Practical Attack on Contactless Payment Cards

Martin Emms
School of Computing Science
Centre for Cybercrime & Computer Security
Newcastle University, NE1 7RU
martin.emms@newcastle.ac.uk

Aad van Moorsel
School of Computing Science
Centre for Cybercrime & Computer Security
Newcastle University, NE1 7RU
aad.vanmoorsel@newcastle.ac.uk

This paper describes a potential attack on EMV contactless payment cards which is low cost, high return and relatively easy to implement. This could have a serious impact on the security of EMV cards because it requires little investment or expertise to carry out successful card fraud, leading to more attacks being attempted. 3D Secure payment authentication addresses the issue, but will only resolve it once all websites are protected by 3D Secure. This paper proposes a low cost solution to address the vulnerability, in which contactless payments cards would only be active when the cardholder wants to make a payment.

EMV, NFC, RFID, Contactless Payment, Credit Card, Debit Card, Security, Chip & PIN, 3D Secure.

1. INTRODUCTION

The intention of this paper is to highlight a potential vulnerability in the new contactless payments system and to propose a workable / low cost solution that addresses the issue.

The most disturbing feature of the attack described in this paper is that it is low tech, low cost and relatively easy to implement. The simplicity of the attack is what makes it both accessible and attractive to criminals.

2. RELATED WORK

Research [2][3][4] into the vulnerabilities of the EMV payments system show that it is relatively difficult to attack the contact chip on EMV cards. The vulnerabilities identified require sophisticated modifications to be made to Chip and PIN terminal [4] or the creation of sophisticated bespoke electronics [2] [3]. The introduction of NFC payments to the EMV system opens new avenues of attack that do not require physical contact with the card and can be implemented using off-the-shelf technology, making possible relatively simple attacks such as the one identified in this paper.

3. UK CARD FRAUD

Since the UK introduction of EMV Chip & PIN payments technology in 2004 the incidence of card fraud has steadily risen, however it remains relatively low when viewed as proportion of the rapidly increasing number (and value) of card transactions [1].

3.1 Changing Profile of Card Fraud

The security features built into EMV may not have eradicated card fraud but they have forced significant changes in the types of card fraud being committed.

The card fraud statistics [1] show a reduction in simple over the counter card fraud, where criminals attempt to use lost, stolen or cloned cards in retail shops (down 67% between 2004 and 2009). At the same time there has been an increase in more sophisticated forms of card fraud, such as card-not-present fraud (up 77%) and UK cards which have been cloned for use in overseas transactions (up 33%).

<table>
<thead>
<tr>
<th>Category of Fraud</th>
<th>2004</th>
<th>2009</th>
<th>Chg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overseas Transactions</td>
<td>£92.5m</td>
<td>£122.7m</td>
<td>33%</td>
</tr>
<tr>
<td>Card Not Present</td>
<td>£150.8m</td>
<td>£266.4m</td>
<td>77%</td>
</tr>
<tr>
<td>Over the Counter</td>
<td>£218.8m</td>
<td>£72.1m</td>
<td>-67%</td>
</tr>
<tr>
<td>Counterfeit / Cloned Cards used in the UK</td>
<td>£129.7m</td>
<td>£80.9m</td>
<td>-38%</td>
</tr>
<tr>
<td>Lost &amp; Stolen Cards</td>
<td>£114.4m</td>
<td>£47.9m</td>
<td>-58%</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>£36.9m</td>
<td>£38.2m</td>
<td>4%</td>
</tr>
<tr>
<td>Card Not Received in the Mail</td>
<td>£72.9m</td>
<td>£6.9m</td>
<td>-91%</td>
</tr>
</tbody>
</table>

Table 1: UK Card Fraud by Category source FFA [1]

3.2 Criminal Sophistication

Proof of the current level of sophistication of criminal gangs can be seen in news reports of card fraud attacks in the UK [5] criminals posing as repair engineers in order to replace legitimate Chip & PIN terminals in unsuspecting shops [6] gangs recruiting members of staff in shops and petrol filling stations to replace Chip & PIN terminals [7] gangs building skimming devices which fit over the top of legitimate ATM machines.

4. CONTACTLESS PAYMENT TECHNOLOGY

The introduction of any new payments technology potentially introduces new weaknesses for the criminals to exploit; contactless payments cards are no different in this respect.

4.1 Exploitable Weakness

The specific weakness exploited in this demonstration is that the contactless cards will divulge the (i) card number

---

1 EMV (Europay, Mastercard, Visa) is a standard for credit card and debit card payments
2 3D Secure implementations Verified by Visa™, MasterCard SecureCode™ and American Express SafeKey™.
(ii) cardholder name (iii) expiry date (iv) issue date, unencrypted to any NFC reader that requests the data. This is not an error, the functionality is fully compliant with the EMV specification for contactless cards. It is assumed that the maximum read range of 10cm makes it difficult to get close enough to read the card without arousing suspicion. This assumption is incorrect.

5. THE DEMONSTRATION

The demonstration is a mock-up of a counter top on which a Chip & PIN terminal has been set up to accept legitimate payments from EMV cardholders. It replicates the design of counters found in many UK filling stations and shops, with a display area for sweets immediately adjacent to the Point Of Sale.

![Point Of Sale mock-up with EMV terminal](image)

**Figure 1:** Point Of Sale mock-up with EMV terminal

5.1 Reading the Card Details

A hidden NFC reader has been set up to capture the details of any contactless card which is inserted into the EMV Chip & PIN terminal. Data capture takes place before card is fully inserted into the terminal so it does not affect the legitimate Chip & PIN transition.

5.2 Capturing the 3 Digit CVV

The 3 digit CVV (Card Verification Value) printed on the back of the card is required to make telephone and/or online purchases. The demonstration captures the CVV using a hidden camera, this technique was selected as it is low cost, easy to implement and it is technology that the criminals are already using in their current attacks.

5.3 High Value Return

The aim of the attack is to capture the data required to purchase high value (easy to resell) items online. Many websites will allow the customer to specify a delivery address which is different from the cardholder address registered with the bank (gifts for friends and family), this allows the criminals to receive the stolen goods without raising suspicion. The £15 transaction limit which is designed to protect contactless cards does not apply as the data is being used to make online purchases.

5.4 Low Cost and Easy Implementation

The demonstration uses a £50 off-the-shelf NFC reader, and a £10 USB camera. All of the software used is either GNU licence or adapted from online source code examples, which are readily accessible to anyone.

5.5 3D Secure Authentication

The major credit card companies have implemented 3D Secure payment authentication for online transactions, which require an extra proof of identity not available from the card. This protects against skimming attacks such as the one identified in this paper. Unfortunately although 3D Secure technology provides excellent protection for online merchants, it offers only limited protection for cardholders whilst the technology is not universally implemented across all websites.

6. PROPOSED SOLUTION

EMV contactless cards are passive in design; they can be read by any reader that comes within the 10cm range without the knowledge of the cardholder. It would be relatively easy to obviate this type of skimming attack, by designing active cards which will only communicate with a reader once the cardholder has intentionally activated the card. Card activation will be achieved by the application of pressure anywhere on the card, this should be possible whilst the card is still inside a wallet, thereby maintaining the convenience and speed of contactless payments. A piezoelectric material will be used to activate the card, removing the requirement for a battery and lowering the cost. A simple switch will isolate the EMV contactless chip from the antenna whilst the card is inactive and connects the chip to the antenna when the cardholder specifically activates the card.

7. REFERENCES