Chip & PIN –
notes on a dysfunctional security system

Saar Drimer
http://www.cl.cam.ac.uk/~sd410/

in collaboration with Steven J. Murdoch, Ross Anderson, Mike Bond

The Institution of Engineering and Technology (IET), Cambridge, UK, 4 March 2010
Presentation outline

- Introduction to EMV ("Chip and PIN") and background
- Yes-card attack
- Relay attack
- Terminal tampering attack
- "no-PIN" attack, and reactions
- The big picture
Chip & PIN has now been running in the UK for about 5 years

- Chip & PIN, based on the EMV (EuroPay, MasterCard, Visa) standard, is deployed throughout most of Europe
- In process of roll-out elsewhere
- Chip authenticates the card; PIN authenticates the cardholder
- UK was an early adopter: rollout in 2003–2005; mandatory in 2006
- Chip & PIN changed many things, although not quite what people expected
UK fraud figures 2004–2008

- Card–not–present
- Counterfeit
- Lost and stolen
- ID theft
- Mail non–receipt
- Online banking
- Check fraud
- Chip & PIN deployment period

Year | Losses (£m) | Total (£m)
-----|-------------|-----------
2004 | 563.1       |           
2005 | 503         |           
2006 | 491.2       |           
2007 | 591.4       |           
2008 | 704.3       |           

Source: APACS
Authorisation of EMV transaction involves many parties
EMV overview – offline PIN

Card and cardholder authentication – PIN is sent to the card for checking if it is correct
The issuer approves the transaction before the exchange of goods takes place; merchant’s receipt says “Verified by PIN”
EMV overview – offline authorisation

The issuer approves the transaction after the goods were exchanged.
First EMV cards issued in the UK...

- Static Data Authentication (SDA)
  - No support for PIN encryption
  - card cannot sign fresh data
  - cheaper than Dynamic Data authentication (DDA) capable chips.
- Magstrip still on card
  - for backwards compatibility/backup
  - for use in non-EMV countries
  - still allows skimming
- Exact copy of magstrip tracks stored on chip
  - allows chip transactions to be processed as magstrip

- The chip is hard to clone completely, so criminals rely on the mechanisms put in place for backwards-compatibility and cross-border interoperability
YES-card attack

Criminal copies all static data onto another card (certificate, application data, etc.) This chip on the YES-card is programmed to reply YES to any PIN entered.
The YES-card attack only works in off-line transactions because the wrong cryptogram would be detected in an on-line authorisation solution: DDA, online authorisation
Relay attack: Alice thinks she’s paying $20, but is charged $2,000 elsewhere.

We take a normal Chip and PIN transaction, separate the card and the terminal, and connect them with a long wire (of course this is not very practical).
Relay attack: Alice thinks she’s paying $20, but is charged $2,000 elsewhere

We take a normal Chip and PIN transaction, separate the card and the terminal, and connect them with a long wire (of course this is not very practical)
Relay attack: Alice thinks she’s paying $20, but is charged $2,000 elsewhere

We take a normal Chip and PIN transaction, separate the card and the terminal, and connect them with a long wire (of course this is not very practical)
Relay attack: Alice thinks she’s paying $20, but is charged $2,000 elsewhere

attackers can be on opposite sides of the world!

Alice inserts her card into Bob’s *fake* terminal, while Carol inserts a fake card into Dave’s *real* terminal. Using wireless communication the $2,000 purchase is debited from Alice’s account.

solution: distance bounding
The relay kit:

$500 worth of off-the-shelf hardware, two laptops and moderate engineering skill is all it takes.
We demonstrated the relay attack on BBC1’s “Watchdog”, February 2007

Watch video: http://www.youtube.com/watch?v=X7pjUIxKoEc
Academic paper and more info: http://www.cl.cam.ac.uk/research/security/banking/relay/
By “tapping” the communication line between the card and the terminal’s processor, criminals can create a magnetic strip version of the card and use at ATMs that do not read smartcards (like in the U.S.)
Tamper proofing is supposed to protect the PIN and card data in transit

- Various standard bodies require that terminals be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)

- Evaluations are performed to well-established standards (Common Criteria)

- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over USD $25,000 per terminal
Protection measures: tamper meshes

Ingenico i3300
Protection measures: tamper meshes

Ingenico i3300
We found how to attack these terminals using paperclips

Ingenico i3300
Dione Xtreme

It’s just a matter of knowing where to drill!

... tamper resistance protects the banks’ keys, not the cardholders’ PINs

solution: PIN encryption, iCVV, better certification of terminals
We demonstrated the attack on BBC
Newsnight in February 2008

Criminals have been tampering with terminals since at least 2006...

Watch video: http://video.google.com/videoplay?docid=7109740591622124830
Academic paper and more info: http://www.cl.cam.ac.uk/research/security/banking/ped/
The no-PIN attack allows criminals to use a stolen card without knowing its PIN.

It requires inserting a device between the genuine card and payment terminal.

This attack works even for online transactions, and DDA cards.
BBC Newsnight filmed our demonstration for national TV

BBC Newsnight, BBC2, 11 February 2010

Watch video: http://www.youtube.com/watch?v=JPAX32lgkrw
Academic paper and more info: http://www.cl.cam.ac.uk/research/security/banking/nopin/
no-PIN attack

This is a normal transaction
The "wedge" (MITM) suppresses the "check PIN" command and replies "YES" to any PIN entered by the crook.
no-PIN attack

<table>
<thead>
<tr>
<th>issuer</th>
<th>terminal</th>
<th>card</th>
<th>EMV command</th>
<th>protocol phase</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>SELECT/READ RECORD</td>
<td>Card authentication</td>
</tr>
<tr>
<td>select file 1PAY.SYS.DDF01</td>
<td>available applications (e.g Credit/Debit/ATM)</td>
<td>signed records, Sig(signed records)</td>
<td>READ RECORD...</td>
<td></td>
</tr>
<tr>
<td>select application/start transaction</td>
<td>unsigned records</td>
<td>PIN retry counter</td>
<td>GET DATA</td>
<td></td>
</tr>
<tr>
<td>PIN: xxxx</td>
<td>PIN OK/Not OK</td>
<td>T = (amount, currency, date, TVR, nonce, ...)</td>
<td>GENERATE AC</td>
<td></td>
</tr>
<tr>
<td>ARQC = (ATC, IAD, MAC(T, ATC, IAD))</td>
<td>T, ARQC</td>
<td>ARPC, ARC</td>
<td>EXTERNAL AUTHENTICATE/GENERATE AC</td>
<td></td>
</tr>
<tr>
<td>ARPC, auth code</td>
<td>TC = (ATC, IAD, MAC(ARC, T, ATC, IAD))</td>
<td>TC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
no-PIN attack

<table>
<thead>
<tr>
<th>issuer</th>
<th>terminal</th>
<th>MITM</th>
<th>card</th>
<th>EMV command</th>
<th>protocol phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>select file 1PAY.SYS.DDF01</td>
<td>available applications (e.g. Credit/Debit/ATM)</td>
<td></td>
<td></td>
<td>SELECT/READ RECORD</td>
<td>Card authentication</td>
</tr>
<tr>
<td>select application/start transaction</td>
<td>signed records, Sig(signed records)</td>
<td></td>
<td></td>
<td>SELECT/GET PROCESSING OPTIONS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unsigned records</td>
<td></td>
<td></td>
<td>READ RECORD...</td>
<td></td>
</tr>
<tr>
<td>PIN retry counter</td>
<td>PIN: xxxx</td>
<td></td>
<td></td>
<td>GET DATA</td>
<td>Cardholder verification</td>
</tr>
<tr>
<td></td>
<td>PIN OK</td>
<td></td>
<td></td>
<td>VERIFY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>T = (amount, currency, date, TVR, nonce, ...)</td>
<td></td>
<td></td>
<td>GENERATE AC</td>
<td>Transaction authorization</td>
</tr>
<tr>
<td></td>
<td>ARQC = (ATC, IAD, MAC(T, ATC, IAD))</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T, ARQC</td>
<td></td>
<td></td>
<td>EXTERNAL AUTHENTICATE/GENERATE AC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARPC, ARC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ARPC, auth code</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TC = (ATC, IAD, MAC(ARC, T, ATC, IAD))</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

solution: ?
It requires possession of a customer’s card [which is valid until it is reported stolen]

Stolen cards are precisely the reason why Chip and PIN was introduced – to authenticate the cardholder.

There are much simpler ways to commit fraud under these circumstances at much less risk to the criminal.

I call this the “we suck anyway defence”, and it is unacceptable.

Cambridge claims that their latest attack is both a new discovery and undetectable; this is not true.

This is worrying... if the attack was known, why wasn’t it fixed?

Source: UK Cards Association (formerly APACS)
http://www.theukcardsassociation.org.uk/view_point_and_publications/what_we_think/-/page/906/
The industry is confident that the forensic signature of such an attack is easily detectable... at the time of the transaction.

The confidence isn’t reassuring. We tried it. Many times. It works.

Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks.

- Absence of evidence is not evidence of absence
- Our many successful no-PIN transactions went undetected
- Criminals are very sophisticated – ATM skimmers, for example
- Break once, use anywhere

Source: UK Cards Association (formerly APACS)
http://www.theukcardsassociation.org.uk/view_point_and_publications/what_we_think/-/page/906/
...card company... will always rely on primary evidence to review the facts of the case and would never use a paper receipt for evidence as suggested.

Untrue. In at least one case, a bank used a receipt as primary evidence to refuse a refund


We believe that this complicated method will never present a real threat to our customers’ cards

Believe? Never?

Source: UK Cards Association (formerly APACS)
http://www.theukcardsassociation.org.uk/view_point_and_publications/what_we_think/-/page/906/
Reaction… “kit is too big”

Miniature SIM card “shims” exist for breaking phones from network lock-in terminal → MITM:

0020008008240000fffffffffff

MITM → terminal:

9000

The no-PIN attack requires three lines of Python code

```python
if DEBUG_VERIFY_PRE and command_ascii[0:4] == "0020":
    debug("Spoofing response to VERIFY command")
    return binascii.a2b_hex("9000")
```
Why is this a significant failure

• Both terminal and card completed a successful transaction from their perspective
  • flags indicate that something failed, but not what actually took place
• First attack on back-end transaction authorisation
  • up to now, our attacks were on how card were used
• Evidence is crucial
  • banks need to keep evidence and prove the correct PIN was used (TVR, ARQC, CVMR, IAD)
• Chip and PIN security is further undermined
  • this is a protocol failure, and it is unclear whether it can be easily fixed
  • when challenged, banks may no longer rely on unsubstantiated security claims
Weak customer protection leaves many victims “out of pocket”

One in five cardholders do not get their money back

banking code/payment services directive are elusive

banks reluctant to provide victims the evidence they use to determine that they are negligent

Banks are not usually required to provide verifiable evidence when disputes occur.

- Evidence in a recent court case – highlighted digits are supposed to indicate a chip transaction, but in proprietary format.
- “Verified by PIN” on receipts is meaningless without the ability to verify it.
- Banks sometimes destroy primary evidence.

Source: http://www.cl.cam.ac.uk/~rja14/Papers/halifax-log.pdf
What has failed?

- Liability engineering – banks care less about the security systems they maintain
- Over-specification – thousands of pages of specification inevitably lead to insecure implementations
- Poor design choices – fallback enable security holes to remain, and protocols to be broken by design
- Tick-box mentality – certification doesn’t work when certification labs carry no penalty for certifying broken equipment
- Not understanding the enemy – assumption that the enemy is incompetent, and that merchants are always honest
- Closed system forced on public – no external review

For all these reasons, the “Chip and PIN” system is fundamentally broken.
The end – thanks!

Our group’s blog:
http://www.lightbluetouchpaper.org/

Further information:
http://www.cl.cam.ac.uk/research/security/banking/

P.C Vey, Published in The New Yorker January 16, 2006
http://www.thenewyorkerstore.com/product_details.asp?mscssid=4p9f5x11p94g8h&sitetype=1&sid=121796