Payment Security: Attacks & Defences

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

Losses (£m)

Year


Total, ex phone (£m)

0 50 100 150 200 250 300

Card–not–present

Counterfeit

Lost and stolen

Mail non–receipt

Cheque fraud

ID theft

Online banking

Phone banking

Chip & PIN deployment period


0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300

0 50 100 150 200 250 300
…even types of fraud Chip and PIN was supposed to prevent

Card-not-present: up 22% to £301m

Lost and stolen: up 7% to £58.9m
Counterfeit: up 3% to £43.4m
...even types of fraud Chip and PIN was supposed to prevent

Card-not-present: up 22% to £301m
Lost and stolen: up 7% to £58.9m
Counterfeit: up 3% to £43.4m

within total fraud figures

UK retail face-to-face: up 11% to £60.8m
UK cash machine: up 10% to £31.9m
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.
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)

issuer

transaction; cryptogram

merchant

result

card

2. PIN entered by customer

$
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)
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)

result: transaction; cryptogram
Criminals have successfully bypassed Chip & PIN

Obtain static data as a result of flawed tamper resistance in Chip & PIN terminals

then

Bypass card authentication through exploiting backwards compatibility mode

Steal cards

then

Bypass cardholder verification by exploiting Chip and PIN protocol flaws
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
Tamper mesh
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

CWL = 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)
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 malfaiteurs 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... »
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 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 rajouten 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.
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
HOW DOES THE STRATEGY WORK

1. Scammers **steal bank cards by stealth** to avoid attracting the attention of their victims too quickly.

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

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

4. The scammers are buying, in general, **consumer products that can be quickly sold** on black-market.
Unpredictable numbers are essential to prove that a real card is present.
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
Response from industry

"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)"
What about online fraud?

Card-not-present: up 22% to £301m

Online banking: up 3% to £40.9m
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
Research at UCL
Research at UCL

• Simply Secure
  • Collaboration with Dropbox, Google
  • Designing and evaluating easy ways to securely communicate and authenticate
• Next generation privacy systems
  • Protecting who you are talking to, not just what you’re saying
• Measuring security
  • From a craft to a science

Studentships available!
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