proximity: Relay Attacks Revisited. Computers & Security 28(7) (Oct 2009)
18. G.Hancke: A Practical Relay Attack on ISO 14443 Proximity Cards. Tech. rep., University of Cambridge Computer Laboratory (Feb 2005)
19. G.Hancke, M.Kuhn: An RFID Distance Bounding Protocol. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005). Athens, Greece (Sep 2005)
20. Z.Kfir, A.Wool: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005). Athens, Greece (Sep 2005)
21. C.Killer: NFCProxy Relay Attack in the Wild. https://www.youtube.com/watch?v=fRtn4ZfkLkM, [online; accessed Jan-2016]
22. C.Killer: Security Challenges in Contactless Payments Solutions. Assignment, Communication Systems Group, Department of Informatics, University of Zurich (Jun 2015)
23. S.Murdoch, S.Drimer, R.Anderson, M.Bond: Chip and PIN is Broken. IEEE Symposium on Security and Privacy (SP 2010). Oakland, CA, USA (May 2010)
24. S.J.Murdoch, R.Anderson: Verified by Visa and Mastercard Securecode: Or, How Not to Design Authentication. 14th International Conference on Financial Cryptography and Data Security (FC2010). Tenerife, Spain (Jan 2010)
25. M.Ngu, C.Scott: How Secure are Contactless Payment Systems?, RSA Conference, San Francisco, USA (April 2015)
26. M.Roland, J.Langer: Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on EMV Contactless. 7th USENIX Conference on Offensive Technologies (WOOT 2013). Washigton, D.C., USA (Aug 2013)
27. J.Vila, R.J.Rodriguez: Practical Experiences on NFC Relay Attacks with Android - Virtual Pickpocketing Revisited. 11th Workshop on RFID Security (RFIDSEC 2015). New York City, USA (Jun 2015)
28. M.Weiß: Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment. Master Thesis, Technische Universität München (May 2010)