Banking Security: Attacks and Defences

Steven J. Murdoch

http://www.cl.cam.ac.uk/users/sjm217/

work with Saar Drimer, Ross Anderson, Mike Bond

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

www.torproject.org

OWASP, March 2013, Leuven, BE
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
- Customer inserts contact-smartcard at point of sale, and enters their PIN
- 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 2004–2011

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses to banks and merchants (£m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>563.1</td>
</tr>
<tr>
<td>2005</td>
<td>503</td>
</tr>
<tr>
<td>2006</td>
<td>491.2</td>
</tr>
<tr>
<td>2007</td>
<td>591.4</td>
</tr>
<tr>
<td>2008</td>
<td>704.3</td>
</tr>
<tr>
<td>2009</td>
<td>529.6</td>
</tr>
<tr>
<td>2010</td>
<td>441</td>
</tr>
<tr>
<td>2011</td>
<td>410.6</td>
</tr>
</tbody>
</table>

Chip & PIN deployment period

Card–not–present
Counterfeit
Lost and stolen
ID theft
Mail non–receipt
Online banking
Cheque fraud

Source: Financial Fraud Action UK
Counterfeit fraud mainly exploited backwards compatibility features

- Upgrading to Chip & PIN was too complex and expensive to complete in one step
- Instead, chip cards continued to have a magstrip
  - Used in terminals without functioning chip readers (e.g. abroad)
  - Act as a backup if the chip failed
- Chip also contained a full copy of the magstrip
  - Simplifies issuer upgrade
  - Chip transactions can be processed by systems designed to process magstrip
- Criminals changed their tactics to exploit these features, and so counterfeit fraud did not fall as hoped
- Fraud against UK cardholders moved outside of the UK
Criminals could now get cash

Criminals collected:

- card details by a “double-swipe”, or tapping the terminal/phone line
- PIN by setting up a camera, tapping the terminal, or just watching

Cloned magstrip card then used in an ATM (typically abroad)

In some ways, Chip & PIN made the situation worse

- PINs are used much more often (not just ATM)
- PoS terminals are harder to secure than an ATM

Tonight (ITV, 2007-05-04)
Chip & PIN vulnerabilities

- Fallback vulnerabilities are not strictly-speaking a Chip & PIN vulnerability
- However, vulnerabilities do exist with Chip & PIN
- To understand these, we need some more background information
- To pay, the customer inserts their smart card into a payment terminal
- The chip and terminal exchange information, fulfilling three goals:

  - **Card authentication**: that the card presented is genuine
  - **Cardholder verification**: that the customer presenting the card is the authorized cardholder
  - **Transaction authorization**: that the issuing bank accepts the transaction
The no-PIN attack

- 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
The no-PIN attack

1. Card details; digital signature
2. Wrong PIN entered by crook
3. Wrong PIN entered by crook; transaction description
4. PIN OK (yes); authorization cryptogram
5. Online transaction authorization (optional)

1/3/4. Card details; digital signature
PIN; transaction description
PIN OK; cryptogram

Why does this attack work?

- **Complexity**
  - 4,000 pages of specification!
  - Data needs to be combined from several different sources and specifications (EMV, MasterCard, ISO, APACS)
  - Despite quantity, no specification actually describes the necessary checks

- **Bad design of flags**
  - Card produces a flag (card verification results – CVR) which says whether PIN verification succeeded
  - But this flag is in an issuer-specific format and so cannot be parsed by the terminal
  - Flag produced by terminal (TVR) is set either if PIN verification succeeded or terminal skipped check
  - Other flags may exist (country-specific, covered by APACS and ISO), but evidently are not checked in practice

- **Implementation problems**
  - Since issuers don’t check flags, terminals mis-report state
Scientific researchers from the University of Cambridge (UK), of which the most well known is Professor Ross Anderson, have announced that they have tested a scenario which attacks the EMV chip card. The attack scenario in question has already been analysed by several teams of independent specialists, as well as CBs own experts, with the conclusion that neither the chip in itself, nor the importance and the advantages of the chip in terms of security have been put into question. What is more, at this stage, the observations are the result of scientific research whose transposition outside laboratory conditions is complex since it would necessitate the use of highly sophisticated material.

— Le GIE des Cartes Bancaires (January 2010)
Response from the criminals

— Le Parisien (January 2012)
Current and proposed defences

- **Skimming**
  - iCVV: Slightly modifying copy of magnetic strip stored on chip
  - Disabling fallback: Preventing magnetic strip cards from being used in EMV-enabled terminals
  - Better control of terminals: Prevent skimmers from being installed

- **YES-card**
  - Dynamic Data Authentication (DDA): Place a public/private keypair on every card
  - Online authorization: Require that all transactions occur online

- **No-PIN attack**
  - Defences currently still being worked on
  - Extra consistency checks at issuer may be able to spot the attack
  - Combined DDA/Application Cryptogram Generation (CDA): Move public key authentication stage to the end
Random numbers?

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>UN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-06-29</td>
<td>10:37:24</td>
<td>F1246E04</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:37:59</td>
<td>F1241354</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:38:34</td>
<td>F1244328</td>
</tr>
<tr>
<td>2011-06-29</td>
<td>10:39:08</td>
<td>F1247348</td>
</tr>
</tbody>
</table>
Reverse engineering
Triton ATM (CPU board)
Triton ATM (DES board)
Surveying the problem
### Characteristic C

<table>
<thead>
<tr>
<th>SRC2 EXP6</th>
<th>SRC2 EXP6B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 77028437</td>
<td>0 5D01BBCF</td>
</tr>
<tr>
<td>1 0D0AF8F9</td>
<td>1 760273FE</td>
</tr>
<tr>
<td>2 5C0E743C</td>
<td>2 730E5CE7</td>
</tr>
<tr>
<td>3 4500CE1A</td>
<td>3 380CA5E2</td>
</tr>
<tr>
<td>4 5F087130</td>
<td>4 580E9D1F</td>
</tr>
<tr>
<td>5 3E0CB21D</td>
<td>5 6805D0F5</td>
</tr>
<tr>
<td>6 6A05BAC3</td>
<td>6 530B6EF3</td>
</tr>
<tr>
<td>7 74057B71</td>
<td>7 4B0FE750</td>
</tr>
<tr>
<td>8 76031924</td>
<td>8 7B0F3323</td>
</tr>
<tr>
<td>9 390E8399</td>
<td>9 630166E1</td>
</tr>
<tr>
<td>Counters</td>
<td>Weak RNGs</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>ATM4</td>
<td>eb661db4</td>
</tr>
<tr>
<td>ATM1</td>
<td>690d4df2</td>
</tr>
<tr>
<td>ATM4</td>
<td>2cb6339b</td>
</tr>
<tr>
<td>ATM1</td>
<td>69053549</td>
</tr>
<tr>
<td>ATM4</td>
<td>36a2963b</td>
</tr>
<tr>
<td>ATM1</td>
<td>660341c7</td>
</tr>
<tr>
<td>ATM4</td>
<td>3d19ca14</td>
</tr>
<tr>
<td>ATM1</td>
<td>5e0fc8f2</td>
</tr>
<tr>
<td>ATM5</td>
<td>F1246E04</td>
</tr>
<tr>
<td>ATM2</td>
<td>6f0c2d04</td>
</tr>
<tr>
<td>ATM5</td>
<td>F1241354</td>
</tr>
<tr>
<td>ATM2</td>
<td>580fc7d6</td>
</tr>
<tr>
<td>ATM5</td>
<td>F1244328</td>
</tr>
<tr>
<td>ATM2</td>
<td>4906e840</td>
</tr>
<tr>
<td>ATM5</td>
<td>F1247348</td>
</tr>
<tr>
<td>ATM2</td>
<td>46099187</td>
</tr>
<tr>
<td>ATM3</td>
<td>650155D7</td>
</tr>
<tr>
<td>ATM3</td>
<td>7C0AF071</td>
</tr>
<tr>
<td>ATM3</td>
<td>7B021D0E</td>
</tr>
<tr>
<td>ATM3</td>
<td>1107CF7D</td>
</tr>
<tr>
<td>Stronger RNGs</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>POS1</td>
<td>013A8CE2</td>
</tr>
<tr>
<td>POS1</td>
<td>01FB2C16</td>
</tr>
<tr>
<td>POS1</td>
<td>2A26982F</td>
</tr>
<tr>
<td>POS1</td>
<td>39EB1E19</td>
</tr>
<tr>
<td>POS1</td>
<td>293FBA89</td>
</tr>
<tr>
<td>POS1</td>
<td>49868033</td>
</tr>
</tbody>
</table>
Cashing out

- Pre-play card: load with cryptograms for expected UNs
- Malware attack: tamper with ATM or POS terminal to produce predictable UNs
- Tamper with ATMs or POS in supply chain
- Collusive merchant, modifies software
- Tamper with communications
Mitigating the attack

- **Detection:**
  - Suspicious jumps in transaction counter
  - Lack of issuer authentication

- **Prevention:**
  - Relying party (issuer) generates the UN
  - Audit trail shows where UNs came from

- **Industry response so far has been mixed**
  - Details disclosed in early 2012
  - Some surprised by the problem
  - Others less so
  - Some knew of this problem but did not admit it

More information: “Chip and Skim: cloning EMV cards with the pre-play attack”, arXiv:1209.2531
1,000 tests (was only 4) then:

Pass Criteria:

- For test script, the Terminal Unpredictable Number (9F37) stored shall:
  - Not be a duplicated value of previous Unpredictable Number values (both sequences included)
  - None of the bits is fixed, i.e. the $i^{th}$ bit is not the same for all 1,000 UNs ($1 \leq i \leq 32$)
  - The average hamming weight shall be between 15 and 17 (i.e. the number of bits set to '1' in the total of 32,000 bits shall be between 15,000 and 17,000)

Terminal Level 2 Test Cases: Unpredictable Number testing Update, EMVCo Terminal Approval Bulletin No. 127
Online banking fraud is a significant and growing problem in the UK

- 174% increase in users between 2001 and 2007
- 185% increase in fraud in 2007–2008 (£21.4m in first 6 months of 2008)
- Simple fraud techniques dominate in the UK:
  - Phishing emails
  - Keyboard loggers
- Still work, and still used by fraudsters, due to the comparatively poor security
A variety of solutions have been proposed to resist phishing

- On-screen keyboards
- Picture passwords
- Device fingerprinting
- One-time-passwords/iTAN

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser
A variety of solutions have been proposed to resist phishing

- On-screen keyboards
- Picture passwords
- Device fingerprinting
- One-time-passwords/iTAN

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser
A variety of solutions have been proposed to resist phishing:

- On-screen keyboards
- Picture passwords
- Device fingerprinting
- One-time-passwords/iTAN

All of these defences have been broken by fraudsters:

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser

### HTTP Header Information

Which headers does your browser send? When communicating with the web, contain information about which type of images are supported, which kind of cookies etc.

<table>
<thead>
<tr>
<th>HTTP Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_ACCEPT</td>
<td>text/html, application/xhtml+xml, application/</td>
</tr>
<tr>
<td>HTTP_ACCEPT_CHARSET</td>
<td>ISO-8859-1, utf-8;q=0.7,*;q=0.7</td>
</tr>
<tr>
<td>HTTP_ACCEPT_ENCODING</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>HTTP_ACCEPT_LANGUAGE</td>
<td>en-us,en;q=0.5</td>
</tr>
<tr>
<td>HTTP_CONNECTION</td>
<td>keep-alive</td>
</tr>
<tr>
<td>HTTP_HOST</td>
<td>browserspy.dk</td>
</tr>
<tr>
<td>HTTP_KEEP_ALIVE</td>
<td>300</td>
</tr>
<tr>
<td>HTTP_REFERER</td>
<td><a href="http://browserspy.dk/geolocation.php">http://browserspy.dk/geolocation.php</a></td>
</tr>
<tr>
<td>HTTP_USER_AGENT</td>
<td>Mozilla/5.0 (Macintosh; U; Intel Mac OS;</td>
</tr>
<tr>
<td>QUERY_STRING</td>
<td></td>
</tr>
<tr>
<td>REMOTE_ADDR</td>
<td>128.232.0.64</td>
</tr>
<tr>
<td>REMOTE_PORT</td>
<td>50625</td>
</tr>
<tr>
<td>REQUEST_METHOD</td>
<td>GET</td>
</tr>
<tr>
<td>REQUEST_URI</td>
<td>/headers.php</td>
</tr>
<tr>
<td>REQUEST_TIME</td>
<td>1261872241</td>
</tr>
</tbody>
</table>
A variety of solutions have been proposed to resist phishing

- On-screen keyboards
- Picture passwords
- Device fingerprinting
- One-time-passwords/iTAN

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser
A variety of solutions have been proposed to resist phishing

iTAN

Customer must provide the requested one time password
A variety of solutions have been proposed to resist phishing

- On-screen keyboards
- Picture passwords
- Device fingerprinting
- One-time-passwords/iTAN

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser
Malware embeds itself into the browser

Changes destination/amount of transaction in real-time

Any one-time password is valid, and mutual authentication succeeds

Patches up online statement so customer doesn’t know
Somehow the response must be bound to the transaction to be authorised

Embed challenge in a CAPTCHA style image, along with transaction

Involving a human can defeat this

May move the fraud to easier banks

Picture: Volksbank Dill eG
Some UK banks have rolled out disconnected smart card readers

CAP (chip authentication programme) protocol specification secret, but based on EMV (Europay, Mastercard, Visa) open standard for credit/debit cards
Reader prompts for input and displays MAC generated by card

- Customer enters PIN
- Card verifies PIN
- Customer enters transaction details (varies between banks)
- Card calculates MAC over:
  - Counter on card
  - Information entered by customer
  - Result of PIN entry
- Reader displays decimal value from:
  - Some bits from the counter
  - Some bits from the MAC
  - (specified by the card’s bit filter)
Usability failures aid fraudsters

CAP reader operates in three modes, which alters the information prompted for and included in the MAC

- **Identify**  No prompt
- **Respond**  8-digit challenge (**NUMBER:**)
- **Sign**  Destination account number (**REF:**) and amount

Banks have inconsistent usage

- **Barclays**  “Identify” for login, “Sign” for transaction
- **NatWest**  “Respond” with first 4 digits random and last 4 being the end of the destination account number

Fraudsters can confuse customers to enter in the wrong thing
**Transaction mode not included in MAC**

Input to MAC does not include the selected operation mode

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>00000000000000</td>
<td>0000000000</td>
</tr>
<tr>
<td>Respond</td>
<td>00000000000000</td>
<td>&lt;challenge&gt;</td>
</tr>
<tr>
<td>Sign</td>
<td>&lt;amount&gt;</td>
<td>&lt;account number&gt;</td>
</tr>
</tbody>
</table>

A “Sign” response, with an empty/zero amount, is also a valid “Respond” response

The account number field is overloaded as being nonce in one mode and destination account number in another

**This ambiguity can be exploited by fraudsters when fooling customers to enter wrong thing**
Nonce is small or absent

No nonce in Barclays variant so response stays valid; only a 4-digit nonce with NatWest (weak – 100 guesses = 63% success rate)

Fake point-of-sale terminal can get response in advance

Even if the nonce was big, a real-time attack still works
We demonstrated this attack on the BBC television programme, Inside Out, earlier this year.
Police think French pair tortured for pin details

Matthew Taylor
The Guardian, Saturday July 5 2008

CAP readers help muggers

CAP reader tells someone whether a PIN is correct

Offers assistance to muggers

Affects customers with CAP-enabled cards, even if their bank doesn’t use CAP

EMV specification always let this be built, but now devices are distributed for free
Software implementation of CAP is possible and desirable

CAP readers contain no secrets; possible to do black-box reverse engineering

CAP stops automated transactions: there is demand for a PC implementation

Some available now

If this software becomes popular, malware will attack it
What does this mean for customers?

CAP is far better than existing UK systems

- Authentication codes are dynamic
- Authentication codes are bound to transaction (although could be better)

Is this better for customers? Maybe no (at least in the UK)

Consumer protection law is vague: you are protected unless the bank considers you “negligent”

When the UK moved from signature to PIN for card payments, customers found it harder to be refunded for fraud (now 20% are left out of pocket)

The UK is moving from password to PIN for online banking. Might we see the same pattern (it is too soon to tell)?
Other authentication tokens fix many of the issues in the UK CAP

HHD 1.3 (standard from ZKA, Germany) is stronger than UK CAP, but more typing is required

- Many more modes, selected by initial digits of challenge
- Mode number alters the meaningful prompts
- Up to 7 digit nonce for all modes
- Nonce, and mode number, are included in MAC
- PIN verification is optional

RSA SecurID and Racal Watchword do PIN verification on server, and permit a duress PIN
More improvements require higher unidirectional bandwidth

For usability, customer should not have to type in full challenge

Allows versatility and better security
Flicker TAN

- Very similar to German CAP system (HHD 1.3)
- Rather than typing in transaction, encoded in a flickering image
- Easier to use, because no need to type in information twice
- Exactly as versatile and secure as HHD 1.3
- Customer needs to carry special reader and their card
- Flickering image may be annoying
- Offered by Sparkasse
USB connected readers

- Class-3 smart card reader (with keypad and display)
- For use with HBCI/FinTS online banking
- Requires drivers to be installed, so not usable while travelling
- Also not usable from work (where a lot of people do their online banking)
- Can also be used for digital signatures
- Can have good security, but details depend on protocol
- Offered by Sparkasse
Cronto PhotoTAN

- Transaction description encoded in a custom 2-D barcode
- More versatile than HHD 1.3 (allows for free text)
- Available on mobile phone (currently Android, iPhone...)
- Also dedicated hardware, for users without a suitable phone
- Secure and convenient, because most people keep their phone on their person
- Used by Commerzbank
- I did this!
Cronto PhotoTAN

- Transaction description encoded in a custom 2-D barcode
- More versatile than HHD 1.3 (allows for free text)
- Available on mobile phone (currently Android, iPhone...)
- Also dedicated hardware, for users without a suitable phone
- Secure and convenient, because most people keep their phone on their person
- Used by Commerzbank
- I did this!
Conclusions

Systems based on EMV are open to a variety of attacks

- While the specification does not forbid implementing resistance measures, it offers little help
- In practice, implementers have slipped up, and customers have been left liable
- EMV’s complexity, and large variety of options are particularly problematic
- In particular, not specifying security checks, and making essential data items optional, are a fundamental problem of EMV
- While the specification could be patched to fix the particular vulnerabilities identified, fixing the systemic problems needs a re-write of the protocol and specification
- For online banking, transaction authentication is now essential, which requires a trustworthy display

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