Online Banking Security

Steven J. Murdoch

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

work with Saar Drimer, Ross Anderson, Mike Bond

UNIVERSITY OF CAMBRIDGE

Computer Laboratory
UK fraud figures 2004–2011

Losses to banks and merchants (£m)

Year
2004 2005 2006 2007 2008 2009 2010 2011
563.1 503 491.2 591.4 704.3 529.6 441 410.6

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

Chip & PIN deployment period

Source: Financial Fraud Action UK
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

Dear Customer

Account Protection Update, To ensure that scam and other account threats, it's strongly recommended to update account protection.

Click on "Protection" to continue the process.

Protection.

Online Internet Banking Security Center
Halifax Internet Banking.

Thanks for your cooperation.

Fraud Prevention Unit
Legal Advisor
Halifax PLC.

Please do not reply to this email. Mail sent to this address.
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

<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/xml,application/json</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 X)</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
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

<table>
<thead>
<tr>
<th>Identify</th>
<th>00000000000000</th>
<th>0000000000</th>
</tr>
</thead>
<tbody>
<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.
CAP readers help muggers

Police think French pair tortured for pin details

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/