Payment Security: Attacks & Defences

Dr Steven J Murdoch
University College London
UK fraud is going up again

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses (£m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>481.4</td>
</tr>
<tr>
<td>2005</td>
<td>452.6</td>
</tr>
<tr>
<td>2006</td>
<td>497.6</td>
</tr>
<tr>
<td>2007</td>
<td>553.5</td>
</tr>
<tr>
<td>2008</td>
<td>597.4</td>
</tr>
<tr>
<td>2009</td>
<td>752.2</td>
</tr>
</tbody>
</table>

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

Chip & PIN deployment period
…even types of fraud Chip and PIN was supposed to prevent

Card-not-present: up 20% to £398.2m

Lost and stolen: up 24% to £74.1m

Counterfeit: down 5% to £45.3m

Online banking: up 64% to £133.5m
...even types of fraud Chip and PIN was supposed to prevent

Card-not-present: up 20% to £398.2m
Lost and stolen: up 24% to £74.1m
Counterfeit: down 5% to £45.3m

within total fraud figures (£567.5m)

Fraud in UK: up 16% to £379.8m
Fraud abroad: up 25% to £187.7m
Chip and PIN transactions have three main stages

- **Card authentication**
  card proves it is real through providing a digital signature that the terminal can verify

- **Cardholder verification**
  card and terminal check that legitimate cardholder is present (normally by card verifying the PIN)

- **Transaction authorisation**
  terminal checks with bank that previous steps have been followed and the transaction should proceed
EMV protocol

1. Card details; digital signature

2. PIN entered by customer

3. PIN entered by customer; transaction description

4. PIN OK (yes/no); authorization cryptogram

5. Online transaction authorization (optional)

Card authentication
Cardholder verification
Transaction authorisation

- EMV protocol
- Issuer
- Customer
- Merchant
Card authentication

1. Card details; digital signature
2. PIN entered by customer
3. PIN entered by customer; transaction description
4. PIN OK (yes/no); authorization cryptogram
5. Online transaction authorization (optional)
Cardholder verification

1. Card details; digital signature
2. PIN entered by customer
3. PIN entered by customer; transaction description
4. PIN OK (yes/no); authorization cryptogram
5. Online transaction authorization (optional)

issuer

merchant

customer

card

result
Transaction authorisation

1. Card details; digital signature

2. PIN entered by customer

3. PIN entered by customer; transaction description

4. PIN OK (yes/no); authorization cryptogram

5. Online transaction authorization (optional)
Criminals have successfully bypassed Chip & PIN

1. Obtain static data as a result of flawed tamper resistance in Chip & PIN terminals
   - Then
   - Bypass card authentication through exploiting backwards compatibility mode

2. Steal cards
   - Then
   - Bypass cardholder verification by exploiting Chip and PIN protocol flaws

Counterfeit

Lost and Stolen
Sensitive data is sent unencrypted between the card and the terminal

- Card number, expiry date, cardholder name …
- Copy of magnetic stripe including CVV (for some cards)
- PIN to be checked by card

Chip and PIN terminals are supposed to protect this information against being recorded: tamper resistance
Tamper switches
Criminal gets all that is needed to make a magnetic stripe card

- Card number, expiry date
- CVV
- Cardholder’s PIN

Compromising a shop terminal now gives criminals enough information to make ATM withdrawal
Criminal gets all that is needed to make a magnetic stripe card

• Card number, expiry date

• CVV

• Cardholder’s PIN
Chip and PIN led to increase in counterfeit fraud
Card is responsible for cardholder verification

- Card states ways by which cardholder verification can be performed and the preference (e.g. first PIN, then signature)

- If PIN used, terminal sends PIN to card and card checks if correct

- PIN sometimes encrypted

- Response not encrypted or authenticated
VISA

Enter PIN

£5.00

CNL = NO

ENT = OK
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)

fake card

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

issuer

transaction; cryptogram

merchant

crook

$
Response from industry

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)

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

— UK Cards Association (February 2010)
L'imparable escroquerie à la carte bancaire

Un dispositif permettant de neutraliser la sécurité des puces des cartes bancaires a été utilisé pour la première fois en France. Plusieurs escrocs ont été arrêtés, mais cette arnaque n'a toujours pas de parade.

Publié le 24.01.2012

Des escrocs, particulièrement expérimentés, sont parvenus à contourner la sécurité de la puce incorporée aux cartes bancaires — réputée inviolable —, avant de multiplier les arnaques. La technique employée — mise au jour en 2010, par un universitaire anglais, le professeur Ross Anderson — a été appliquée pour la première fois en France par une équipe établie en région parisienne et dans le Nord. Plusieurs d'entre eux viennent d'être interpellés par les enquêteurs de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Selon les premiers éléments de l'enquête, les malfrats ont réalisé près de 6000 achats pour un préjudice de plus de 500 000 €.

Les policiers craignent de voir cette technique se répandre. « Pour l'heure, même si la personne qui s'est fait voler ou qui a perdu sa carte fait opposition sur cette dernière, les escrocs peuvent, malgré tout, continuer à s'en servir, note un policier spécialisé. C'est tout le problème de cette technique. »
Response from criminals

The unstoppable credit card scam

A device to neutralize the security chip bank card was used for the first time in France. Many scammers have been arrested, but this scam still does not have a parade.

Published on 24.01.2012

Crooks, highly experienced, have managed to bypass the security chip embedded bank cards - deemed invincible - before multiplying scams. The technique - unearthed in 2010 by a British academic, Professor Ross Anderson - was applied for the first time in France by a team based in the Paris region and in the north. Many of them have just been arrested by investigators from the Central Office for the Fight against Crime related to Information Technology and Communication (OCLCTIC). According to preliminary investigation, the thugs have made nearly 5,000 purchases for damages of more than €500,000. Officers fear that this technique spread. "For the time being, even if the person who was stolen or lost card opposed to the latter, scammers may nevertheless continue to use it, says a specialist officer. That's the whole problem with this scam. Thieves rajoutent on the map stolen a second chip that tricks the payment terminal at the merchant, into believing that the PIN is the correct compound. The perpetrator should then not exceed the amount of €428, by which a payment authorization is..."
Crooks, highly experienced, have managed to bypass the security chip embedded bank cards - deemed inviolable - before multiplying scams. The technique - unearthed in 2010 by a British academic, Professor Ross Anderson - was applied for the first time in France by a team based in the Paris region and in the north. Many of them have just been arrested by investigators from the Central Office for the Fight against crime related to information technology and communication (OCLCTIC). According to preliminary investigation, the thugs have made nearly 6,000 purchases for damages of more than €500,000. Officers fear that this technique spread. "For the time being, even if the person who was stolen or lost card opposed to the latter, scammers may nevertheless continue to use it, says a specialist officer. That's the whole problem with this scam. Thieves rajoutent on the map stolen a second chip that tricks the payment terminal at the merchant, into believing that the PIN is the correct compound. The perpetrators should then not exceed the amount of €100 at which a payment authorization is requested to the bank. But below this amount, the purchase is always accepted. "Investigators
Scammers **steal bank cards by stealth** to avoid attracting the attention of their victims too quickly.

They then modify the card, replacing **existing chip with another**, programmed with **software that blocks the security**.

The scammers can then **enter any PIN** to pay for purchases costing less than €100.

The scammers are buying, in general, **consumer products that can be quickly sold** on black-market.
Response from criminals

Response from criminals

Unpredictable numbers are essential to prove that real card is present.

1. Card details; digital signature

2. PIN entered by customer

3. PIN entered by customer; transaction description

4. PIN OK (yes/no); authorization cryptogram

5. Online transaction authorization (optional)
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
Reverse engineering
Reverse engineering
Surveying the problem
Exploiting the vulnerability

• 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
While Cambridge scientists have identified a theoretically potential, but technically complicated, type of card fraud, there is absolutely no evidence of this being undertaken in the real world.

— UK Cards Association (September 2014)
Quiz

- Please visit kahoot.it using smartphone, tablet or computer and enter PIN which will be shown next.
- You may play individually or in a team.
- Responses are anonymous (unless you choose to use your real name).
- You have 20 seconds to answer each question, and the faster you answer the more points you get.
- Does not count towards module assessment.
What about online fraud

<table>
<thead>
<tr>
<th>Year</th>
<th>Total (£m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>481.4</td>
</tr>
<tr>
<td>2005</td>
<td>452.6</td>
</tr>
<tr>
<td>2006</td>
<td>497.6</td>
</tr>
<tr>
<td>2007</td>
<td>553.5</td>
</tr>
<tr>
<td>2008</td>
<td>597.4</td>
</tr>
<tr>
<td>2009</td>
<td>752.2</td>
</tr>
</tbody>
</table>

The diagram shows the losses from various types of fraud, including:
- Card–not–present
- Counterfeit
- Lost and stolen
- Mail non–receipt
- ID theft
- Cheque
- Phone banking

The losses are measured in millions of pounds (£m).
Up as well

Card-not-present: up 20% to £398.2m

Online banking: up 64% to £133.5m
Pay a bill

Destination account number

Recipient name

Amount

One time password
EMV-CAP in the UK
EMV CAP’s weakness: attacker controls user experience

• User thinks they are typing random challenge but it is really part of an account number

• User thinks it’s OK that details on device don’t match those they entered on the computer

• User thinks they are performing a POS transaction but really it’s online banking
Usability is a security requirement
If something goes wrong do you get your money back?

- In the US, very likely yes (Regulation E & Z)

- In the EU, it’s more complicated (Payment Services Directive) …

  - Banks are permitted to refuse a refund for fraudulent transaction if customer has been “grossly negligent” in complying with bank terms and conditions

- What is considered “grossly negligent” and is this definition fair?
“You must take all reasonable precautions … including but are not limited to:

…
not choosing security details that may be easy to guess
…

Never writing down or otherwise recording your PIN and other security details in a way that can be understood by someone else

…
keeping your security details unique to your accounts with us

…
not allowing anyone else to have or use your card, security devices, PINs, or any of your security details”
Over $\frac{1}{3}$ of customers have 3 or more PINs

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 digits</td>
<td>1</td>
<td>88</td>
<td>65</td>
<td>41</td>
<td>31</td>
<td>8</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2.28</td>
</tr>
<tr>
<td>5 digits</td>
<td>233</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.05</td>
</tr>
<tr>
<td>6 digits</td>
<td>228</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.08</td>
</tr>
</tbody>
</table>

Table 2. Distribution of Participant's PINs

www.limesurvey.org

www.prolific.ac

IP address geolocation has significant error rates, but this confirms that our sample is predominantly from the UK as intended.
Almost half of PINs are used once per month or less frequently.

<table>
<thead>
<tr>
<th>Frequency of Use</th>
<th>4-digit PINs</th>
<th>5-digit PINs</th>
<th>6-digit PINs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#1</td>
<td>#2</td>
<td>#3</td>
</tr>
<tr>
<td>Every day</td>
<td>34</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Several times a week</td>
<td>117</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>Once per week</td>
<td>59</td>
<td>35</td>
<td>12</td>
</tr>
<tr>
<td>Once per month</td>
<td>21</td>
<td>37</td>
<td>24</td>
</tr>
<tr>
<td>Several times per year</td>
<td>6</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Once per year or less</td>
<td>1</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Never</td>
<td>2</td>
<td>12</td>
<td>14</td>
</tr>
</tbody>
</table>
Customers find ways to manage this otherwise impossible task

- About $\frac{1}{3}$ of customers write down their PIN and keep it with the card (e.g. in a wallet, diary, phone)

- About $\frac{1}{4}$ of customers use their PIN elsewhere (mainly mobile phone)

- About $\frac{1}{2}$ of customers share their PIN with someone else (mainly spouse/partner or other family members)

- These actions are treated as gross negligence if there is no other more likely explanation for fraud

- Is this fair? What can be done about it? Our work is ongoing
Conclusions

• Don’t underestimate criminals

• Better statistics are needed
  • Outside of UK
  • Customer losses

• Usability is a security requirement, especially when it comes to online payments
In late 2009, my colleagues and I discovered a serious vulnerability in EMV, the most widely used standard for smart card payments, known as “Chip and PIN” in the UK. We showed that it was possible for criminals to use a stolen credit or debit card without knowing the PIN, by tricking the terminal into thinking that any PIN is correct. We gave the banking industry advance notice of our discovery in early December 2009, to give them time to fix the problem before we published our research. After this period ex-