An Off-the-shelf Relay Attack in a Contactless Payment Solution

Christian Killer, Christos Tsiaras, Burkhard Stiller
University of Zürich, Communication Systems Group, Binzmühlestrasse 14, 8050 Zürich, Switzerland
Email: christian.killer@uzh.ch , {tsiaras l stiller}@ifi.uzh.ch

***Abstract*—The enhanced Radio-Frequency Identification (RFID) technology called Near Field Communication (NFC), is a standards-based wireless communication technology. Passive 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. Nowadays, many Point-of-Sale (POS) terminals, credit cards and also mobile devices are NFC-capable and facilitate contactless payments. Thus, many security sensitive applications already use the contactless technology. A very important attack in the NFC security domain, is the relay attack. This work illustrates a practical relay attack on public transport POS terminals, using off-the-shelf mobile devices and hardware, and summarizes possible countermeasures against relay attacks in NFC communication.**

***Keywords*—NFC, contactless, Security, EMV, Relay attack,**

I. Introduction

Near Field Communication (NFC) technology is 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 the omnipresent protocol in use for smart card payments around the world. The Point-of-Sales (POS) exchanges EMV protocol messages with the chip on the smart card, while selected data is signed with a cryptographic Message Authentication Code (MAC) that is generated by using a symmetric key which is saved on the card. 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 was used, fraud incidents in POS dramatically decreased. However at the same time there was a significant increment of transactions and mainly card-not present fraud increased [23][30]. The widespread distribution of EMV-compliant payment-cards, immediately raised the question if any security issues have to be further investigated. Prior research showed that the EMV protocol has major vulnerabilities that can be exploited [3][25].

The usage of the contactless payment solutions is rapidly growing and the NFC technology is expected to dominate in the micro-payments domain [26]. Nowadays, 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 [35][37][24].

A critical attack in NFC and Radio-frequency Identification (RFID), is the relay attack. The risk of relay attacks in RFID communications has been well-known for years, but still EMV-compliant POS terminals are vulnerable. In some countries, public transport POS machines are equipped with a contactless terminal for credit cards. If such systems were vulnerable to relay attacks, the physical presence of the credit card would not be necessary anymore. This presents a major flaw and disrupts security and privacy assumptions, mainly due to the fact that, most of these contactless smart cards are based on the International Organisation for Standardisation (ISO) / International Electronical Commission (IEC) 14443 standard [18] and are intended to operate over a distance of around 10cm. This paper concentrates on the ISO 14443 of operation mode Type A standard which is used in most contactless cards. Furthermore, the aim of this paper is to implement a practical relay attack on public transportation EMV-compliant POS machines, only using two off-the-shelf mobile tablets, a wireless router and a VISA payWave credit card [37].

The remainder of this paper is structured as follows. Some related work is discussed in Section II, followed by the NFC relay attack setup in Section III. Section IV presents technical details about the implementation of this work, and Section V proposes possible countermeasures to prevent NFC relay attacks. Finally, Section VI summarizes this paper and draws conclusions.

II. Related Work

Relay attacks on ISO/IEC 14443 Type A-based smartcards are introduced in [13]. The radio frequency (RF) communication was relayed up to a distance of 50 meters using Bluetooth [2], or the Institute of Electrical and Electronics Engineers (IEEE) 802.15 standard [17], as a communication channel. This work illustrates how the reduction in complexity of a potential attack is immensely decreased, due to the fact that the potential attacker can use commercially available tools. Moreover, it highlights the potential security implications for current contactless applications.

Recently, 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 [4][5]. 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 50 cm far away. This is a fivefold increase in distance compared to the distance of a genuine 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 even be conducted faster than an actual genuine transaction. This results an optimized, time-saving relay attack [4][5].

There are three different Authentication methods for EMV cards, Static Data Authentication (SDA), Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA) [33]. There are weaknesses concerning these card authentication methods. Cards using SDA are vulnerable to the well-known and trivial "yes-card" attack, where an attacker can copy the static certificate data from a genuine chip to another counterfeit chip. Thereupon, the attacker can use the counterfeit 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. Furthermore, DDA similarly to SDA, also suffers from protocol weaknesses which CDA tries to dissolve. CDA combines DDA, the signing of changing transaction data, with the use of an application cryptogram (AC) generated by the card.

All of these Authentication methods improve the security of contactless transactions. Yet, prior research has also observed that the payment terminal itself can be forced to fall back to old Cardholder Verification methods (CVM) methods, such as downgrading a full EMV credit card to perform a EMV Mag-Stripe transaction [30]. If such an attack vector is possible, all of the other security measures are rendered useless.

Another critical issue concerning EMV, is the EMV Personal Identification Number (PIN) verification “wedge” vulnerability. This vulnerability allows an attacker to use stolen cards without knowing the correct PIN. To do so, the attacker copies a card and modifies that counterfeit card in such a way, that the counterfeit card will accept any PIN entered, for both offline and online transactions [25].

Prior research presented a proof-of-concept for the so-called Pre-Replay attack [3]. An attacker can use a tampered terminal to collect card details. Later on, the attacker can replay the collected data 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. In detail, the attack vector exploits a protocol specification flaw. The flaw is the fact that the POS terminal rather generates predictable, than unpredictable numbers. The deeper protocol design flaw is that the terminal generates the number and the issuer relies on this

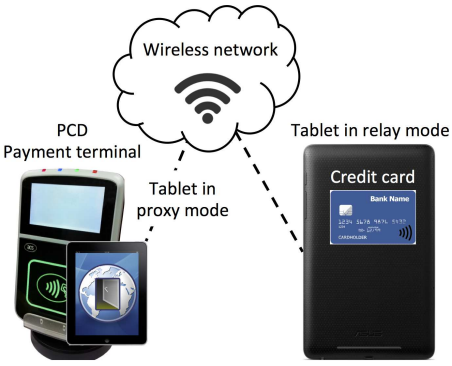

Figure 1. Relay Attack Setup.

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.

III. Architecture

A. Terminology

The terminology used in this work is derived from the application NFCProxy [20]. However, the first attack on RFID systems [12] used a different terminology. The device which emulates a valid smart card is called the proxy in [12]. In this work the device emulating a valid smart card is termed the tablet in Proxy Mode. The device activating the genuine card, termed the Mole in [12], is termed the tablet in Relay Mode.

B. ISO/IEC 14443 Contactless Smart Card Standard

The relay attack presented in this paper applies to ISO/IEC 14443 [18] smart cards of operation mode type A. These smart cards are passive, hence they’re inductively coupled RFID transponders with a fairly small reading 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). ISO/IEC 14443 type A cards only use amplitude key shifting modulation with modified Miller coding [16] for the downlink from PCD to PICC. For the Uplink from PICC to PCD, load modulation by On/Off Keying (OOK) of a Manchester coded stream is used.

C. Relay Attack High-level Architecture

When referring to a relay attack in relation with NFC, the communication channel between the PCD and the PICC is not restricted to the immediate radio frequency field that is established between the two. Basically, this field is virtually extended by redirecting the communication through a remote tunnel. In consequence, the physical presence of the PICC is no longer required. In Figure 1, the PCD is the POS payment terminal, the PICC is the credit-card. As a remote tunnel, a dedicated IEEE 802.11 wireless network was used. This work assumes that the delay occurring is below 1.5 s and therefore the attack is possible [3].

IV. Implementation

A. NFC Proxy

NFCProxy [20] is the main Software (S/W) used to carry out the relay attack in this work. Concerning the Hardware (H/W), to facilitate the relay attack in this work, two commercially available off-the-shelf mobile tablets were used. NFCProxy requires an extension of certain versions (9.1 and 10.1) of the CyanogenMod [6]. The installation of those versions is mandatory because NFCProxy requires certain code that is handling Host Card Emulation (HCE), which was removed in newer versions. CyanogenMod is an unofficial branch of the Android Operating System (OS) [1]. Thus, 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 [28], which is used on many commercially available devices. Besides the two tablets running CyanogenMod, an IEEE 802.11 wireless network interface needs to be provided. To achieve this, in this work a portable IEEE 802.11 b/g/n wireless router has been used, which was powered on with a mobile power source.

B. Hardware Specification of the Setup

To facilitate the replay attack it is essential to meet the exact H/W and S/W requirements. Thus, an exact listing of the exact setup used is provided below.

- Two identical Mobile Tablets
  - Brand/Model: ASUS Nexus 7v1,
    Operating System: CyanogenMod 10.1
- Wireless Router
  - Brand/Model: Alfa Network Hornet-UB
    Chip Set: Atheros AR9331 SoC,
    Frequency: 2.4 GHz,
    TX Power: 802.11 b/g/n
- Credit-Card
  - Brand: VISA
    Model: Visa Card Classic
    payWave Limit: CHF 40.-

C. Relay Attack Proof-of-Concept

The Relay Attack implementation was tested at two different public transport POS terminals that were capable of handling contactless transactions [22]. Two relay attacks at two different terminals were video-recorded and can be seen in a proof of concept (POC) video [21]. In Switzerland, most POS terminals are provided by the same supplier, using the same models [36]. Therefore, it can be assumed that most of these systems are vulnerable to a relay attack as illustrated in this paper.

D. EMV Contactless Transaction

EMV Contactless [9] is the standard for contactless PICCs, which doesn't replace the EMV Contact standard, but offers a faster alternative. The contact chips, for both contact and contactless PICCs, are usually based on the ISO/IEC 7816 [19] standard and the 'contactless integrated circuit' is designed according to ISO/IEC 14443 1-4 [18].

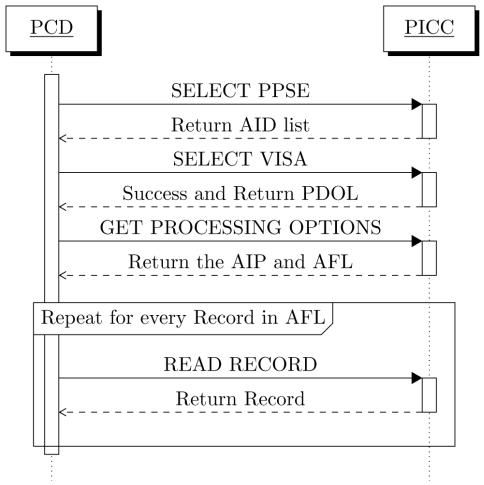

Figure 2. EMV Contactless Transaction Sequence Diagram.

In contact systems, the ISO/IEC 7816-3 standard specifies the Open Systems Interconnection (OSI) layer 1 (Transport), 2 (Data link) and 4 (Physical)[29]. However, in contactless systems, these three layers are specified in ISO/IEC 14443 2-4 [18]. 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 on OSI layer 7 (Application) is the same as specified in 7816-4 for contact based systems. Further, the transaction protocol supports the use of so-called Application Protocol Data Units (APDU).

Yet, 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 REQA. After that, the 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, the PICC sends 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 for answer to select (RATS) as command and expects an answer to reset (ATS) as 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.

Visa's payWave transactions are using the quick Visa Smart Debit/Credit (qVSDC) protocol, 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) (5^{th} message in Figure 2) request, because the card will respond to the GPO by calculating the Application Cryptogram (AC) and sign the data in the next response (6^{th} message in

Figure 2). The different steps in a Visa contactless transaction can be divided into 8 steps [4]. This work focuses on the Visa payWave Contactless EMV standards, because the POC was implemented assuming/using a Visa Basic credit-card. However, adopting the necessary steps to use a MasterCard is possible as proposed in [5].

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 containing application details. In more detail, it contains the Processing Options Data Object List (PDOL) with all the 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, now the PCD requests the processing options. In essence, the PCD responds with the PDOL Related data encoded according to the PICCs 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 CVV). The AFL also indicates if any of the data will be provided for the Authentication Process. As a result, the card is in control what 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 requested records.

The Visa payWave logs that were recorded during the POC implementation [21] follow the same basic structure as described above. As a card authentication method, the off-line 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 5th also included an Unpredictable Number (UN). The card is expected to return 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 2, message 7 and 8 are repeated for every record in the AFL. Therefore the PCD starts to read data (message 7) records 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 7th message. In the second response (message 8) of the card, the PAN, expiration date, issuer code and the ICC Public Key Certificate is returned. If everything was accepted by the POS terminal, the transaction was successful.

There are three main Cardholder Verification Methods (CVM) which are supported by EMV. There is Online and Offline PIN verification, or the use of signatures (which is used for magnetic-stripe cards). Usually, for low amount transactions (payWave limit is $40), no additional CVM is used. the card only authenticates itself with CDA by generating an application cryptogram.

V. Possible Countermeasures

To carry out the relay attack as presented in this paper, an attacker doesn't have to decrypt or understand any of the encrypted data. Hence, providing sufficient protection against such passive relay attacks is difficult, because the attack can't be prevented by application-level cryptography [15]. Therefore, to supplement the existing security mechanisms, additional countermeasures are required. These countermeasures should focus on the main aspects of the attack: (1) the added time delay and (2) any unnoticed access to the card [13]

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 or mesh) and thus prevent unwanted remote activation [13]. A selection of other possible countermeasure is presented in this paper.

A. Additional Verification

Relay attacks could be prevented by introducing secondary authentication procedures (*E.g.* password, biometrics). However, such additional verification countermeasures demand more user-interaction which eliminates the convenience emerging from the use of the contactless smart cards. Another issue that could arise is the resulting increase in transaction time, which might not be acceptable in every application.

B. Time Measurement

A valid and genuine contactless transaction has a certain time range 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 [3] of contactless cards, setting a time limit could easily lead to valid transactions being rejected.

Theoretically, if an accurate response time would be recorded for every PICC and PCD combination, it would in fact be possible to implement a maximum time duration for a transaction as presented in this work [38]. The implementation of such a Time Measurement challenge-response protocol would most certainly make practical relay attacks impossible [30].

In contrary, prior research also concluded that the observed time variance on dynamic messages between various cards was even larger than the introduced overhead by the relay [5]. In conclusion, simply using an overall time limit on static or dynamic (*E.g.* the GENERATE AC message response in MasterCard PayPass, the GET PROCESSING OPTIONS message response in Visas PayWave) cannot be used as an efficient countermeasure against relay attacks.

The attacks in the POC video [21] lasted between 671 and 2050 ms and were accepted either way. Yet, the EMV Contactless standard officially only allows up to 500 ms of total time per transaction [7] [11] [8] [10]. Prior research could also observe equal behavior. 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 [12]. In conclusion, timing constraints aren't sufficient to provide enough protection against relay attacks.

C. Distance Bounding

Distance bounding protocols are a typical countermeasure against relay attacks. Prior research has widely studied and proposed good solutions. In essence, a cryptographic distance bounding protocols enables the PCD to compute a maximum distance between the PCD and the PICC. Basically, distance bounding protocols assume that the PICC and the PCD share a secret and then measure 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 with an accuracy of a few meters. However, it would still be possible to perform a relay attack with specialized hardware relaying communication close to the speed of light [5].

Distance bounding mechanisms have to be implemented into the physical communication layer to calculate appropriate numbers, because all the mechanisms above the physical layer, such as collision-avoidance, result in fatal inaccuracy of time measurement [14] [38]. This inaccuracy could be prevented using a specially dedicated and fast RF communication channel. Still, because of the aforementioned inaccuracy, complex distance bounding protocols are, only theoretically, the best countermeasure against relay attacks at the moment.

D. Relay Cost Bounding

A simplified distance bounding protocol has been proposed in this work [5]. The proposed PaySafe protocol is EMV compliant and therefore uses existing fields within EMV (*E.g.* Unpredictable Number (UN) 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 (4^{th} in Figure 2) to the reader, the PICC generates a nonce it temporarily stores. Then the PCD sends a timed GET PROCESSING OPTIONS request to the PICC (5^{th} in Figure 2). The PICC now immediately responses with the nonce generated in the previous step. This response doesn't 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 now easily detect such a deviation. The suggested upper bound for time out is 80 ms. In conclusion, the PaySafe protocol would stop relay attacks using mobile phones or off-the-shelf USB NFC readers.

VI. Summary and Conclusion

This paper discusses various security issues concerning the EMV protocol. Furthermore, it takes a deeper look at a practical approach to the relay attack. Further, this approach was focused on public transportation POS machines. The POC shows a successful relay attack over an IEEE 802.11 Wireless network, using two commercially available tablets and publicly available S/W.

Even though the official EMV specification defines 500 ms as maximum duration for a transaction [9], the transactions have taken up to 2060 ms and were accepted. Similar behavior has been observed in prior research. Possible countermeasures against relay attacks include Additional Verification mechanisms which could prevent the attack by adding more security but giving away convenience emerging from the usage of contactless smart cards. The second type of countermeasure, time measurement, can't be efficiently deployed because of the variance in dynamic messages and the possibility to cache static messages. The third type of countermeasure, distance bounding, can't be deployed because of the lack of performance and accuracy of the communication channels in ISO/IEC 14443 systems. However, prior research developed the PaySafe [5] protocol, which is a simplified distance bounding protocol that is EMV compliant.

There are many possible attack scenarios, *E.g.*, an attacker, with his tablet in Relay Mode, can stay at a POS equipped with a contactless reader. A second attacker with his tablet in Proxy mode and an additional antenna [20], can stay in a very crowded place and try to activate foreign cards and relay the APDUs back and forth. Additionally, such an attack scenario needs a different communication channel (*e.g.*, via SMS or accessing a web server using 4G) to access multiple distant locations (*e.g.*, different cities). Fortunately, such an attack doesn't scale up and the pay-off is not significant compared to card-not-present fraudulent activities.

Nevertheless, the classic relay attack on EMV contact transactions probably offers a larger attack potential. Mainly due to the fact that targets can be of higher value [31], and not only below the low limit (*e.g.*, payWave limit of CHF 40.-) of contactless transactions.

Concluding, even though the relay attack has been a prominent research topic, the EMV-compliant payment systems [36] in place are still vulnerable and effective countermeasures are theoretically available, but not deployed yet. The POC attack in this paper was implemented using a Visa Card Classic with payWave, but it could work with other credit cards as well. The ease to intercept and relay a full transaction shows that these systems need to be hardened against relay attacks, as currently there is not an effective defense strategy in place.

ACKNOWLEDGMENT

This work was supported partially by the SmartenIT and the FLAMINGO projects, funded by the EU FP7 Program under Contract No. FP7-2012-ICT-317846 and No. FP7-2012-ICT-318488, respectively. Special thanks are addressed to Michael Roland for providing help regarding Near Field Communication (NFC) chipsets and Europay, Mastercard and Visa (EMV) protocol analysis.

REFERENCES

[1] Android, URL: https://www.android.com/, Visited in May 2015.

[2] Bluetooth, URL: http://www.bluetooth.com, Visited in May 2015.

[3] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, R. Anderson, *Chip and Skim: Cloning EMV Cards with the Pre-play Attack*, IEEE Symposium on Security and Privacy (SP), pp 49-64, San Jose, CA, U.S.A., May 18-21, 2014.

[4] J. van den Breekel, *Relaying EMV Contactless Transactions using Off-The-Shelf Android Devices*, BlackHat Asia. March, 2015.

[5] 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, January 26?30, 2015.

[6] CyanogenMod, URL: http://www.cyanogenmod.org/, Visited in May 2015.

[7] EMVCo, *Application Independent ICC to Terminal Interface Requirements*, eBook v4.3, November, 2011.

[8] EMVCo, *Application Specification*, eBook v4.3, November, 2011.

[9] EMVCo, *Architecture and General Requirements* eBook v2.5, March, 2015.

[10] EMVCo, *Cardholder, Attendant, and Acquirer Interface Requirements*, eBook v4.3, November, 2011.

[11] EMVCo, *Security and Key Management*, eBook v4.3, November, 2011.

[12] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, 6th international conference on Radio frequency identification: security and privacy issues (RFIDSec10), pp 35-49, Istanbul, Turkey, June 8-9, 2010.

[13] G. P. Hancke, *A Practical Relay Attack on ISO 14443 Proximity Cards*, Technical report, University of Cambridge Computer Laboratory, February, 2005.

[14] G.P. Hancke, M.G. Kuhn, *An RFID Distance Bounding Protocol*, First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005), Athens, greece, September 5-9, 2005.

[15] G. P. Hancke, K. E. Mayes, K. Markantonakis, *Confidence in smart token proximity: Relay attacks revisited.* Computers and Security 28, pp. 615-627, 2009.

[16] E. Haselsteiner, K. Breitfuss, *Security in near field communication (NFC)*, Philips Semiconductors Austria, Workshop on RFID security, p. 3, 2006.

[17] IEEE 802.15, URL: http://www.ieee802.org/15/, Visited in May 2015.

[18] ISO/IEC 14443, *Identification cards - Contactless integrated circuit(s) cards - Proximity cards.*

[19] ISO/IEC 7816 *Identification cards - Integrated circuit cards.*

[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), pp 47-58, Athens, Greece, September 5-9, 2005.

[21] C. Killer, *NFCProxy Relay Attack in the Wild*, URL: http://tiny.uzh.ch/em, Visited in May 2015.

[22] E. Lee, *NFC Hacking: The Easy Way*, Blackwing Intelligence, URL: http://tiny.uzh.ch/en, Visited in May 2015.

[23] 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 (FC 2010), pp 336-342, Tenerife, Canary Islands, January 25-28, 2010.

[24] MasterCard payPass, URL: http://tiny.uzh.ch/es, Visited in May 2015.

[25] S. J. Murdoch, S. Drimer, R. Anderson, M. Bond, *Chip and PIN is Broken*, IEEE Symposium on Security and Privacy (SP), pp 433-446, Oakland, CA, U.S.A., May 16-19, 2010.

[26] M. Ngu, C. Scott, *How Secure are Contactless Payment Systems?*, RSA Conference, San Francisco, U.S.A., April 20-24, 2015.

[27] NFCProxy, URL: http://sourceforge.net/projects/nfcproxy/, Visited in May 2015.

[28] NXP PN544 NFC Controller, URL: http://www.nxp.com/documents/leaflet/75016890.pdf, Visited in May 2015.

[29] M. Roland, , *Security Issues in Mobile NFC Devices*, T-Labs Series in Telecommunication Services, 2015.

[30] M. Roland, J. Langer, *Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on EMV Contactless*, 7th USENIX conference on Offensive Technologies (WOOT13), Washington D.C., U.S.A., August 13, 2013.

[31] A. Ross, S. J. Murdoch, *EMV: Why Payment Systems Fail*, Communications of the ACM, Vol. 57, Issue 6, pp 24-28, June 2014.

[32] J. de Ruiter, E. Poll. *Formal Analysis of the EMV Protocol Suite*, LNCS Theory of Security and Applications, pp 113-129, January, 2012.

[33] SBB CFF FFS, *The SBB Ticket Machine*, URL: http://tiny.uzh.ch/eo, Visited in May 2015.

[34] Smart Card Alliance Contactless Payment Council, *EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality*, October, 2012, URL: http://tiny.uzh.ch/et, Visited in May 2015.

[35] Smart Card Alliance Contactless Payment Council, *Smart Cards Applications*, URL: http://tiny.uzh.ch/ep, Visited in May 2015.

[36] SIX Payment Services, URL: http://tiny.uzh.ch/eq, Visited in May 2015.

[37] Visa payWave, http://tiny.uzh.ch/er, Visited in May 2015.

[38] M. Weiss, *Performing Relay Attacks on Contactless Smart Cards Using Mobile Equipment*, Master Thesis, Technische Universität München, May, 2010.