Verified by Visa and MasterCard SecureCode
Vulnerabilities and Consequences

Year
Losses (£m)
2004 2005 2006 2007 2008
0 50 100 150 200 250 300
●
●
●
●
●
●
● ●
●
● ● ●
●
●
●
●
● ●

Steven J. Murdoch
http://www.cl.cam.ac.uk/users/sjm217/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

Chip & PIN is now being deployed worldwide

- Chip & PIN, based on the EMV (EuroPay, Mastercard, Visa) standard, is deployed throughout most of Europe
- The UK was an early adopter (started 2003, complete by 2006)
- Deployment has started in Canada and Mexico
- Transactions (point-of-sale and ATM) are authorized using a smart card and PIN
- Chip is more difficult to clone than older magnetic stripe, but there are still vulnerabilities (see my talk tomorrow, 13:45)
# UK card fraud continues to rise

![Graph showing UK card fraud losses from 2004 to 2008.](image)

<table>
<thead>
<tr>
<th>Year</th>
<th>Card-not-present</th>
<th>Counterfeit</th>
<th>Lost and stolen</th>
<th>ID theft</th>
<th>Mail non-receipt</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>0</td>
<td>50</td>
<td>100</td>
<td>150</td>
<td>200</td>
</tr>
<tr>
<td>2005</td>
<td>50</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>250</td>
</tr>
<tr>
<td>2006</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>250</td>
<td>300</td>
</tr>
<tr>
<td>2007</td>
<td>150</td>
<td>200</td>
<td>250</td>
<td>300</td>
<td>350</td>
</tr>
<tr>
<td>2008</td>
<td>200</td>
<td>250</td>
<td>300</td>
<td>350</td>
<td>400</td>
</tr>
</tbody>
</table>

**Source:** APACS (March 2009)

**Totals (£m):**
- 505 (2004)
- 440 (2005)
- 427 (2006)
- 535 (2007)
- 610 (2008)
Criminals have adapted to Chip & PIN

Since 2003, fraud has shifted to areas where Chip & PIN is not used

- **Card not present** (up 118% to £328.4m)
- Fraud abroad (up 149% to £230.1m)
- Online banking (up 330% to £52.5m)

- Banks have rolled out mitigation measures in each of these categories (with varying success)
- In this talk I will discuss one defence against card-not-present fraud: **3-D Secure**
- Branded as Verified by Visa and MasterCard SecureCode
Customers enter a password online

Online shopping website shows a password form on check-out
Customer’s bank verifies the password to authorize the transaction
The form is often embedded
3-D Secure suffers from a number of security vulnerabilities

- Enrolment is often weak:
  - e.g. date of birth and card details for Bank of Scotland
- Customer cannot tell who will see their password:
  - Password should only be sent to the bank, but
  - A criminal could put up a fake form
- Often customers have increased liability for such transactions:
  - Normally merchants take the losses, and a charge-back fee
  - With a 3-D Secure password, the customer is *de facto* liable
Criminals have already started attacks

When I called my bank, and said that the site securesuite.co.uk asked for my password, they said is was a scam.

Actually this was legitimate, and run by RSA (aka Cyota/EMC), who provide 3-D Secure services to many banks.
The customer has been left out

- The “3-D” part of the name indicates the three domains protected by 3-D Secure:
  - Acquirer (merchant and their bank)
  - Issuer (the customer’s bank)
  - Payment System (MasterCard or Visa)

- Note that there is no mention of the customer here!

- Liability has shifted to the customer, but they have not been given the ability to prevent fraud
- Criminals are taking advantage of this weakness
- More sophisticated attacks are likely
- Regulatory pressure is needed to fix the problem

Questions?