How is ATM fraud happening?
Chip and PIN is Broken

Dr Steven J. Murdoch
University of Cambridge
EMV

EuroPay  MasterCard  Visa

Source: APACS 2010

They were wrong
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.
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: ____________________________
(6 - 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/YY)

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.
Counterfeit
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
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?
- ...
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

MAC and transaction sent to bank for verification

online transaction authorization

card authentication
Messages relayed without modification

cardholder verification
criminal enters 0000
Terminal to MitM: 0000 entered by criminal

cardholder verification

MitM to Terminal: PIN correct yes!

Terminal to Card: description of transaction
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)
diagram that, nonce, TVR, etc.

... 

did PIN verification fail?

was PIN required and not entered?

Card: No (not attempted)
Terminal: No (verification succeeded)
"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."
"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.
"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
"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.
24/07/1988
KART NO
11:39
S.K.T.: 12/10

EMV: 0000000031010/00000000-F000
APP LABEL: VISA DEBIT

ORJİNAL FİS İSAKLAYINIZ.
HÜSÜRLİYE 2. Nüşhayı Veriniz.

TESEKKÜRLER
FORTIS
Banks claim EMV is infallible, so victims do not get their money back 44% according to latest figures
The EMV protocol and its flaws

Chip and PIN is Broken

Dr. Steven J. Murdoch
University of Cambridge

Responses
How is ATM fraud happening?