COMPUTING SCIENCE

Harvesting High Value Foreign Currency Transactions from EMV Contactless Cards Without the PIN

Martin Emms, Budi Arief, Leo Freitas, Joseph Hannon and Aad van Moorsel

TECHNICAL REPORT SERIES

No. CS-TR-1421 May 2014

TECHNICAL REPORT SERIES

No. CS-TR-1421 May, 2014

Harvesting High Value Foreign Currency Transactions from EMV Contactless Cards Without the PIN

M. Emms, B. Arief, L. Freitas, J. Hannon and A. van Moorsel

Abstract

In this paper we present an attack which allows fraudulent transactions to be collected from EMV contactless credit and debit cards without the knowledge of the cardholder. The attack exploits a previously unreported vulnerability in EMV protocol, which allows EMV contactless cards to approve unlimited value transactions without the cardholder's PIN when the transaction is carried out in a foreign currency. For example, we have found that Visa credit cards will approve foreign currency transactions for any amount up to €999,999.99 without the cardholder's PIN, this side-steps the £20 contactless transaction limit in the UK. In reality, the criminals would choose a value between €100 and €200, which is low enough to be within the victim's balance and not to raise suspicion, but high enough to make each attack worthwhile. This paper outlines a scenario in which fraudulent transaction details are transmitted over the Internet to a "rogue merchant" who then uses the transaction data to take money from the victim's account. The attack described in this paper differs from previously identified attacks on EMV cards, in that it can be used to directly access money from EMV cards rather than to buy goods. The attack is novel in that it could be operated on a large scale with multiple attackers collecting fraudulent transactions for a central rogue merchant which can be located anywhere in the world where EMV payments are accepted.

Printed and published by Newcastle University,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

EMMS, M., ARIEF, B., FREITAS, L., HANNON, J., VAN MOORSEL, A.

Harvesting High Value Foreign Currency Transactions from EMV Contactless Cards Without the PIN
[By] M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel
Newcastle upon Tyne: Newcastle University: Computing Science, 2014.

(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1421)

Added entries

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR-1421

Abstract

In this paper we present an attack which allows fraudulent transactions to be collected from EMV contactless credit and debit cards without the knowledge of the cardholder. The attack exploits a previously unreported vulnerability in EMV protocol, which allows EMV contactless cards to approve unlimited value transactions without the cardholder's PIN when the transaction is carried out in a foreign currency. For example, we have found that Visa credit cards will approve foreign currency transactions for any amount up to €999,999.99 without the cardholder's PIN, this side-steps the £20 contactless transaction limit in the UK. In reality, the criminals would choose a value between €100 and €200, which is low enough to be within the victim's balance and not to raise suspicion, but high enough to make each attack worthwhile. This paper outlines a scenario in which fraudulent transaction details are transmitted over the Internet to a "rogue merchant" who then uses the transaction data to take money from the victim's account. The attack described in this paper differs from previously identified attacks on EMV cards, in that it can be used to directly access money from EMV cards rather than to buy goods. The attack is novel in that it could be operated on a large scale with multiple attackers collecting fraudulent transactions for a central rogue merchant which can be located anywhere in the world where EMV payments are accepted.

About the authors

Martin Emms is studying for a research PhD at Newcastle University's Centre for Cybercrime and Computer Security (CCCS). My research into potential vulnerabilities in the EMV payments system brought about by the introduction of Near Field Communications (NFC) payment technologies (i.e. NFC payment cards, mobile phone payments applications, NFC payment tags and NFC payment / top-up wrist bands). Supervised by Professor Aad van Moorsel with the School of Computing Science at Newcastle University. Martin has also been working with a local women's support centre in the North East of England to better understand the issues faced by survivors of domestic violence. The main focus of this research has been enabling survivors to access online / electronic domestic violence support services without the fear of being caught by their abuser. His role has been to design new applications that can help survivors access support services without leaving tell-tale electronic footprints.

Dr. Budi Arief is the leading Research Associate (RA) at the Centre for Cybercrime and Computer Security at Newcastle University, one of the recognised UK Academic Centres of Excellence in Cyber Security Research. His research interests include human aspects of computer security, the dependability of computer-based systems, and mobile/ubiquitous computing. In particular, he is applying his extensive experience in interdisciplinary research to address issues related to cybercrime and cyber security. These include investigation into how technology can be used to help everyday users and vulnerable groups, such as children and domestic violence survivors. Budi also manages the UK EPSRC-funded Cybercrime Network, and is a Researcher Co Investigator of the Hyper-DoVe (Hyper-privacy: Case of Domestic Violence) project aiming to help domestic violence survivors.
In the past, Budi had worked as an RA on various projects, including the EPSRC-funded Dependability Interdisciplinary Research Collaboration (DIRC), two EU-funded projects (FP6-IST RODIN and FP6-IST TRACKSS), and the EPSRC-funded Trustworthy Ambient Systems (TrAmS) platform grant.
He has published over 35 papers, has acted as reviewers for journals/conferences, and he is currently serving as an expert reviewer of an EU FP7 project in the area of Internet of Things.

Leo Freitas is a lecturer in Formal Methods working on the EPSRC-funded AI4FM project at Newcastle University. Leo received his PhD in 2005 from the University of York with a thesis on 'Model Checking Circus', which combined refinement-based programming techniques with model checking and theorem proving. Leo's expertise is on theorem proving systems (e.g. Isabelle, Z/EVES, ACL2, etc.) and formal modelling (e.g. Z, VDM, Event-B), with particular interest on models of industrial-scale. Leo has also contributed extensively to the Verified Software Initiative (VSTTE).

Joseph Hannon is a final year Computer Science student (at Newcastle University) on route to a 1st in his MComp. His research interests include credit card security, malware and mobile development.

Aad van Moorsel is a Professor in Distributed Systems and Head of School at the School of Computing Science in Newcastle University. His group conducts research in security, privacy and trust. Almost all of the group's research contains elements of quantification, be it through system measurement, predictive modelling or on-line adaptation. Aad worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. He got his PhD in computer science from Universiteit Twente in The Netherlands (1993) and has a Masters in mathematics from Universiteit Leiden, also in The Netherlands. After finishing his PhD he was a postdoc at the University of Illinois at Urbana-Champaign, Illinois, USA, for two years. Aad became the Head of the School of Computing Science in 2012.

Suggested keywords

ELECTRONIC COMMERCE
CYBERCASH
DIGITAL CASH
PAYMENT SCHEMES
SECURITY
SMARTCARDS

Harvesting high value foreign currency transactions from EMV contactless cards without the PIN

ABSTRACT

In this paper we present an attack which allows fraudulent transactions to be collected from EMV contactless credit and debit cards without the knowledge of the cardholder. The attack exploits a previously unreported vulnerability in EMV protocol, which allows EMV contactless cards to approve unlimited value transactions without the cardholder's PIN when the transaction is carried out in a foreign currency. For example, we have found that Visa credit cards will approve foreign currency transactions for any amount up to €999,999.99 without the cardholder's PIN, this side-steps the £20 contactless transaction limit in the UK. In reality, the criminals would choose a value between €100 and €200, which is low enough to be within the victim's balance and not to raise suspicion, but high enough to make each attack worthwhile. This paper outlines a scenario in which fraudulent transaction details are transmitted over the Internet to a "rogue merchant" who then uses the transaction data to take money from the victim's account. The attack described in this paper differs from previously identified attacks on EMV cards, in that it can be used to directly access money from EMV cards rather than to buy goods. The attack is novel in that it could be operated on a large scale with multiple attackers collecting fraudulent transactions for a central rogue merchant which can be located anywhere in the world where EMV payments are accepted.

Categories and Subject Descriptors

K.4.4 [**COMPUTERS AND SOCIETY**]: Electronic Commerce – *Cybercash, digital cash, Payment Schemes, Security;* C.3 [**SPECIAL-PURPOSE AND APPLICATION-BASED SYSTEMS**]: - *Smartcards*

General Terms

Security

Keywords

Contactless cards, EMV, fraudulent transaction, foreign currency transaction limits, rogue merchant.

1. INTRODUCTION

Our research has identified a practical attack on EMV[1] contactless credit and debit cards, which allows large-scale "harvesting" of fraudulent payments from unsuspecting cardholders. The attack exploits six functional characteristics of EMV contactless credit and debit cards:

- Many EMV credit cards will approve *unlimited value transactions in a foreign currency*; this allows the attack to maximise the money extracted from each credit / debit card.
- The *contactless interface* allows transactions to be extracted whilst the card is still in the cardholder's wallet.
- The cardholder's *PIN is not required for contactless transactions*; this allows the fraudulent transaction to be extracted from the card without any further interaction from the cardholder.
- Visa contactless cards will approve *transactions in offline mode*; this allows the attack to be performed without connecting to the card payment system, thereby avoiding any additional security checks by the bank.
- The *merchant details are not included* in the data signed by the card; this allows the merchant details to be added later, making the attack more flexible and scalable.
- While the EMV protocol requires payment cards to authenticate themselves to the Point of Sale (POS) terminals, currently *there is no requirement for POS terminals to authenticate themselves*.

The main contribution of this paper is the identification of a newly discovered vulnerability of the EMV protocol centred on the card's handling of foreign currencies. This is made possible by a combination of the six functional characteristics described above. The introduction of EMV contactless cards has created a situation comparable to that described by Reason in his "Swiss cheese" model [9] where layers of protection can be compromised if holes on each layer line up to create an exploitable attack. In this case, the six characteristics line up in a way that defeats the safeguards put in place by EMV. Through this paper we also contribute two potential solutions which will block this vulnerability.

The ability to capture fraudulent transactions and store them for later transmission to a "rogue merchant" makes this attack different from previously described relay attacks [1] on EMV contactless cards. The relay attack depends upon very close coordination between two attackers; the first attacker has to be in contact with the victim's card whilst the second attacker makes a purchase at a POS terminal. This makes relay attacks difficult to operate on a large scale. Relay attacks are also limited to making £20 contactless purchases.

Similar to the "Chip & PIN is broken" attack [3], our attack can potentially be operated on a large scale. "Chip & PIN is broken" allows attackers to buy goods from retailers, whereas the attack described in this paper is different in that it targets the money in the victim's bank account.

The very recent "Chip and Skim" attack [4] is similar to our attack in that it could be operated on a large scale and it extracts money from the victim's account. It would be interesting to explore the possibility of using our mobile phone contactless-transaction-collecting app as the "skimming" platform for the Chip and Skim attack.

[1] EMV (Europay, MasterCard, and Visa) is a global standard to support interoperable card payment system between Visa, MasterCard, American Express and JCB.

The rest of the paper is organised as follows. Section 2 provides an overview of the attack, which is composed of two stages: collection of fraudulent transactions, and converting these transactions into money. Section 3 outlines existing safeguard to protect EMV transactions, while Section 4 looks into the EMV functionality exploited by the attack. Section 5 outlines the experimental software implementation to carry out the attack, including an Android app and a rogue merchant server. Section 6 presents some results from executing the attack, demonstrating the feasibility of such attack. In Section 7 we offer potential methods for preventing the attack and Section 8 concludes our paper.

2. OVERVIEW OF THE ATTACK

Figure 1 shows the key elements of the attack and how they interact with the EMV payment system.

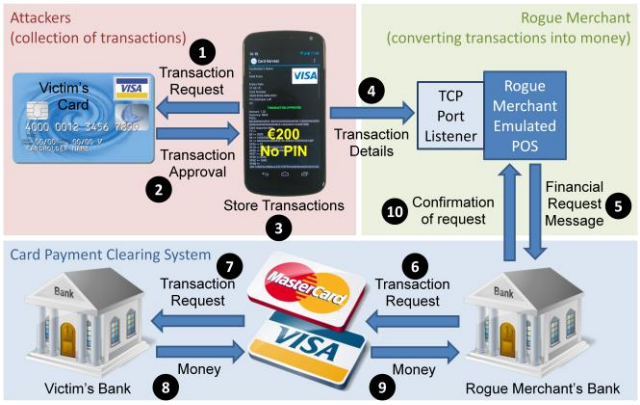

Figure 1: Transaction harvesting attack

The attack consists of two stages:

- *Attackers (collection of fraudulent transactions)*: attackers using Near Field Communication (NFC) enabled Android mobile phones can collect fraudulent transactions from unsuspecting cardholders. This can be done whilst the contactless card is still in the cardholder's pocket. (see steps 1 to 3 of Figure 1).
- *Rogue merchant (converting transactions into money)*: a rogue merchant converts the collected transactions into money in their bank account by sending the transaction data to a bank. (steps 4 to 5 of Figure 1).

Finally the transaction request enters the *Card payment clearing system* where the rogue merchant's bank acts innocently to transfer the transactions into the card payment system which transfers the money from the victim's bank account into the "rogue merchant's" bank account. (see steps 6 to 10 of Figure 1).

2.1 Collecting fraudulent transactions

Transactions are collected using a malicious app written for NFC-enabled Android mobile phones. The app automatically initiates and collects a transaction immediately upon detection of a contactless credit / debit card in the phone's NFC field. This process takes less than 500 milliseconds from card detection to transaction completion.

It is imagined that attackers will operate in a similar way to pickpockets, hiding their activity in crowded situations such as on public transport or in the crowd at an event. When a credit / debit card is detected, the app gives the attacker an audible signal through their headphones; a second audible signal is given when the transaction collection is complete. This will allow the attacker to operate without attracting too much attention.

2.1.1 Hardware

An Android mobile phone is chosen as the attack platform due to the following reasons:

- Android mobile phones have a built-in NFC reader.
- An Android phone is an innocuous item for the attacker to carry in a crowded place; for example, it will not raise attention if the attacker is stopped by the police, since everyone carries mobile phones these days.
- The mobile phone platform provides portability, Internet connectivity and good battery life, making it a very capable attack platform.

2.1.2 The transaction collecting app

The attack starts when the NFC-enabled Android phone identifies a contactless credit / debit card which is vulnerable to this attack in the victim's wallet. The app sends a transaction request to the vulnerable card. At the same time, it will also play an audible alert to the attacker to signal that a vulnerable card has been found.

The victim's card approves the transaction by signing the transaction data with its RSA private key. This is possible because at the moment, the EMV protocol does not require the Point of Sale (POS) terminal to authenticate itself to the card.

The signed data elements are used in the EMV payment clearing process as confirmation that the transaction has been approved by a genuine EMV credit / debit card. The signing of the transaction data also ensures that the transaction details (such as the transaction amount) cannot be changed subsequent to the card authorising the transaction. The app plays a second audible alert to notify that transaction collection is complete.

2.1.3 Storage of approved transactions

The app was designed to operate in locations where an Internet connection is not always available, for example on underground public transport. Therefore the app will initially just store the transaction authorisation data returned by the victim's card. When a reliable Internet connection is available, the app will send the stored transaction data to the rogue merchant who will convert the transaction data into money. For the full list of transaction authorisation data elements see Section 5.1.5.

The ability to capture fraudulent transactions offline and store them for later transmission is one of the novel features of this attack. This allows the attack to be operated on a large scale.

Furthermore, storing the transactions minimises the time required to collect fraudulent transactions as the app does not have to wait for a connection. It also allows the attackers to operate in victim-rich crowded places that are normally without an Internet connection such as on subway trains, on busses and in lifts.

2.2 Converting transaction data into money

The criminals would set up a rogue merchant account with an acquirer bank in one of the 76 countries that accept EMV payments. This rogue merchant will receive the fraudulent

transactions collected by the attackers and convert them into money by sending the transaction data to the bank.

The rogue merchant consists of three elements:

- An Internet-based listening service, which will receive collected transaction data from attackers.
- A data format conversion process, which converts the fraudulent transactions collected by the attackers into the format required by the bank.
- A "rogue" Point of Sale (POS) terminal, which must imitate the actions of a legitimate POS terminal so that it does not raise the bank's suspicion. To achieve this, the rogue POS takes the previously converted data, adds the merchant data and sends that data to the bank using an Internet Protocol (IP) connection.

2.2.1 Internet-based listening service

The rogue merchant provides an Internet-based listening service on a pre-arranged IP address and port number, to receive the fraudulent transactions from the attackers. The transactions are initially stored to be processed later, once the merchant details have been added to the transaction and the connection to the acquirer bank is available.

2.2.2 Data format conversion process

Financial presentment request messages are used to transmit EMV credit / debit card transactions between the merchant (who captured the transaction) and the acquirer bank (who will process the transaction).

Merchant-related data such as merchant ID, terminal ID and the merchant's bank account details are added to the transaction to complete the data required by the EMV card clearing system. The fraudulent transaction is now ready for transmission to the acquirer bank.

The exact format of the message will differ slightly between different acquirer banks. However, there are a number of mandatory fields that are the same for every acquirer bank. Standard 70 [5] in the UK and ISO 8583 [6] in other EMV countries define the mandatory data fields which must appear in the financial presentment request message and the optional fields which may differ between the acquirer banks.

The software for our attack prototype implements a Standard 70 message format, complete with all of the mandatory fields and a number of optional fields (see Section 5).

2.2.3 "Rogue" POS terminal process

Once correctly formatted, the financial presentment request message is sent to the bank. The acquirer bank returns a financial presentment response message, to which the merchant responds with a financial presentment confirmation message that acknowledges receipt of the acquirer's response message.

The supported communication options for this message exchange are PSTN, X25 over ISDN, IP over ISDN, and IP over public networks (i.e. the Internet) for transmission of messages between the merchant and the acquirer bank. The software implementation presented in this paper uses IP over the Internet.

Our software implements data format conversion (Section 2.2.2) and implements the sending of the financial presentment request message over an IP connection protected by SSL/TLS encryption.

For obvious reasons we were not willing or able to check against a real bank. Of course, one approach to defeating the attack is to try to detect rogue POS behaviour at the bank, but it is not clear how well this can be done. A simple solution would be to have the payment card reject any contactless foreign currency transaction immediately, but is just not practical. As we will argue in Section 7, a more effective solution can be implemented by either forcing foreign currency contactless transactions to be carried out in online mode only, or where that is not possible, to switch the transaction to "Chip & PIN".

3. EMV TRANSACTION SAFEGUARDS

In the UK, EMV credit / debit cards can perform two different transaction types: contactless "tap and go" transactions, and contact "Chip & PIN" transactions.

3.1 Contactless "tap and go" transactions

Contactless transactions are intended to be a quick and convenient replacement for small cash purchases. In a contactless payment, the credit / debit card is placed on the POS terminal's contactless reader for less than 1 second and the payment is approved.

There are two significant differences between a contactless transaction and a contact "Chip & PIN" transaction. First, the contact transaction requires the cardholder to enter their PIN, whereas the PIN is not required for contactless transactions. Second, contact transactions require the card to be removed from the wallet and inserted into the POS terminal, whilst contactless transactions is completed wirelessly by placing the card on the POS terminal, this can be done whilst the card is still in the wallet.

PIN entry provides one of the key safeguards in "Chip & PIN" transactions. The PIN ensures that only the cardholder, who knows the PIN, can use the card. Contactless transactions are not protected by PIN entry. EMV have therefore implemented the following safeguards to limit the potential loss from lost or stolen contactless cards:

- In the UK, each contactless transaction is limited to £20; any transaction above this value will require a Chip & PIN transaction.
- EMV cards are limited to five consecutive contactless transactions, after which the PIN must be entered in a "Chip & PIN" transaction.

These safeguards ensure that the maximum loss due to a lost or stolen contactless card is £100.

3.2 Contact "Chip & PIN" transactions

The majority of EMV card transactions are "Chip & PIN" transactions. "Chip & PIN" transactions allow purchases up to the balance of a debit card or the credit limit of a credit card.

"Chip & PIN" transactions are protected by the following safeguards. First, the cardholder must enter their PIN to authorise the transaction. This is used to ensure that the person making the payment is the authorised cardholder.

Second, if the value of the transaction is greater than the card's *offline* transaction limit, the card will request that the POS terminal makes an *online* connection to the bank to perform additional authorisation checks. The POS terminal must connect to the bank to provide the card with the *online* authorisation code. The bank will respond with the authorisation code only if the card has not been reported lost or stolen, and the account has sufficient funds to pay for the transaction. The card will only authorise the transaction if it receives a valid online authorisation code from the POS terminal.

3.3 Cryptographic protection of transactions

The EMV payment system utilises RSA cryptography to ensure that only genuine EMV credit / debit cards can authorise transactions. This is achieved by requesting the card to generate a digital signature of the transaction data. This serves two purposes: it proves that a genuine EMV card, with a bank-issued private key, authorised the transaction; and it prevents the merchant from changing the transaction data (e.g. transaction amount) after the card has approved the transaction.

4. EMV FUNCTIONALITY EXPLOITED BY THE ATTACK

The attack circumvents the safeguards built into EMV credit / debit cards by exploiting some EMV functionality that has been made vulnerable due to the introduction of contactless payment interface. In particular, there are three features that are exploited in our attack scenario:

1. Contactless foreign currency transactions. As described in Section 3.1, the safeguards built into EMV will limit the maximum value allowed for each contactless transaction to £20. Any amount over £20 will require the cardholder to enter their PIN, and any amount above the *offline* transaction limit (e.g. £100) will require the POS terminal to connect to the bank to perform additional checks before the transaction is approved. Our research has found that EMV credit and debit cards can be tricked into approving contactless transactions of much higher value than £20, simply by requesting the transaction in a foreign currency. In our experiments, EMV cards have been found to approve contactless transactions up to €999,999.99 without requesting the PIN, and without requesting that the POS terminal goes *online* to perform additional checks. This sidesteps the usual safeguards employed by EMV payments system.
2. Wireless interaction with card. This attack exploits the wireless interface on contactless cards to collect transaction authorisations whilst the card remains in cardholder's wallet. This means the cardholder remains unaware that they have been exploited until their card statement arrives, thereby allowing the attack to operate for longer and be more lucrative to the attackers.
3. Merchant data can be added later. The merchant ID and terminal ID are not part of the data signed by the card in the Application Cryptogram (AC) (Section 5.1.5). This allows the rogue merchant to fill in whatever merchant details they wish onto an already approved transaction.

5. IMPLEMENTATION

To validate our research, we have implemented a number of software elements which demonstrate the viability and practicality of the attack. The software consists of three separate applications:

- An Android mobile phone app which captures transactions from the cards. Transactions are stored on the Android phone to be transmitted to the rogue merchant later.
- A rogue merchant Internet listening service which waits to receive the captured transactions from attackers using the Android mobile phone app.
- A rogue merchant bank communications module which packages the transactions into financial presentment request messages for transmission to the bank. This module handles all of the communication with the bank, which involves sending the financial presentment request messages and receiving acknowledgement messages.

5.1 Android transaction capture app

We have implemented the attack platform on an NFC enabled Android mobile phone as this would be an innocuous device for an attacker to carry around in a crowd.

5.1.1 Attack platform

For implementation and testing, we selected the Google Nexus 5 mobile phone. Implementing on a mobile phone platform limits the effective range to approximately 1 cm. However in testing the Nexus 5 was capable of extracting transactions from an EMV contactless card which was located in a leather wallet in the pocket of a pair of jeans worn by our "unsuspecting" test victim.

5.1.2 Android app operation

The attacker starts by pre-setting the amount and currency for all the transactions which will be captured from the victims cards. Figure 2 shows the attacker setting the amount to 999,999.00 and setting the currency to 0978 which is the code for Euros. In testing we have also obtained transaction approvals in US Dollars for $999,999.99 (currency code 0840).

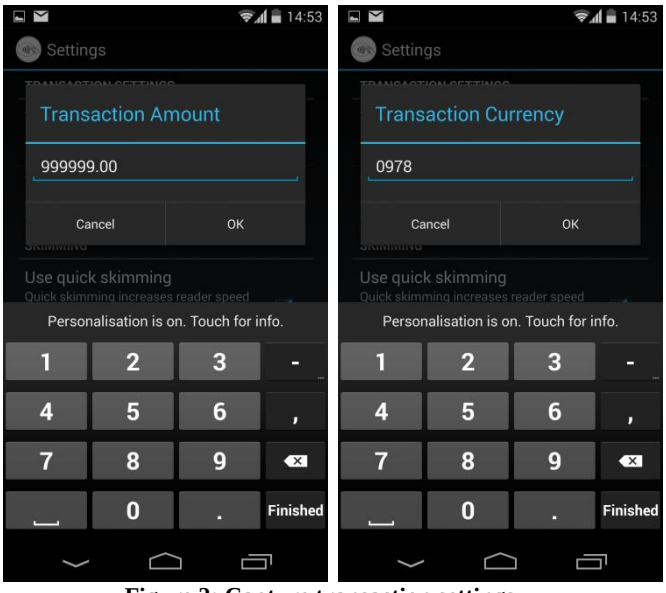

Figure 2: Capture transaction settings

The app is now ready and will automatically collect a transaction from every EMV contactless card that it detects, without any further interaction from the attacker. This will minimise the chance of the attacker being detected, as they are not constantly interacting with their phone.

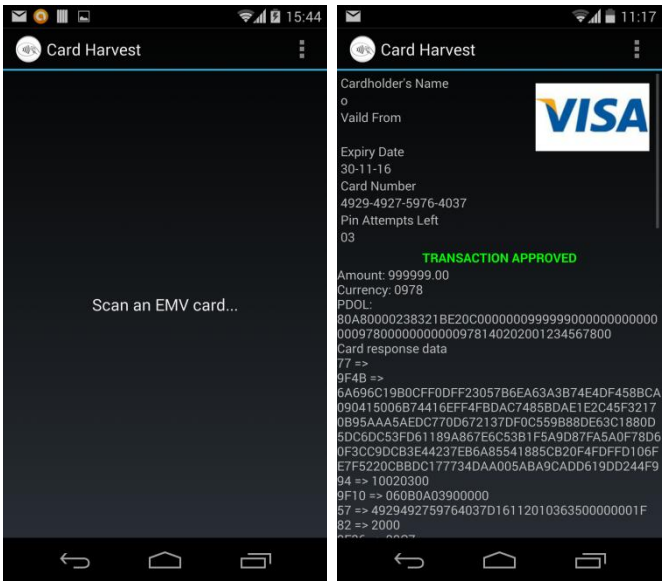

Figure 3: Capturing the transaction

In Figure 3 the first screen shows the app waiting to detect an EMV contactless card. The second screen shows the €999,999.99 transaction being captured from the card.

When the app detects an EMV contactless card, it sounds an audible alert in the attacker's headphones; a second alert is given once the transaction has been successfully collected. This takes less than 500 milliseconds. Once the transaction has been captured the app stores the transaction data for transmission to the rogue merchant later. As soon as the app has collected a transaction it automatically returns to waiting to detect another EMV card is ready to collect the next transaction.

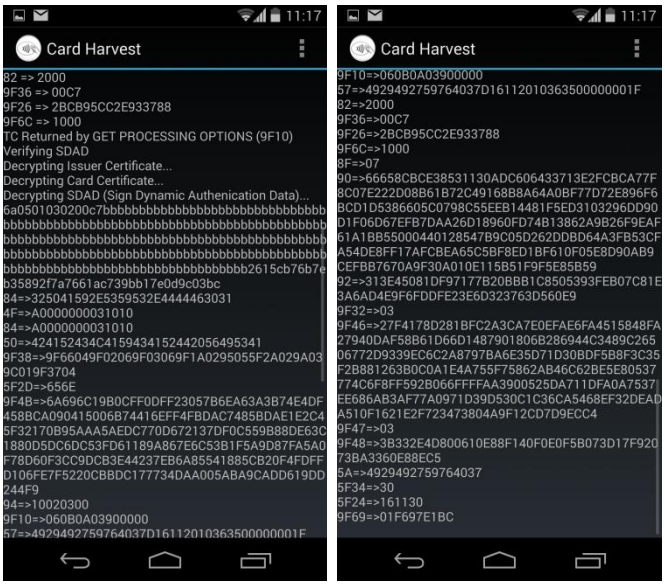

Figure 4: Captured transaction data

Figure 4 shows the data elements as captured by the app, this includes all of the data and cryptographic authorisation codes required by the bank to accept the transaction as genuine.

The mobile app stores transaction data until it has an Internet connection, at which point the app transmits the data to the rogue merchant.

5.1.3 Transaction protocol

The code implements the Visa fDDA [8] contactless transaction protocol sequence as this is an *offline* only contactless protocol. This allows the attack to be performed in less than 500 milliseconds and avoids additional validation by the bank.

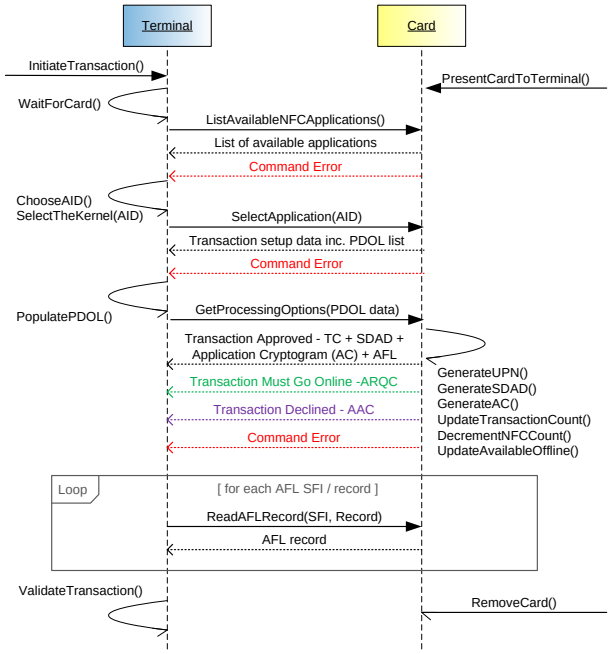

Figure 5: Transaction Capture Protocol Sequence

5.1.4 Storing the transaction data

The transaction data is sent by the card in TAG / Length / Value (TLV) format, the Android application stores all of the data fields returned by the card. The bank requires that the Application Cryptogram (AC) from the card be present in the information sent to the bank.

5.1.5 Application Cryptogram (AC)

When an EMV card approves a transaction, it creates the AC which is an 8 byte MAC code generated from the transaction data. This ensures that the transaction data cannot be altered after the card has approved the transaction and proves to the bank that the transaction has been approved by a genuine EMV card. The following transaction data fields are included in the AC:

- amount authorised (value of the purchase)
- amount other (cashback amount if required)
- terminal country code (UK - 0826, USA - 0840 etc.)
- terminal verification results (POS status code)
- transaction currency code (UK£ - 0826, US$ - 0840 etc.)
- transaction date
- transaction type (purchase - 00, cash - 01, refund - 20)
- unpredictable number (prevents cloned cards)
- application interchange profile (card's security capabilities)
- application transaction counter (card's transaction counter)

Table 1: Financial presentment message data requirements

Item	Name	Description and mapping to EMV card data
1	bit map extended	List of fields included in the message
2	primary account number	0x5A 16 digit card account number. This data is included in the Application Cryptogram (section 5.1.5)
3	processing code	Constant 00 for goods and purchases
4	amount, transaction	0x9F02 the transaction amount. This data is included in the Application Cryptogram (section 5.1.5)
5	amount, reconciliation	Transaction amount 0x9F02 converted into the currency to be applied to the victim's card, this value is calculated by the rogue POS terminal.
7	date and time, transmission	Date and time the rogue POS transmits the transaction to the bank
9	conversion rate, reconciliation	Conversion rate for the reconciliation amount, calculated by the rogue POS terminal.
10	conversion rate, cardholder billing	As above; this value is calculated by the rogue POS terminal.
11	systems trace audit number	Transaction sequence number generated by the rogue POS terminal.
14	date, expiration	0x5F24 – Expiry date of the card (YYMM)
16	date, conversion	Date / time of the currency conversion (same as 7).
19	country code, acquiring institution	Country code of the rogue POS terminal (e.g. 0826 - UK, 0840 USA, 0036 Australia)
20	country code, primary account number	0x5F28 –Country code for the card i.e. 0826 – UK
21	country code, forwarding institution	0x5F28 –Country code for the bank that issued the card i.e. 0826 – UK
22	point of service entry mode	Type of POS terminal, constant value "051" for Chip & PIN / EMV contactless terminals.
23	card sequence number	0x5F34 – Identifies subsidiary EMV cards issued on the same 16 digit account number.
25	point of service condition code	Constant "00" normal card presentment.
26	point of service PIN capture code	Constant "x8xx" indicates a POS terminal that accepts up to 8 digits
27	approval code length	Constant set by acquirer bank
32	acquiring institution identification code	Constant set by acquirer bank
33	forwarding institution identification code	Constant set by acquirer bank, indicates the institution that will provide the card payment clearing (steps 6 to 9 in Figure 1)
34	primary account number, extended	Not applicable top Visa - used only when the primary account number begins with "59"
39	action code (was response code)	Constant "0xx" for financial transaction request messages
43	card acceptor name/location	Constant string name and location of the merchant
49	currency code, transaction	0x5F2A – Currency code of the transaction. This data is included in the Application Cryptogram (section 5.1.5)
50	currency code, reconciliation	Currency code for reconciliation see item 5.
51	currency code, cardholder billing	0x9F42 - Currency Code from the card.
66	country code, receiving institution	0x5F28 –Country code for the bank that issued the card i.e. 0826 – UK
100	receiving institution identification code	Code that identifies victim's bank - ISO 7812
102	account identification 1	Information contained in 16 digit card account number 0x5A.
103	account identification 2	Information contained in 16 digit card account number 0x5A

In the above table data elements from the EMV card data are denoted by their EMV reference number e.g. 0x5A.

The AC is sent to the acquirer bank as part of the Financial Presentment message (see). This allows the bank to verify that the transaction details supplied by the merchant are the same as the transaction approved by the EMV card.

If any of the data fields in the transaction data have been changed, the MAC will be invalid when the acquirer bank checks it.

5.1.6 Transmission to the rogue merchant

Our software can collect and store multiple offline transactions, without a connection to the Internet. The stored transactions can then be transmitted once a suitable connection is available. The transaction details will include all of the data elements required by the bank. Some of these data elements such as the AC are digitally signed by the card to cryptographically protect the transaction (see Section 3.3). The AC is used to by the bank to validate that a genuine EMV card approved the transaction.

5.2 The rogue merchant application

The rogue merchant application consists of three processes:

- an Internet listening service to receive the transactions from the Android transaction capture app
- a data conversion module which converts the EMV data in TLV format into the ISO 8583 / Standard 70 format required by the bank

- a POS terminal emulation which sends the formatted data to the bank to collect the money from the fraudulent transactions

5.2.1 Internet based listening service

This is a simple Internet based service which listens to a pre-agreed IP address and port number. The Android transaction capture app (Section 5.1) connects to the pre-arranged IP address and port number to send all of the collected transactions to the rogue merchant. The listening service stores the transactions for later processing.

5.2.2 Data conversion process

The data conversion process accepts TLV data as captured from the EMV credit / debit card and converts it into ISO8583 / Standard 70 format required by the bank.

To request the money from the victim's account, the rogue merchant must send a financial presentment message (in ISO8583 or Standard 70 format) to the acquirer bank that holds their merchant account.

Table 1 shows the data fields required by the ISO 8583 financial presentment message and shows how the rogue merchant will complete the data fields from the data generated by the EMV card during transaction approval.

5.2.3 POS terminal emulation

Once the financial presentment request message has been generated, it is sent to the acquirer bank to complete the transaction and transfer the money from the victim's bank account into the rogue merchant's account.

In the UK, communications with the acquirer bank over a public IP network must be protected using Secure Sockets Layer/Transport Layer Security (SSL/TLS) or IPSec [5].

The use of standard encryption such as SSL/TLS and/or IPSec allows the rogue terminal to be implemented in Java on a PC platform; no specialist hardware is required.

Table 2 shows the communication sequence required for the POS emulation to transmit a transaction to the acquirer bank.

Table 2: POS / acquirer communication sequence

Message	From ⇨ To	Purpose
financial presentment request message	POS ⇨ Acquirer	Requests approval and money transfer by the acquirer
financial presentment response	Acquirer ⇨ POS	Contains the answer to the request
financial presentment confirmation	POS ⇨ Acquirer	Confirms that the response was received

6. TEST RESULTS

The attack software has been tested against various UK-issued credit / debit cards. Table 3 shows the vulnerability of several different card types.

Table 3: Vulnerability of UK-issued contactless card types

Card Type	Max value	Comment
Visa credit cards (UK currency)	£85.00	Visa credit cards will approve multiple transactions until offline limit reached.
Visa credit cards (foreign currency)	€999,999.99 $999,999.99	Visa credit cards will approve foreign currency transactions up to the maximum value possible in EMV
Visa debit cards (UK currency)	£45.00	Visa debit cards will approve multiple transactions until offline limit reached.
Visa debit cards (foreign currency)	€0.00 $0.00	Visa debit cards decline foreign currency contactless transactions
MasterCard	N/A	MasterCard is not affected by this attack as the cards request online completion of transactions in local currency and foreign currencies

6.1 Transaction capture timings

The Android transaction capture app is designed to operate as quickly as possible, thereby reducing the risk of detection for the attacker. The software automatically collects the fraudulent transaction as soon as it detects a Visa contactless credit or debit card. Table 4 shows analysis of protocol timings from 20 captured fraudulent transactions.

Table 4: Fraudulent transaction capture timings

Statistic	milliseconds
Average transaction duration (card discovery to transaction approval)	478ms
Standard deviation	36ms
Fastest transaction	452ms
Slowest transaction	527ms

7. POTENTIAL SOLUTIONS

The key weakness exploited in this paper is that Visa credit cards will authorise unlimited value transactions in a foreign currency. This makes the attack described in this paper both scalable and very lucrative.

The solution is relatively simple, changing future Visa credit cards to implement one or both of the following:

- the cards will request *online* completion of contactless foreign currency transactions; making the transaction subject to the additional *online* verification steps.
- the cards will force "Chip & PIN" completion of all foreign currency transactions; this will eliminate the possibility of high value transactions without the added security of cardholder's PIN.

8. CONCLUSION

In this paper we have demonstrated that it is possible to collect high value transactions from contactless Visa credit cards whilst the card is still in the victim's pocket. The attack exploits a previously undocumented flaw in the cards, in which the cards

will approve transactions of unlimited value in a foreign currency. Combined with the lack of POS terminal authentication and the threat of contactless payment card skimming, this vulnerability poses a real risk that allows high value fraudulent transaction to be harvested and converted into money.

Our experimental results show that the attack could be implemented in the "real world" as:

- it takes less than 500milliseconds to collect a transaction
- NFC enabled Android phones are cheap and readily available
- the phone looks innocent if the attacker is challenged by the police or a member of the public

We have also outlined a scenario by which the captured fraudulent transactions could be exploited by a rogue merchant to access the money in the victim's bank account. The rogue merchant receives the transactions and passes them off as genuine transactions to their bank. It should be noted that although we have implemented the rogue POS terminal software, we have not tested it against a live acquirer transaction clearing system.

From this we can conclude that this attack represents a plausible threat to contactless Visa credit cards. We can also see that it can be easily remedied.

We have proposed two simple changes in the operation of Visa credit cards that would eliminate the risk posed by this attack. Both of which use the existing functionality of the cards and would therefore be relatively inexpensive to implement.

9. ACKNOWLEDGEMENTS

Our thanks to <removed for blind review> for assisting with some of the Android coding.

10. REFERENCES

[1] Francis, L., Hancke, G., Mayes, K., Markantonakis, K. 2012. Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. *The 2012 Workshop on RFID and IoT Security (RFIDsec 2012 Asia)*, Nai-Wei, L., Yingjiu, L. (editors). Vol. 8, IOS Press (Cryptology and Information Security Series), pp. 21-32. http://eprint.iacr.org/2011/618.pdf

[2] Drimer, S. and Murdoch, S.J. 2007. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. *16th USENIX Security Symposium*, Boston, MA, USA. http://www.cl.cam.ac.uk/~sjm217/papers/usenix07bounding.pdf

[3] Murdoch, S.J., Drimer, S., Anderson, R., Bond, M. 2010. Chip and PIN is Broken. *IEEE Symposium on Security and Privacy*, pp. 433-446. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5504801&isnumber=5504699

[4] Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S., Anderson, R. 2014. Chip and Skim: cloning EMV cards with the pre-play attack. *35th IEEE Symposium on Security and Privacy*. http://arxiv.org/pdf/1209.2531.pdf

[5] Standard 70 - Card Acceptor to Acquirer Interface Standards (2013) - The UK Cards Association Limited.

[6] ISO 8583:1995 - Financial transaction card originated messages — Interchange message specifications (1995) - International Organization for Standardization

[7] EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems - Version 4.3 (2011) http://www.emvco.com/specifications.aspx?id=223

[8] EMVCo – EMV Contactless Specifications for Payment Systems - Version 2.4 (2014) http://www.emvco.com/specifications.aspx?id=21

[9] Reason, J. - *Human Error*, Cambridge University Press (1990).