COMPUTING SCIENCE

The Dangers of Verify PIN on Contactless Cards

Martin Emms, Budi Arief, Troy Defty, Joseph Hannon, Feng Hao and Aad van Moorsel

TECHNICAL REPORT SERIES

No. CS-TR-1332 May 2012

TECHNICAL REPORT SERIES

No. CS-TR-1332 May, 2012

The Dangers of Verify PIN on Contactless Cards

M. Emms, B. Arief, T. Defty, J. Hannon, F. Hao, A. van Moorsel

Abstract

Contactless / Near Field Communication (NFC) card payments are being introduced around the world, allowing customers to use a card to pay for small purchases by simply placing the card onto the Point of Sale terminal. Although the terminal needs to be able to verify a PIN, it is not clear if such PIN verification features should be available on the NFC card itself. We show that contactless Visa payment cards have (largely redundant) functionality, Verify PIN, which makes them vulnerable to new forms of wireless attack. Based on careful examination of the Europay, MasterCard and Visa (EMV) protocol and experiments with the Visa fast Dynamic Data Authentication transaction protocol, we provide a set of building blocks for possible attacks. These building blocks are data skimming, Verify PIN and transaction relay, which we implement and experiment with. Based on these building blocks, we propose a number of realistic attacks, including a denial-of-service attack and a newly developed realistic PIN guessing attack. The conclusion of our work is that implementing Verify PIN functionality on NFC cards has no demonstrated benefits and opens up new avenues of attack.

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

Bibliographical details

EMMS, M., ARIEF, B., DEFTY, T., HANNON, J., HAO, F., VAN MOORSEL., A.

The Dangers of Verify PIN on Contactless Cards
[By] M. Emms, B. Arief, T. Defty, J. Hannon, F. Hao, A. van Moorsel

Newcastle upon Tyne: Newcastle University: Computing Science, 2012.

(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1332)

Added entries

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR-1332

Abstract

Contactless / Near Field Communication (NFC) card payments are being introduced around the world, allowing customers to use a card to pay for small purchases by simply placing the card onto the Point of Sale terminal. Although the terminal needs to be able to verify a PIN, it is not clear if such PIN verification features should be available on the NFC card itself. We show that contactless Visa payment cards have (largely redundant) functionality, Verify PIN, which makes them vulnerable to new forms of wireless attack. Based on careful examination of the Europay, MasterCard and Visa (EMV) protocol and experiments with the Visa fast Dynamic Data Authentication transaction protocol, we provide a set of building blocks for possible attacks. These building blocks are data skimming, Verify PIN and transaction relay, which we implement and experiment with. Based on these building blocks, we propose a number of realistic attacks, including a denial-of-service attack and a newly developed realistic PIN guessing attack. The conclusion of our work is that implementing Verify PIN functionality on NFC cards has no demonstrated benefits and opens up new avenues of attack.

About the authors

Martin Emms is currently studying for a research PhD at Newcastle University's Centre for Cybercrime and Computer Security (CCCS). His research focuses on the potential vulnerabilities in Near Field Communications (NFC) based payment technologies and solutions that can reduce or eliminate these vulnerabilities. The research involves a meticulous examination of the EMV protocol to understand the security mechanisms incorporated into the EMV payment process. It also involves examination of the new payment formats which are currently being released NFC cards, mobile phone payments applications, NFC payment tags and wrist bands.

Budi obtained his Bachelor of Computing Science with First Class Honours from Newcastle University in 1997. He had a one year placement (industrial training) during his undergraduate study with Mari Computer System Ltd. from 1995 to 1996. He went on to study for a PhD at Newcastle University with a scholarship from the School of Computing Science and an Overseas Research Studentship (ORS) from the British Council. He completed his PhD in July 2001 with a thesis entitled "A Framework for Supporting Automatic Simulation Generation from Design". He currently works as a Research Associate at the School of Computing Science. He had previously worked as a Research associate on the TrAmS, TRACKSS, Rodin and DIRC projects, as well as a Teaching Fellow between October 2008 and September 2010.

Troy Defty completed his BSc Computing Science degree at Newcastle University in June 2012.

Joseph Hannon is currently studying towards his MComp Computing Science degree at Newcastle University.

Feng Hao received a BEng (2001) and a MEng (2003) in electrical and electronic engineering from Nanyang Technological University, Singapore, and a Ph.D (2007) in computer science from the University of Cambridge, England. His research interests include biometrics, cryptography, fuzzy search algorithms, information coding, and error correction codes. Feng is currently a Lecturer in Security at Newcastle University.

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

SECURITY ATTACKS
NFC
EMV
VISA
FDDA
CHIP & PIN
SKIMMING
VERIFY PIN
RELAY
PAYMENTS
CREDIT CARD
DEBIT CARD.

The Dangers of Verify PIN on Contactless Cards

Martin Emms Budi Arief Troy Defty Joseph Hannon Feng Hao Aad van Moorsel

Centre for Cybercrime & Computer Security
School of Computing Science, Newcastle University
Newcastle upon Tyne NE1 7RU, UK
+44 191 222 8072

{martin.emms, budi.arief, t.a.j.defty, joseph.hannon, feng.hao, aad.vanmoorsel}@ncl.ac.uk

ABSTRACT

Contactless / Near Field Communication (NFC) card payments are being introduced around the world, allowing customers to use a card to pay for small purchases by simply placing the card onto the Point of Sale terminal. Although the terminal needs to be able to verify a PIN, it is not clear if such PIN verification features should be available on the NFC card itself. We show that contactless Visa payment cards have (largely redundant) functionality, Verify PIN, which makes them vulnerable to new forms of wireless attack. Based on careful examination of the Europay, MasterCard and Visa (EMV) protocol and experiments with the Visa fast Dynamic Data Authentication transaction protocol, we provide a set of building blocks for possible attacks. These building blocks are data skimming, Verify PIN and transaction relay, which we implement and experiment with. Based on these building blocks, we propose a number of realistic attacks, including a denial-of-service attack and a newly developed realistic PIN guessing attack. The conclusion of our work is that implementing Verify PIN functionality on NFC cards has no demonstrated benefits and opens up new avenues of attack.

Categories and Subject Descriptors

C.3 [**Computer Systems Organization**]: Special-Purpose and Application-Based Systems – *Smartcards*; K.4.4 [**Computers and Society**]: Electronic Commerce – *Cybercash, digital cash*, *Payment schemes, Security*; K.4.1 [**Computers and Society**]: Public Policy Issues – *Abuse and crime involving computers.*

General Terms

Economics, Reliability, Experimentation, Security, Human Factors, Legal Aspects.

Keywords

Security attacks; NFC; EMV; Visa; fDDA; Chip & PIN; skimming; Verify PIN; relay; payments; credit card; debit card.

1. INTRODUCTION

Contactless payments are designed to be a quick, convenient and safe card payment method that is an alternative to cash. Often referred to as *Near Field Communication (NFC)* payments, contactless payments are quicker than traditional Chip & PIN payments [12][13][14][15], as there is no PIN entry or signature required from the cardholder to authorize the payment. Since payment can be made simply by placing the card near to the Point of Sale (POS) terminal, it is possible to make a payment by placing the wallet containing the card on the POS, without taking the card out of the wallet. NFC also supports payments made by NFC enabled mobile phones such as Google Wallet [19] and Orange QuickTap [27].

Europay, MasterCard and Visa (EMV), commonly called *Chip & PIN*, is a global payments system deployed across Europe, Asia Pacific, Australia, Canada and Latin America, with a total of 1.5 billion EMV cards and over 21 million EMV POS terminals worldwide [35]. This number stands to increase as Visa intends to introduce EMV to the United States [32].

The introduction of NFC payments has brought a fundamental change to the structure of the EMV protocols. The EMV Chip & PIN specifications comprise a single protocol which covers the operation of all EMV compliant cards and EMV compliant POS terminals. For NFC payments, in addition to the base specification [5][6][11], there are now four versions of the EMV protocol, each of which is specific to one of the major card issuers: JCB [7], MasterCard [8], Visa [9] and American Express [10]. This greatly increases the complexity of the EMV protocol standards which are composed of 700+ pages for EMV Chip & PIN and 1300+ pages for EMV NFC. The increase in complexity and the addition of issuer specific functionality will also increase the potential for anomalies and errors to be introduced.

The implementation work presented in this paper shows that these anomalies translate into concrete security concerns in the operation of contactless Visa credit and debit cards:

1. *Visa NFC Cards Allow PIN Verification over NFC*

   NFC enabled Visa cards issued by Barclays Bank[1] will allow any NFC reader, such as mobile phones and USB readers for PCs, to access the Verify PIN functionality on the card. In one of the attack scenarios presented in this paper we show that criminals can use NFC to probe the card for its PIN number and collect the card details without the knowledge of the cardholder. This seriously compromises the security of the individual cardholder carrying a Chip & PIN as banks have traditionally blamed the customer for being careless with their PIN if a PIN number is entered on a fraudulent transaction.

2. *Relaying NFC Transactions using Mobile Phones*

   The logic which underpins NFC payments is that the cardholder must present their card to the POS terminal to authorize the payment, this is enforced by the practical NFC read range being approximately 4 cm to 10 cm. However, our

[1] Our experiments have been conducted using Visa credit and debit cards issued by Barclays Bank UK, this does not imply that the issue is limited to Barclays issued cards, it is probable that all NFC enabled Visa cards will implement similar functionality

work shows that a Visa *fDDA*[2] transaction (see Figure 3 for details) can be successfully relayed to a payment card at a remote location using two mobile phones, with the card returning a successful transaction authorization. This negates the assumption that the card was present when the transaction was performed and thereby negates the "proximity" element to the security argument for NFC payments. In this paper we present the relay as a means of accessing the Verify PIN functionality on an NFC payment card whilst the cardholder is performing a legitimate NFC transaction.

The operation of NFC enabled Visa cards are controlled by the Visa EMV specification [9], on which this research is based. This implies that many of the cards implemented to this specification will be prone to the vulnerabilities we have identified so far.

In this paper, we present a number of viable attacks on NFC card payments using a combination of NFC data skimming, NFC Verify PIN and NFC transaction relay functionality. There are several goals within the attacks we have proposed: (i) collecting the card details for "card not present" fraud, (ii) probing the card for its PIN number for ATM withdrawals, and (iii) maliciously locking the card. This is all done wirelessly so the cardholder is unaware that their card has been accessed. Moreover, the paper explains the anomalies that we have identified in the EMV contactless specifications. The paper also describes the concrete implementations we have carried out to prove that it is viable to exploit the anomalies. From these implementations, we put forward viable attack scenarios, and finally we discuss the implications of and possible solutions for these anomalies.

2. RELATED WORK

Our previous research into the EMV contactless card payments includes an illustration of a skimming attack on NFC payment card [16], which gathered the card's details (including the card's CVV from the back of the card), and the use of an Android mobile phone to skim the card data whilst still in the victims' wallet [30]. The use of mobile phones as a method of skimming data from NFC card payments has also been documented by RHUL [17] and by a report on the UK Channel4 News [25]. The Verify PIN attack we explore in this paper could easily be incorporated to a skimming attack based on a mobile phone platform or on a hidden NFC reader attached to a PC.

Cambridge University researchers have found – through an online survey – that some PIN numbers are much more likely than others [2]. This could increase the likelihood of guessing the correct 4-digit PIN from 1 in 5000 to 1 in 100. This research is backed up by a recent newspaper report [34] of a burglar in the UK who successfully took out money from two stolen cards by guessing the PIN of the cards using the birthday information on the driving licence found in the same stolen wallet. This poses the possibility of enhancing the attack in the future by taking the birthday information from an NFC enabled ID card or drivers licence, which may also be present in the wallet being scanned.

Royal Holloway University London (RHUL) have carried out NFC relay experiments using mobile phones which relay multiple protocols including card payment transactions [18][20].

Tel Aviv University have published experimental work which shows that the range of NFC can be extended to 25 cm [23]. This raises the possibility of the Verify PIN attack being deployed in a scenario where victims are simply passing through a doorway or turnstile with their wallet in their pocket. Note that the technical challenges involved are significant.

[2] Visa *fast Dynamic Data Authentication (fDDA)* transactions use a new protocol sequence which significantly speeds up the processing of Visa NFC transactions [9].

3. BUILDING BLOCKS

Our approach has been to read the EMV specifications for both the original Chip & PIN transactions and the new NFC contactless transactions meticulously, and to produce a software emulation of a POS terminal which precisely implements the functionality as per the EMV specifications.

From this core understanding of the EMV Chip & PIN and EMV NFC operational functionality, we have designed a number of implementations to validate our understanding that the specification meets the operation of genuine cards and POS terminals. We then proceeded to investigate any anomalies we have observed in the concrete implementations of the functionality of the specification through testing our theories against real payment cards. Finally, we used our implementations to test the cards in unusual modes of operation outside the specification.

The research presented in this paper focuses on the security impact of adding the NFC payment application to existing Chip & PIN cards. Our implementation work has highlighted the following anomalies in the operation of NFC enabled payment cards issued by Visa in the UK:

3.1 PIN Verification Using the NFC Interface

Our experiments show that Barclay Visa NFC cards will support the enciphered Verify PIN functionality on the NFC interface. This functionality enables the attack scenarios we outline later.

Although the Verify PIN functionality is listed in the Visa NFC specification [9], this function is not used in the protocol sequence of the NFC transaction. Authorization is performed by simply placing the card on the reader, i.e. there is no PIN entry required.

Our assertion that Verify PIN is a redundant functionality is supported by experiments on NFC enabled MasterCard cards, which do not support Verify PIN over NFC. Moreover, the MasterCard NFC specification [24] specifically states that "*Offline Personal Identification Number (PIN) is not supported for performance, usability, and security reasons.*"

We looked in the specifications for valid reasons for the functionality to be included, one thought was that it may be to support future mobile phone NFC transactions. However, both Visa and MasterCard have included logic for future support "*consumer devices*" into their respective versions of the EMV contactless specification [8][9], which state that any PIN entry will be performed on the consumer device.

3.2 NFC Transaction Relay using Mobile Phones

Our implementation work proves that it is possible to successfully relay Visa fDDA transactions using two NFC enabled mobile phones. We need a relay because we cannot implement this functionality on one NFC device; we need one phone to communicate with the card and another to communicate with the POS terminal, this is due to the physical operation of NFC transmission. The implementation used our University's WiFi network to transfer commands between the two mobile phones, this allowed us to relay transactions to a credit card located in another room.

The relay technology we have developed can be used as a platform for "man-in-the-middle" attacks [1] on NFC cards where extra commands are inserted into the protocol sequence during the relay process. The EMV protocol was proven vulnerable to the "man-in-the-middle" attack, which changed the protocol sequence to allow transactions to be authorized using an incorrect PIN [26].

The ability to relay transactions takes away one of the fundamental security features of NFC transactions, in that to authorize the payment the cardholder must present the card to the POS terminal (the card has to be placed within 4 cm to 10 cm of the POS terminal). Without this key assumption being true, it follows that it cannot be asserted that the cardholder consented to the transaction.

4. IMPLEMENTATION WORK

We now present the details of our implementation, from which we can construct attack scenarios described later in Section 5.

4.1 Implementation 1 – NFC Card Data Skimming

Our previous work includes skimming the data from payment cards with implementations on Android mobile phones and on the PC platform using USB NFC readers [16].

In these implementations, the data skimmed from the card are the cardholder's name, the card number (PAN), the expiry date, and the start date. A recent news article by Channel4 [25] proves that this data is enough to make fraudulent purchases from some online retailers. The average time to skim all of the data from an NFC payment card is 281 ms (we ran the skimming protocol sequence five times on the same NFC Visa card; the time to execute each sequence was very consistent with a standard deviation of 46 ms).

Skimmed data from the card can then be used in an attack on its own as discussed above, or it cab result in a much more damaging attack when the skimmed data is incorporated into one of the more sophisticated attack scenarios described in Section 5.

4.2 Implementation 2 – NFC Verify PIN

This experiment shows that NFC enabled Visa credit and debit cards issued by Barclays Bank UK will perform the Verify PIN command over the NFC interface – which as NFC transactions do not require PIN entry – is a redundant functionality that can potentially compromise the security of the protocol.

The Visa fDDA transaction protocol used for this experiment is illustrated in Figure 1, which shows the typical sequence of commands being executed for the protocol. These commands include those for opening communication with the card, asking the card to list available applications, selecting the card application, reading the number of remaining PIN attempts, and performing the Verify PIN command. In particular, we need to check the number of PIN attempts remaining before executing the Verify PIN command. Typically, three PIN attempts are allowed, so for our attack, we can perform Verify PIN twice, leaving at least one remaining PIN attempt to avoid locking the cards. This is to avoid alerting the cardholder that he has been attacked.

The average time to execute the whole sequence was 681 ms. If an attacker were to implement an attack such as the one described in Section 5.1, it would be easy to hide this extra time in a standard NFC transaction which can take up to 5 seconds depending on the make and model of the POS terminal.

Interestingly, although the contact Chip & PIN interface of the Barclays Visa cards support Verify PIN using both a plaintext PIN and enciphered PIN, the NFC interface only supports enciphered PIN. Not allowing plaintext PIN to be transmitted over NFC is logical, as a plaintext PIN could easily be captured using the NFC eavesdropping [22] capabilities of products such as the ProxMark3 [28]. However, this raises a question on why would Visa deliberately remove plaintext PIN from their NFC cards, but not completely remove the redundant Verify PIN command from the NFC interface altogether.

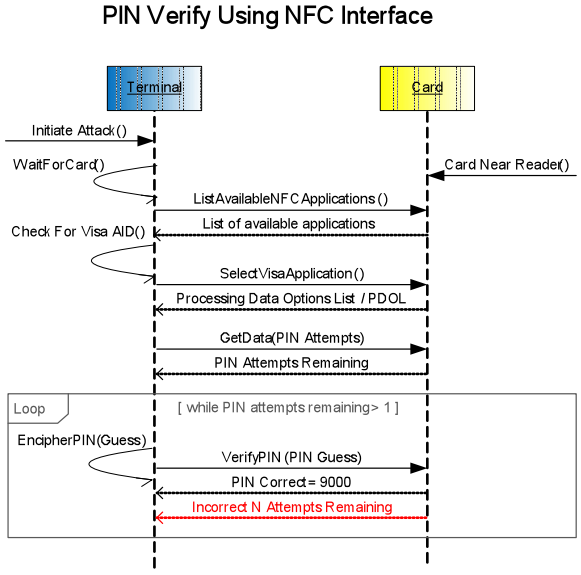

Figure 1. Visa fDDA Transaction Protocol

4.2.1 Denial of Service Attack using NFC

Our implementation of a Verify PIN attack uses the protocol sequence shown in Figure 1, which includes two enciphered PIN attempts in a loop. To implement an attack which denies the use of the card to the cardholder, we simply need to include a third (incorrect) PIN attempt to the sequence, which will result in the card being locked. The average time taken for two PIN attempts is 680 ms. With three PIN attempts, approximately 870 ms is needed to execute the card locking sequence.

The Verify PIN attack has been tested on the Android Galaxy Nexus mobile phone which can read an NFC card, whilst the card is inside a wallet in a trouser pocket [30]. Given that it is possible to block the victim's card in their pocket with a commercially available mobile phone, it is easy to see that this is the kind of attack that could be implemented as a malicious prank, aimed a annoyance rather than commercial gain. Nonetheless, it might be possible for malicious attackers to hold a bank ransom by threatening to upset their customers by locking their NFC cards.

4.3 Implementation 3 – Relaying a Visa fDDA Transaction using Mobile Phones

The process of authorizing an NFC transaction involves the cardholder presenting their card within approximately 4 cm to 10 cm of the POS terminal and holding it there until the POS indicates that authorization has been competed. In this experiment, we relay a Visa fDDA transaction to an NFC card at a remote location with one mobile phone being placed on the card as a *proxy reader* and the other mobile phone being placed on the

POS terminal as a *proxy card*. However, the ability to relay a transaction to a card at a remote location and have the card return a valid authorization code negates the assumption that the cardholder has authorized the transaction.

The relay attack circumvents the functionality within EMV – Dynamic Data Authentication (DDA) – designed to ensure fraudulent transactions cannot take place if the genuine card is not present. This is because the relay attack uses the genuine card to authorize the transaction in real-time.

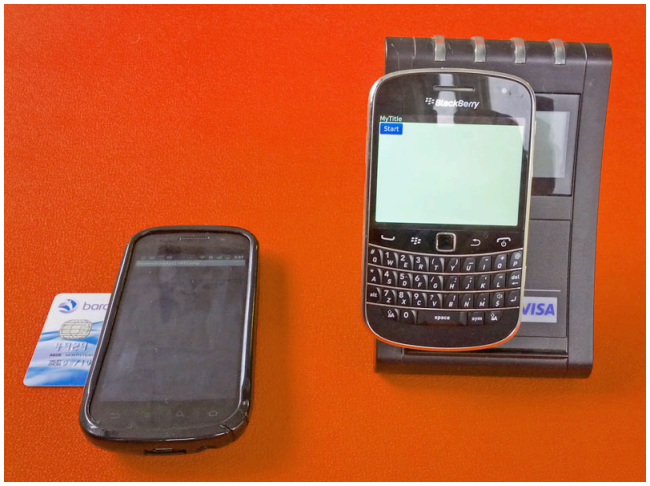

Figure 2. NFC Transaction Relay Using Mobile Phones

Our experiments – along with research carried out at RHUL [18][20] – prove that it is possible to successfully relay NFC payments using *off-the-shelf* equipment, in this case two NFC enabled mobile phones. As depicted in Figure 2, the Blackberry Bold 9900 phone on the right acts as a *proxy card*, receiving commands from the POS terminal and relaying them to the Android Nexus S phone on the left. The Android phone – acting as a *proxy reader* – then passes these commands to the NFC card. In turn, the responses of the NFC card are passed back to the POS terminal through these two phones.

The protocol sequence being relayed in this experiment is the Visa fDDA transaction specified in [9], and detailed in Figure 3. The transaction sequence shown in Figure 3 is initiated by the POS, which specifies the amount, date and currency code of the transaction. The POS terminal waits for a card to be present, and then asks the card to list available applications. The terminal then selects the Visa card application, invoking the Get Processing Options command to pass the details of the transaction to the card, upon which the card returns the signed transaction along with the application cryptogram which signifies that the transaction has been authorized by the card. The POS terminal finally reads the records containing the RSA keys required to check the signed data to complete the transaction. In our experiments, the whole sequence takes 530 ms to execute when the card is directly on the terminal and 1,640 ms to execute when relayed.

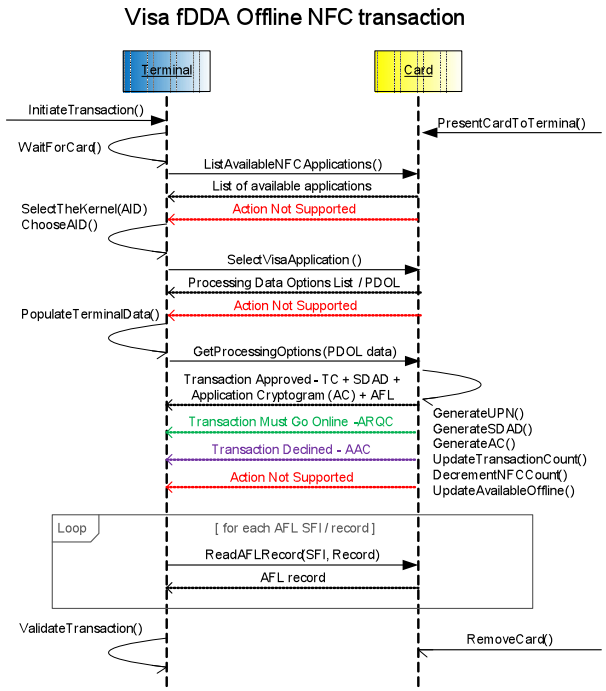

Figure 3. Visa fDDA Protocol Sequence

It can be argued that NFC relay attacks are unlikely as NFC transactions do not require a PIN, so it is much easier just to steal the card. However, this ignores the real threat of the relay attack, which lies in the ability to use it as an enabling platform for other forms of attack. The relay hides the attack by incorporating it into a legitimate transaction. In Section 5 of this paper, we present an example of how the relay can be used to hide the skimming of the card's data, as well as to perform two Verify PIN commands.

Research shows that a relay can be used as the platform for a "man-in-the-middle" attack on EMV transactions [26][3]. As transactions pass through the relay, the "man-in-the-middle" can both record and alter the data, commands or sequence of the protocol being passed between the POS terminal and the card. Although "man-in-the-middle" attacks are limited, due to EMV cards signing the transaction data to prevent it being altered, the control data such as Cardholder Verification Methods (CVMs) are plaintext and can be modified in flight to alter the behavior of the transaction.

4.3.1 Delay Added by the Relay

It is inevitable that a relay will add delays into the protocol sequence. Figure 4 shows the comparative timings for NFC Visa fDDA transaction with the card directly placed on the reader (in blue), compared to the same transaction relayed (in red). Figure 4 also provides details of the average time taken for each command in the sequence, which from left to right follows the sequence described in Figure 3. The timings are taken from the first byte transmitted by the reader to the last byte returned by the card.

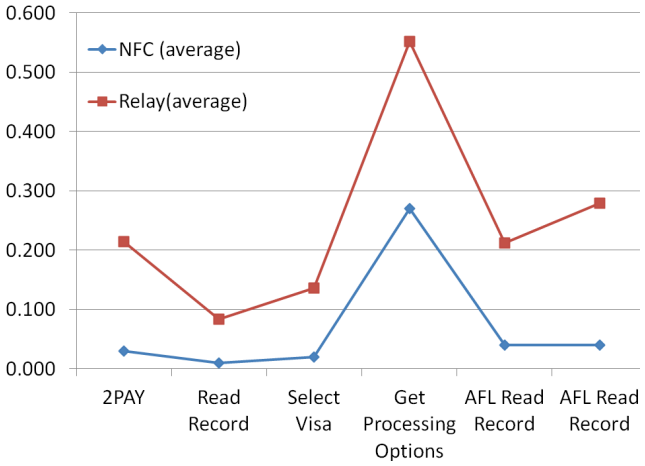

Figure 4. NFC Transaction Command Execution Times[3]

The average total transaction times are 530 ms for the NFC transactions, compared to an average of 1,640 ms for relayed transactions (the relay transaction sequence was executed five times and the standard deviation was 270 ms). Our experiments found that each command in the sequence had an underlying execution time, for example Get Processing Options demands the most processing from the card and therefore takes significantly longer than any other command. The additional network lag evident in the relay results reflects the amount of data returned by each command. Again, it is the Get Processing Options command that returns the most data and therefore has the greatest network lag.

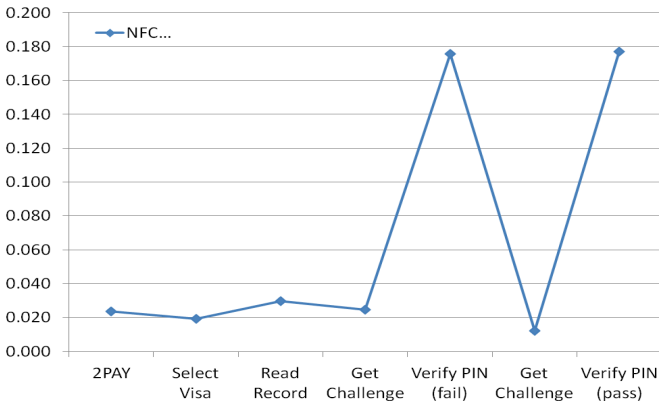

Figure 5. Verify PIN Command Execution Times[3]

In addition to the time taken for the transaction relay, there is also the time required to perform the two PIN attempts. Figure 5 shows the time taken for each command in the sequence described in Figure 1. These commands are: list available card applications, select the Visa card application, read the number of remaining PIN attempts, call Get Challenge for data to encipher the PIN, perform Verify PIN command, call Get Challenge for a new unpredictable number, and perform Verify PIN command.

The average time taken for two PIN attempts (assuming the first attempt is a failure) is 681 ms (we ran the execution sequence five times, the standard deviation was 122 ms). Adding that to the relayed transaction time of 1,640 ms gives an average total time for that attack of 2,320 ms, which is almost five times longer than the 530 ms taken for the standard Visa fDDA transaction. However, this is still well within the 4-5 seconds typically experienced at a normal NFC POS terminal.

[3] The command-response timings are taken from the first byte of the command being sent to the last byte of the card's response being received.

4.3.2 Multi-Protocol Support

In the current implementation, the relay software does not interpret the protocol commands being passed to and fro. This means that the relay is not restricted to the EMV protocol and could be used on many different NFC smart card applications (e.g. Oyster cards). This is also the case for the relay experiments implemented by RHUL [18][20].

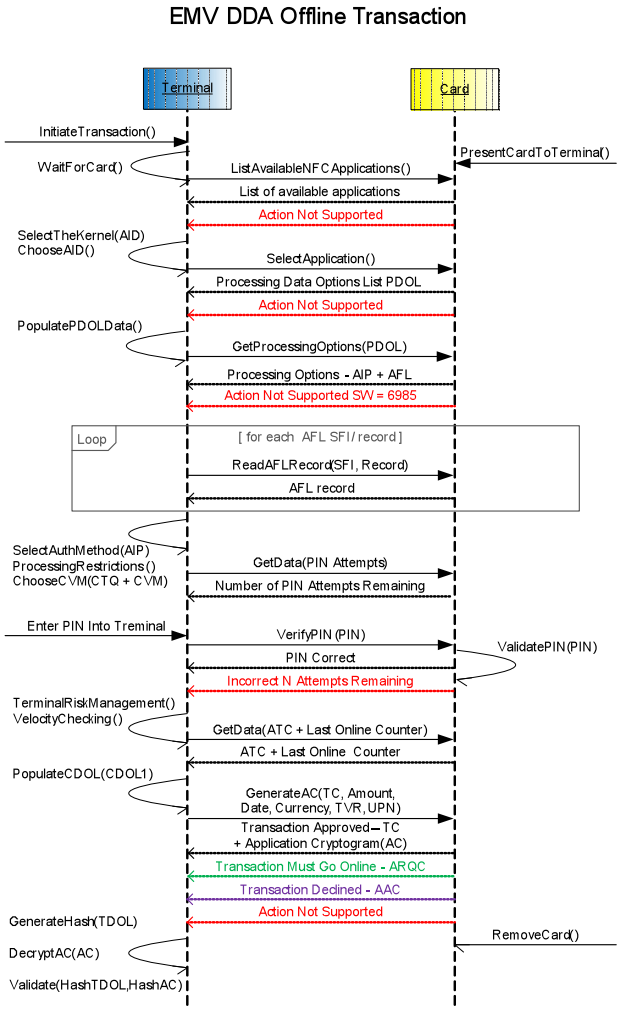

Figure 6. Chip & PIN Transaction Protocol

4.4 Implementation 4 – Ad-hoc Access to Verify PIN Command

As a control experiment, we ran the Verify PIN script used in Implementation 1 on a number of current UK issued non-NFC payment cards. All of the cards tested in this experiment were currently valid credit or debit cards issued by UK banks, and included both Visa and MasterCard branded cards. It was observed that all of the cards tested prevented access to the Verify PIN command, returning "command not supported" message.

The experiment was expanded to execute Verify PIN as part of the Chip & PIN transaction protocol sequence. Figure 6 shows that it is the correct (or intended) usage of this protocol [14]. Each of the cards tested successfully performed the Verify PIN command when it was part of the appropriate command sequence. These results show that EMV payment cards are stateful and are aware of the correct sequence of commands.

Our experiments indicate that it is the Get Processing Options command which initiates the transaction [14] and changes the state of the card, which in turn activates commands such as Verify PIN, Get Challenge and Generate AC which are all used to ensure that the card and the cardholder are genuine before the transaction is authorized.

Our experiment also shows that ad-hoc access to the Verify PIN and Get Challenge commands is allowed on Barclays Visa NFC cards but not allowed by Visa cards without NFC and not allowed by MasterCard both with and without NFC. In particular, the experiment found that only Barclays Visa NFC cards would perform Verify PIN and Get Challenge commands out of sequence.

These findings indicate that Visa NFC cards have relaxed some of the security features in existing Chip & PIN cards that prevent access to secure functionality of the card.

5. ATTACK SCENARIOS

In this paper, we present attack scenarios that take advantage of the NFC data skimming functionality, NFC Verify PIN functionality, and NFC relay functionality described above. The objectives of these scenarios are (i) to skim the data from the card, (ii) to obtain the card's PIN number, (iii) to hide the attack from the victim by hiding it in a real transaction, and (iv) to maliciously lock the card.

5.1 Scenario 1 – Pay & Display Attack

The scenario we present is an NFC enabled *"Pay & Display"* parking machine serving a large car park. This attack scenario depends on a high volume of people with NFC enabled credit and debit cards visiting an unfamiliar location, which is exactly the type of situation that will occur in London at the 2012 Olympic Games. The situation is compounded by the marketing push for the introduction of many new NFC cards, NFC mobile phones and NFC POS terminals centered on the Olympics, which could mean that there will be a lot of cardholders and merchants who will be unfamiliar with the correct operation of NFC.

In order to attack an NFC payment card, the card must pass within 4 cm to 10 cm of a malicious NFC reader and remain in range for a few seconds. The easiest way to achieve this for large numbers of cards, without the cardholders becoming suspicious, is to incorporate the PIN attempts into a situation where the cardholder is presenting the card for a legitimate transaction, such as paying for car park fee.

5.1.1 Situation

We have highlighted *"Pay & Display"* parking meters as a potential attack scenario for the following reasons: (i) a large busy car park will produce the volume of NFC card reads, (ii) the machine is unattended, which allows the criminals to attach the malicious NFC relay to the parking machine, (iii) the false front required to hide the attack equipment would be similar to current cash machine skimmers, and (iv) NFC parking meters have been piloted in the UK [33].

5.1.2 Technology

The attack consists of three elements:

- a proxy reader (an Android Nexus S phone), which will communicate with the victim's card,
- a proxy card (a Blackberry 9900 phone), which will relay the commands from the parking machine to the Android phone,
- a convincing false front for the parking meter, behind which the two NFC mobile phones will be mounted.

Figure 7. Parking Machine Attack

5.1.3 The Attack Sequence

The sequence for the attack in Figure 7 would be as follows (the numbers in the list refer to the numbers in Figure 7):

1. The sequence is triggered by the victim presenting their NFC enabled card to the parking machine.
2. Behind the false front Android Nexus S detects the card and initiates the protocol.
3. The Android phone will interrogate the card to find out how many PIN attempts are remaining.
4. The Android phone will attempt to guess the PIN number of the card making as many guesses as it can without locking the card, the victim is left with one valid PIN attempt.
5. If the PIN is guessed correctly (see Section 5.1.4) the Android phone will send an SMS to a nearby attacker to alert them that the person currently at the parking machine has a known PIN and should be followed to a convenient location to be mugged for their card (Section 5.1.5).
6. The Android phone signals to the Blackberry 9900 that it is ready for the real transaction.

7. The Blackberry switches on NFC emulation and the parking machine's POS terminal will initiate a transaction.
8. The Blackberry relays commands from the POS terminal to the Android phone, which then passes them directly to the card.
9. The Android phone relays the card's responses to the Blackberry, which sends them to the POS terminal.
10. When the transaction is complete the parking machine will produce the ticket and the victim leaves unaware that anything abnormal has occurred.

5.1.4 PIN Guessing

Recent research by Cambridge University [2] based on a survey of real 4-digit PIN numbers in use on bank cards to plot a distribution of PIN numbers *"in the wild"* reveals two key facts that make Scenario 1 a viable attack. First, PIN numbers are much more predictable than 1 in 9999. The distribution showed that there is a list of the more popular PIN numbers, from which the Cambridge team calculated a 1.44% chance of guessing a correct PIN within three attempts when using their "most popular" list derived from the distribution, which equates to guessing the PIN correctly for one in every 69 cards. Second, the survey results show that 39.8% of respondents carried multiple cards in their wallet and of those, 34.3% used the same PIN on several cards. This works out at 13.69% of wallets yielding multiple cards with the same PIN.

The Cambridge research only gives probability of guessing the correct PIN for three PIN attempts of 1.44% and six pin attempts of 1.94%. Our attack uses two PIN attempts, so we are estimating a success rate of 1.00% (1 in 100 cards). This would be more than enough to make the attack worthwhile.

A recent court case [34] reinforces the Cambridge findings, as a burglar was able to correctly guess the PIN number of two stolen bank cards by trying the birth date from the driving license he had also found with the cards.

5.1.5 Pay Off

Once criminals have the victim's PIN, they need the card to go with it. This would probably mean pick pocketing or mugging the victim at a location far enough away from the parking machine so as not to produce a crime cluster around the car park. If the victim has multiple cards, the Cambridge research [2] also shows that the same PIN should be attempted on the other cards as there is a good possibility that they will have the same PIN.

For every PIN guessed correctly, there will be many cards which were read but not guessed correctly. Nonetheless, the criminals can still gain from these failed attempts. Our earlier experiments [16] show that it is easy to skim the details required for "*Card Not Present"* fraud from an NFC card. The 16-digit card number, the customer name and the card expiry date would be collected as a by-product of the PIN guessing and relay activities. "*Card Not Present"* fraud is the term given to over the telephone or online fraudulent transactions; it is responsible for 65% (£ 221 million) of UK card fraud losses in 2011 [31]. The value of this data was highlighted by a recent UK news report where NFC skimmed data was used to buy goods on the Amazon site where no CVV[4] was required to authorize the transaction [25]. Therefore, this data can be either used to attempt to purchase goods directly or can be sold on as large list of credit card details.

[4] Card Verification Value (CVV) is a 3-digit code printed on the back of the card required in Card Not Present transactions to prove that the customer is in possession of the genuine card.

5.2 Scenario 2 – Lost in the Mail

Consider a situation where a rogue mail employee uses an NFC enabled mobile phone to scan all of envelopes containing the credit and debit cards that pass through their hands. The rogue employee keeps the envelopes where the PIN is guessed correctly and lets the other cards continue on into the system to be delivered to the cardholder. The cards with correctly guessed PIN numbers can then be used to make ATM withdrawals.

The rogue employee would probably be found relatively quickly if they were a local delivery person as their activity would produce a recognizable cluster of lost cards. However, we envisaged this attack taking place in a distribution center where there would probably be a better chance of avoiding detection, making the risks worthwhile. Note that there is no relay technology required for this attack, just the Verify PIN implementation on the NFC enabled mobile phone.

5.3 Scenario 3 – Door Entry Systems

People entering a building with an NFC door entry system usually hold their entire wallet up to the reader to gain access. The wallet contains the door entry card but may also contain one or more NFC payment cards. This is a dangerous attack scenario as people use the same door reader day after day, giving the attack many chances to guess the PIN; the person entering the building would be completely unaware that the NFC payment card had been accessed as it does not leave their wallet.

Further consideration of this attack shows it to be technically difficult with currently available *off-the-shelf* NFC readers. Nonetheless, this may improve in the future with better readers and software. The technical challenges involved here are in distinguishing between and communicating with two or more cards, as well as dealing with the constraints that door entry systems operate much faster than NFC payments (typically less than a second), giving little time to add extra commands.

6. DISCUSSION

Why have Visa included the Verify PIN functionality on NFC?

Our implementation work indicates that Visa have removed plaintext Verify PIN using NFC but included enciphered Verify PIN using NFC, even though NFC transactions do not require PIN entry. The Visa contactless specification [9] describes the Verify PIN function but does not include the command in the transaction protocol sequence. Therefore a question arises on why Visa have included an apparently redundant functionality which is a potential security risk.

It does not appear that this is an oversight in the implementation as Visa have removed plaintext Verify PIN which could be picked up by an NFC eavesdropping device but left in the enciphered Verify PIN functionality which is safe from eavesdroppers.

MasterCard seem to have taken a different view on the operation of their NFC cards, stating "Offline Personal Identification Number (PIN) is not supported for performance, usability, and security reasons" [24].

The obvious assumption is that Visa have a future use for the Verify PIN functionality, however we have not found any reference to it in the currently published documentation.

Our analysis of this issue leads to the conclusion that Verify PIN is a potentially dangerous redundant functionality which should be removed from Visa NFC cards.

6.1 Discussion of the Verify PIN attack

In the future, the PIN guessing attack could be improved in cases where the victim's date of birth might be available from one of the other NFC cards in their wallet [34]. This does not have to be a driving license (which is likely to be protected with sufficient security measures); it could be an NFC library card, an NFC gym card or an NFC loyalty card.

We have also considered the implications of the growing use of NFC cards for multiple different applications (such as door entry, transport systems, and library cards) and human factors which influence the way in which we use NFC cards. Our conclusion is that the most dangerous situations are those where people present their wallet full of NFC cards to a reader and let the reader decide which NFC card it wants to read. The individual is completely unaware of which cards have been accessed and what data has been read.

Our experimental work [16] utilizes a PC platform with more powerful NFC readers than is available on the mobile phone. The more powerful readers give a faster, more reliable read of multiple cards within a wallet presented to the reader, which would facilitate the development of more complex attacks such as reading other cards to find a birthday and trying combinations of that for the PIN number.

6.2 Discussion of the Relay Attack

The implementation of a relay attack using the Android and Blackberry mobile phones produced a reliable attack platform for the Verify PIN attack and would be a suitable vehicle for *man-in-the-middle* attacks.

The relay is also a suitable vehicle for many other attack scenarios as it allows a genuine transaction to proceed, thereby reassuring the victim that nothing unusual has occurred.

The protocol transfer delays introduced by the relay are significant – 1,640 ms for a relayed fDDA transaction as opposed to 530 ms for the same transaction without the relay. However, this should not be too much of an issue as (i) the relayed time is still well within the 4 to 5 seconds transaction time of an NFC transaction at a POS; (ii) to avoid or minimize rejected transactions, it is not in the interest of the EMV specification to enforce strict response times.

Implementing stricter timing constraints and distance bounding [4][29] are methods via which the POS terminal could detect and possibly prevent the relay. However, a key element of the EMV protocols is the interoperability of POS terminals and cards from different manufactures and different countries, ensuring that transactions are successfully captured from the first attempt; implementing tighter restrictions would affect interoperability, possibly causing a lot of valid cards to be rejected.

Research into the timing constraints enforced by Chip & PIN terminals [4] proves, from relay experiments carried out on live terminals, that POS will tolerate very high latencies. The research also suggests that the relay can make it appear as if the card is responding more quickly by sending certain commands in the protocol sequence before the POS requests them and pre-recording the card's responses. The unpredictable number in the Get Processing Options (GPO) prevents this command from being pre-sent and replayed, however in the Visa fDDA transaction, the card signs its response using RSA cryptography, which takes some time, so the POS terminal is expecting a lengthy delay, in our experiments 270 ms from the first byte of the GPO command being sent to the last byte of the card's response being received.

A relay attack could also take advantage of the ISO 14443 protocol negotiation process, as described in [20], which allows the card to set the timeout value for its own responses. This would allow the Blackberry phone in the attacking relay to set the timeout to 5 seconds allowing plenty of time for the relay.

A distance bounding protocol is a more sophisticated technique of protecting against relay attacks. It utilizes cryptographic challenge-response timings [21] to accurately measure the distance between the card and the reader. However, it is the additional sophistication of this technique, which would add a new protocol layer into EMV contactless transactions, that would make it too expensive to implement given the number of EMV cards and EMV POS terminals worldwide [35].

6.3 Discussion of Ad-hoc Access to Verify PIN Command

Within the Visa specification of the new fDDA NFC payments protocol, there is an underlying requirement for speed, illustrated by the following excerpt taken from [9] *"10.1 Card in Field - The primary requirement is the maximum time that a card must be present in the reader field when presented for a single presentment. This is a maximum of 500 ms (0.5 seconds)…"*

Table 1. Comparing EMV and fDDA Transaction Sequences

EMV Offline Transaction Sequence [14 pp. 84]		Visa fDDA Transaction Sequence [14 pp. 134]	
1	Card detected in POS	1	Card detected by POS
2	Select card application Select()	2	Select card application Select()
3	Initiate Transaction Get Processing Options()	3	Authorize Transaction Get Processing Options()
4	Read the card data Read Record()	4	Card authorizes transaction
5	Check processing restrictions of card	5	Read the card data Read Record()
6	Customer enters PIN or signature to verify Get Challenge() Verify PIN()	6	Card can be removed from the POS
7	Pass the transaction details to card Generate AC()	7	POS verifies the card's authorization
8	Card authorizes transaction	8	Check processing restrictions of card
9	POS verifies the card's authorization		
	Card can be removed from the POS		

This focus on speed is driven by the need to successfully complete the transaction before the card is removed from the NFC field. In the Visa NFC fDDA transaction protocol, this has lead to a reversal of the normal EMV sequence, the table below gives a

comparison of the equivalent EMV offline DDA[5] protocol sequence with the new Visa fDDA protocol sequence.

In the comparison shown in Table 1 above, step 3 in the EMV Offline and Visa fDDA NFC transactions uses the Get Processing Options (GPO) command in slightly different ways. In the EMV transaction, this command signals to the card that a transaction is starting, whereas in the NFC transaction, it is used as the request to authorize the transaction. This change of functionality in the GPO command is a likely explanation for Visa NFC cards allowing ad-hoc access to the Verify PIN functionality, the other cards tested in our experiments only allowed Verify PIN to be called after the GPO command had been called.

6.4 Potential Solutions

In this section, we discuss potential solutions to the issues raised in this paper. This discussion is bounded by the understanding that any changes to EMV will have a large impact due to the large number of EMV payment cards and POS terminals deployed worldwide. Moreover, changes can affect a number of parties: card issuers (Visa, MasterCard, American Express and JCB), the issuing banks (Barclays, HSBC, Royal Bank of Scotland etc.) and the companies who manufacture the POS terminals.

6.4.1 Solution(s) for Visa NFC Verify PIN

The specification for Visa NFC transactions does not require the Verify PIN functionality on the card, therefore this issue could be resolved if Visa removes the Verify PIN functionality from the NFC interface.

In this case, the changes would be restricted to the software on Visa NFC cards; the POS terminals and backend bank software would remain the same. The cost of the changes could be minimized especially if done when cards are replaced when they are due (e.g. approaching expiry date), rather than a complete reissue for every cardholders.

6.4.2 Solutions(s) for NFC Card Details Skimming

Criminals are focusing on *"Card Not Present"* fraud, which has grown from 23% of all card fraud losses in 2001 to 65% in 2011 [31]. There are two security measures designed to prevent this kind of fraud. First, the usage of the CVV printed on the back of the card, which is mandatory for all online and telephone transactions. Second, there are optional schemes such as Verified by Visa, where the website asks for an additional preauthorized pass-code.

Unfortunately, investigations carried out by a UK Channel4 News [25] revealed that one of the largest online retailers, Amazon, was not implementing the basic CVV check, thereby making the card details skimmed from NFC cards much more valuable.

The same Channel4 News report suggested that the data on the NFC cards should be encrypted to protect it from criminal hackers. However this would not be practical for two reasons: (i) the RSA encryption used by EMV cards and POS terminals is publicly documented [13], so a malicious programmer could easily create the algorithms for encryption and decryption of EMV data, and (ii) this would require major changes to all of the EMV cards and POS terminals around the world, which would be too expensive.

A possible solution would be to make the PAN[6] available on NFC different from the PAN printed on the front of the card and only valid for NFC transactions, thereby making NFC skimmed data worthless in *"Card Not Present"* transactions. Changing the NFC PAN to be different from the PAN printed on the front of the card would stop data skimmed from NFC cards being used in "Card Not Present" transactions.

7. CONCLUSION

In this paper we have presented implementation work and research into attack scenarios, which together make a compelling case for attacks combining NFC data skimming, NFC Verify PIN and NFC transaction relay to be a profitable activity for criminals.

In our implementation work, we have successfully built and tested mobile phone and PC applications which prove that the attacks scenarios described in this paper are technically viable.

Our key findings suggests that it would seem prudent for Visa to remove the Verify PIN functionality from their NFC cards as it is not used for the correct operation of contactless transactions.

In the broader context of electronic payment, the magnetic strip is the most vulnerable interface included on EMV credit and debit cards. Magnetic strip reader technology is cheap, simple to implement and attackers have achieved considerable experience and success in exploiting it. The process of phasing out the magnetic strip has recently moved forward with Visa and MasterCard announcing that they will switch from magnetic strip to Chip & PIN in The United States by 2015 [32]. After magnetic strip is removed, NFC will be the most obvious way to attack payment cards because of its wireless interface. Therefore resolving any security issues in NFC will be a high priority in the immediate future.

8. ACKNOWLEDGMENTS

Mike Bond and Ross Anderson for their help in formulating ideas for different attack scenarios. Nicholas Little for his coding work on the POS terminal emulator.

9. REFERENCES

[1] Anderson, R. 2007. RFID and the Middleman. *Financial Cryptography and Data Security* (2007), 46-49.

[2] Bonneau, J. and Anderson, R. 2012. A birthday present every eleven wallets? The security of customer-chosen banking PINs. *International Conference on Financial Cryptography*.

[3] Choudary, O.S. 2010. The Smart Card Detective: a hand-held EMV interceptor. Cambridge.

[4] Drimer, S. and Murdoch, S. 2007. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. *USENIX Security Symposium*.

[5] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book A - Architecture and General Requirements.

[6] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book B - Entry Point Specification.

[5] Dynamic Data Authentication is a method by which EMV offline transaction can be securely authenticated by the card using its Private Key and the POS can verify the authentication using the card's Public Key.

[6] Primary Application Number (PAN) is the 16 to 20 digit number on the front of the card which uniquely identifies the card and the account to which the card has been issued.

[7] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book C-1 - Kernel 1 (JCB).

[8] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book C-2 - Kernel 2 (MasterCard).

[9] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book C-3 - Kernel 3 (Visa).

[10] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book C-4 - Kernel 4 (American Express).

[11] EMVCo. 2011. EMV Contactless Specifications for Payment Systems Book D - Communication Protocol Spec.

[12] EMVCo. 2008. EMV v4.2 ICC Specifications for Payment Systems Book 1 - Application Independent ICC to Terminal Interface Requirements.

[13] EMVCo. 2008. EMV v4.2 ICC Specifications for Payment Systems Book 2 - Security Key Management.

[14] EMVCo. 2008. EMV v4.2 ICC Specifications for Payment Systems Book 3 - Application Specification.

[15] EMVCo. 2008. EMV v4.2 ICC Specifications for Payment Systems Book 4 - Cardholder, Attendant and Acquirer Interface Requirements. Interface.

[16] Emms, M. 2011. Practical Attack on Contactless Payment Cards. *HCI2011 Workshop - Heath, Wealth and Identity Theft.*

[17] Francis, L., Hancke, G., Mayes, K. and Markantonakis, K. 2009. Potential Misuse of NFC Enabled Mobile Phones with Embedded Security Elements as Contactless Attack Platforms. *International Conference for Internet Technology and Secured Transactions*.

[18] Francis, L., Hancke, G., Mayes, K. and Markantonakis, K. 2011. Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. *eprint.iacr.org/2011/618.pdf*. Accessed: 2012-05-04.

[19] Google Wallet - How It Works. 2012. *http://www.google.com/wallet/how-it-works.html#in-store.* Accessed: 2012-04-27.

[20] Hancke, G. 2005. A Practical Relay Attack on ISO 14443 Proximity Cards. Technical report. University of Cambridge Computer Laboratory. (January 2005), 1-13.

[21] Hancke, G., Mayes, K.E. and Markantonakis, K. 2009. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*. 28, 7 (Oct. 2009), 615-627.

[22] Hancke, G.P. 2008. Eavesdropping Attacks on High-Frequency RFID Tokens. *Workshop on RFID Security (RFIDSec)*, 100-113.

[23] Kirschenbaum, I. and Wool, A. 2006. How to Build a Low-Cost, Extended-Range RFID Skimmer. *15th USENIX Security Symposium*.

[24] MasterCard 2008. PayPass - M/Chip Acquirer Implementation Requirements.

[25] Millions of Barclays Card Users Exposed to Fraud. 2012. http://www.channel4.com/news/millions-of-barclays-card-users-exposed-to-fraud. Accessed: 2012-03-23.

[26] Murdoch, S., Drimer, S., Anderson, R., and Bond, M. 2010. Chip and PIN is Broken. *2010 IEEE Symposium on Security and Privacy*, 433-446.

[27] Orange QuickTap. 2012. http://shop.orange.co.uk/mobile-phones/contactless/overview.jsp. Accessed: 2012-04-27.

[28] ProxMark3 User Manual. 2011. http://code.google.com/p/proxmark3/wiki/HomePage.

[29] Rasmussen, K.B. and Capkun, S. 2010. Realization of RF Distance Bounding. In *Proceedings of the USENIX Security Symposium*.

[30] Secrets and Lies demonstrations. 2012. http://cccs.ncl.ac.uk/secrets-and-lies-event.

[31] UK Payments Administration. 2012. Fraud The Facts. http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/. Accessed: 2012-05-04.

[32] Visa Pushed EMV in the United States. 2012. http://video.cnbc.com/gallery/?video=3000071991&play=1. Accessed: 2012-04-11.

[33] Wave and Pay parking comes to the UK. 2009. http://www.parkeon.com/uk/wave-and-pay-parking-comes-to-the-uk.html. Accessed: 2012-05-04.

[34] Willey, G. 2012. PIN Number burglar used victims' card. *Newcastle Evening Chronicle* 2012-04-27.

[35] Worldwide EMV Deployment. 2011. http://www.emvco.com/about_emvco.aspx?id=202. Accessed: 2012-04-11.