Chip and PIN: 5 Years On

Steven Murdoch

www.lightbluetouchpaper.org
Chip and PIN: 5 Years On

Steven Murdoch

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

EuroPay  MasterCard  Visa
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.
Many credit card holders believe their bank is infallible, so victims do not get their money back. According to latest figures, 44% of credit card transactions are not recovered.
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.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcode:</td>
<td>(8 - 20 Characters, case sensitive)</td>
</tr>
<tr>
<td>Date of Birth (mm/dd/yyyy):</td>
<td></td>
</tr>
<tr>
<td>Social Security Number:</td>
<td></td>
</tr>
<tr>
<td>Mother's Maiden Name:</td>
<td></td>
</tr>
<tr>
<td>Card Number:</td>
<td>(16 digits, no dashes or spaces)</td>
</tr>
<tr>
<td>Card Expiration Date (mm/yyyy):</td>
<td></td>
</tr>
<tr>
<td>Card CVV2:</td>
<td></td>
</tr>
<tr>
<td>ATM or Check Card PIN:</td>
<td>(4-12 digits)</td>
</tr>
</tbody>
</table>

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

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
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.

Letter denying refund for disputed transactions (American Express)
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

customer enters PIN

MAC and transaction sent back for verification
	online transaction authorization

Bank of America Transformed with EMV Chip Cards

Visit bankofamerica.com/moreinfo for 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)
transaction
amount, currency, date, nonce, TVR, etc

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


... 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>x</td>
<td>0</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!

- Transaction authorization
  - Terminal to Card: description of transaction
  - Card to Terminal: MAC over transaction and other details

- Criminal enters 0000
card authentication
Messages relayed without modification

cardholder

 verifies
criminal enters 0000
Card to Terminal: card details

Terminal to MitM: 0000 entered by criminal

cardholder verification

MitM to Terminal: PIN correct yes!

Terminal to Card: description of transaction
cardholder verification
transaction authorization

Messages relayed without modification
and other details

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)
Rate, nonce, TVR, etc

- 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 as 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 [redacted] 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>[redacted]</td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>[redacted]</td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>[redacted]</td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>3187.54</td>
<td>[redacted]</td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>85.56</td>
<td>[redacted]</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.
24/07/1968
KART NO
11:38
S.K.T.: 12/10

ENV: 00000000031810/0010099999/F000
APP LABEL: VISA DEBIT

ORJİNAL FİŞ SAKLAYINIZ.
MUSTERİYE 2. NUSHAYI VERİNİZ.

TESEKKÜRLER
FORTIS
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."
WRONG
"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
Downloads of Omar's thesis (per hour)
Many credit card holders believe that EMV (EMV is infallible, so victims do not get their money back. 44% according to latest figures.