Chip and PIN is Broken
Steven Murdoch

The EMV protocol and its flaws

EMV

Responses

work with Saar Drimer, Mike Bond, Omar Cheoualy, Ross Anderson

www.lightbluetouchpaper.org
Chip and PIN is Broken

Steven Murdoch

work with Saar Drimer, Mike Bond, Omar Choudary, Ross Anderson
EMV

EuroPay  MasterCard  Visa

They were wrong
EMV is deployed or in planning in most countries except the US, but vendors are working hard to change this.

Smart card based payments
Used on 750m cards, billions of pounds, euros, dollars

Many customers claim that their card has been stolen and used.

Banks claim EMV is infallible, so victims do not get their money back. 44% according to latest figures.
Banks claim EMV is infallible, so victims do not get their money back 44% according to latest figures.
Counterfeit
Lost and stolen
Mail non-receipt
Card—not—present

Counterfeit

Lost and stolen
**Security Confirmation**

To continue with Online Banking, please provide the information requested below.

**Passcode:**
(8 - 20 Characters, case sensitive)

**Date of Birth (mm/dd/yyyy):**

**Social Security Number:**

**Mother’s Maiden Name:**

**Card Number:**
(16 digits, no dashes or spaces)

**Card Expiration Date (mm/yyyy):**

**Card CVV2:**

**ATM or Check Card PIN:**
(4-12 digits)

**Quick Help**

**What do I need to know?**
We use your information, only to identify you. The information is safe and secure. No one else can access it. Entering either your SSN ensures you get access to your Bank of America accounts.

Bank of America is committed to keeping your information secure with our Online Banking Guarantee.
Card-not-present
Added Safety Online

Welcome to Barclaycard Secure.
You are not currently registered for this new free service.
Barclaycard Secure, provided in association with Verified by Visa, protects your card when you shop online with this and other participating retailers.

Simply complete the details below to activate this free security service.

Card Expiry Date:  [ ] / [ ] (MM/YY)
Card Security Code:  [ ]
The last 3 digits on the back of your card (more help)
Card holder name as printed on the card:
Cardholder Date of Birth:  [ ] / [ ] / [ ] (DD/MM/YYYY)
Email address:
How will it be used?

Continue
Back

By registering now, you agree to the Terms and Conditions of Use.
Click here to view: Terms and Conditions of Use Privacy Policy.
Online banking up 14% in 2009
Chip & PIN deployment period

<table>
<thead>
<tr>
<th>Year</th>
<th>Card-not-present</th>
<th>Counterfeit</th>
<th>Lost and stolen</th>
<th>Mail non-receipt</th>
<th>Cheque fraud</th>
<th>ID theft</th>
<th>Online banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>563.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>503</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>491.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>591.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>704.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>529.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total, ex phone (£m)

Source: APACS 2010
9. RESPONSIBILITY

You understand that you are financially responsible for all uses of RBS Secure.

Example of revised terms and conditions for online purchases (Royal Bank of Scotland)
10. Chip and PIN charges cannot be disputed as card would have been in possession when charges were put through.
They were wrong

BBC Newsnight, February 2010
A simplified EMV transaction

card authentication
Card to Terminal: card details, digital signature

Terminal to Card: PIN as entered by customer

cardholder verification
Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction

transaction authorization
Card to Terminal: MAC over transaction and other details
card authentication

Card to Terminal: card details, digital signature

Terminal to Card: PIN as entered by customer
customer enters PIN
Card to Terminal: card details

Terminal to Card: PIN as entered by customer

cardholder verification

Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction
Terminal to Card: description of transaction

transaction authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

online transaction authorization

Bank to Terminal: transaction authorized (yes/no)
MAC and transaction sent to bank for verification

online transaction authorization

Bank to Terminal: transaction authorized (yes/no)
What went wrong?
Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction

transaction authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

online transaction authorization

Bank to Terminal: transaction authorized (yes/no)
transactions

amount, currency, date, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...

...
date, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...
### TVR Byte 3:

<table>
<thead>
<tr>
<th>b8</th>
<th>b7</th>
<th>b6</th>
<th>b5</th>
<th>b4</th>
<th>b3</th>
<th>b2</th>
<th>b1</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Cardholder verification was not successful</td>
</tr>
<tr>
<td>x</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Unrecognised CVM</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>PIN Try Limit exceeded</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>PIN entry required and PIN pad not present or not working</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>PIN entry required, PIN pad present, but PIN was not entered</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>Online PIN entered</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>0</td>
<td>x</td>
<td>RFU</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>0</td>
<td>x</td>
<td>RFU</td>
</tr>
</tbody>
</table>
If the PIN is not required by the terminal, the TVR is all zeros
If the PIN is entered correctly, the TVR is still all zeros

A man-in-the-middle tell the card that the PIN was not required and the terminal that the PIN was correct

Now the criminal can use a stolen card, give the wrong PIN to the terminal and still have the transaction succeed
How the attack works

card authentication
Card to Terminal: card details, digital signature

Terminal to MitM: 0000 entered by criminal

cardholder verification
MitM to Terminal: PIN correct yes!

Terminal to Card: description of transaction

transaction authorization
Card to Terminal: MAC over transaction and other details

criminal enters 0000
card authentication
Messages relayed without modification
criminal enters 0000
Terminal to MitM: \textbf{0000} entered by criminal

cardholder verification

MitM to Terminal: PIN correct \textbf{yes!}

Terminal to Card: description of transaction
cardholder verification

transaction authorization
transaction authorization

Messages relayed without modification
MAC and transaction sent to bank for verification

online transaction authorization

Bank to Terminal: transaction authorized (yes/no)
Terminal to Card: description of transaction

Transaction Authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

Online Transaction Authorization

Bank to Terminal: transaction authorized (yes/no)
- did PIN verification fail?
- was PIN required and not entered?
- ...
Card: No (not attempted)
Terminal: No (verification succeeded)
• did PIN verification fail?
• was PIN required and not entered?
• ...
Card: No (not required)

Terminal: No (was entered)
"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."

"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time so they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."

Responses
UK Cards Association, February 2010

"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."
"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."
We also requested at the time of this claim, supporting documents from [redacted] and were provided a copy of the till receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [redacted] at the time.

Timings and location of these charges are as follows.....

£3000.00 - 20/05/08 - 12.27pm  
£4000.00 - 20/05/08 - 12.28pm  
£2500.00 - 20/05/08 - 12.30pm

All made at [redacted]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.
"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."
Below is a list of the dates and times of all transactions performed in [BLANK] from 23rd July 2009 onwards. I have also included further computerised records for your information:

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Retailer/ATM</th>
<th>Successful/Unsuccessful</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/07</td>
<td>211.66</td>
<td>[BLANK]</td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>[BLANK]</td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>[BLANK]</td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>3187.54</td>
<td></td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>85.56</td>
<td>[BLANK]</td>
<td>Unsuccessful</td>
</tr>
</tbody>
</table>

According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.
0x08 = PIN entry required, PIN pad present, but PIN was not entered
"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."
"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN.

... Consequently, we would ask that this research be removed from public access immediately.

"Second, you seem to think that we might censor a student’s thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values.
"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN.

... Consequently, we would ask that this research be removed from public access immediately and would hope that you are able to give us comfort about your policy towards future disclosures."

UK Cards Association
"Second, you seem to think that we might censor a student’s thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values.

Ross Anderson
University of Cambridge
Banks attempt to suppress maths student's exposé of chip and pin

UK banks attempt to censor academic paper; Cambridge University resists

An anonymous reader writes:
*Representatives of the UK banking industry have sent a take-down notice (PDF link) to Cambridge University. The letter is in response to an exposé of a fatal flaw in Chip and Pin security, by a Cambridge maths student. Banks have attempted to suppress the article by the student.*

**THE INDEPENDENT**

**ECONOMIST**

Bank censorship attempt rebuffed

A trade association of bankers attempted to get the University of Cambridge to withdraw a thesis by Omar Choudary on the No-PIN attack on Chip and Pin. Ross Anderson has told the UK Cards Association that the paper will not be taken offline in a robust response to that request. Anderson points out that the material on the No-PIN attack has already been published by himself and others on the Cambridge University web site.
Downloads of Omar's thesis (per hour)
Many credit card holders have been frustrated by the EMV standard, which they claim is infallible, so victims do not get their money back. According to latest figures, 44% of EMV transactions are rejected due to issues.