The EMV protocol and its flaws

Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond

Responses
EMV

EuroPay  MasterCard  Visa

Security

- AES
- 128-bit encryption
- PCI DSS compliance

Total fraud in the UK

- Dip in 2005-2006
- Up 25% to £704.3m

Effect on fraud

Total card holding
- Online banking
- Pre-paid cards
- In-store applications

Smart card based payments
- Used on 750m cards, billions of pounds, euros, dollars
- May continue for at least 20 more years

EMV compliant or EMV compliant with accepted credit card brand.
EMV

EuroPay
MasterCard
Visa
EMV is deployed or in planning in most countries except the US, but vendors are working hard to change this.

Point-of-sale and ATM

Smart card based payments

Used on 750m cards, billions of pounds, euros, dollars

Credit and Debit

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.
security

does not affect

Makes

even for

Allows
Security

Allows PIN-based authentication, even for offline transactions

Makes card cloning harder

don't affect

online banking

card-not present

checks

False applications
Effect on fraud

Chip & PIN deployment period

Data from APACS (2009)
Allows PIN-based authentication, even for offline transactions

Makes card cloning harder
Lost and stolen
down 53% to £54.1m

Mail non receipt
down 86% to £10.2m
Allows PIN-based authentication even for offline transactions

Makes card cloning harder

Online banking card-not-present
counterfeit

up 31% to £169m
online banking
up 330% to £52.5m

card not present
up 118% to £328.4m

checks
down 9% to £41.9m
card not present up 118% to £328.4m

checks down 9% to £41.9m

false applications up 28% to £47.4m
Total fraud in the UK
dip in 2005—2006, but up 25% to £704.3m
Banks claim EMV is infallible, so victims do not get their money back 44% according to latest figures.
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

Online transaction authorization
Back to terminal (command to authorize the transaction and the customer receives the card back)
card authentication

Card to Terminal: card details, digital signature

Terminal to Card: PIN as entered by customer
customer enters PIN
Card to Terminal: PIN correct (yes/no)

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

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

Bank to Terminal: transaction authorized (yes/no)

transaction authorization
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)

MAC and transaction sent to bank for verification
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?
- ...

Section
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 tells 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

1. Card authentication
   - Card to Terminal: card details, digital signature

2. Terminal to MitM: 0000 entered by criminal

3. Cardholder verification
   - MitM to Terminal: PIN correct yes!

4. Terminal to Card: description of transaction

5. Transaction authorization
   - Card to Terminal: MAC over transaction and other details

6. Criminal enters 0000

7. Online transaction authorization
   - Terminal to bank for confirmation

   - Bank to Terminal: transaction completed
card authentication

Messages relayed without modification
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)
transaction authorization

Terminal to Card: description of transaction

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

Bank to Terminal: transaction authorized (yes/no)
... did PIN verification fail?

Card: No (not attempted)  Terminal: No (verification succeeded)
Card: No (not attempted)
Terminal: No (verification succeeded)
late, 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

"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." 

In addition to the TVR, the card produces a CVR (card verification results) and the terminal may optionally produce a CVMR (cardholder verification method result)
"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 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 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

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.
"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."
"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.
FORITS TESEKURLEK

MÜSTERİYE2. MÜŞAHİ,YERİNZ

ORJİNAL FİŞ SAKALAVIZI

APP LABEL : VISA DEBIT

ERV : #88888888888888888888

S.K.T.: 12/10

KART NO

24/07/1588

1:38
In addition to the TVR, the card produces a CVR (card verification results) and the terminal may optionally produce a CVMR (cardholder verification method result) attack, the CVR will not match the CVMR
In our attack, the CVR will not match the CVMR
We hear that the industry are working on a defence based on comparing the CVR and CVMR, but it is not quite that simple:

- Sometimes the CVMR is not produced by the terminal (it is optional)
- Sometimes it is produced but wrong (it has not been considered useful, until now)
- Sometimes it is produced but dropped or corrupted on the way back
Many credit card holders are frustrated by the EMV system, which they believe is infallible. However, according to recent figures, only 56% of cardholders are able to recover their lost money, meaning that 44% of victims do not get their money back.
Chip and PIN is Broken

The EMV protocol and its flaws

Responses

EMV
How is ATM fraud happening?