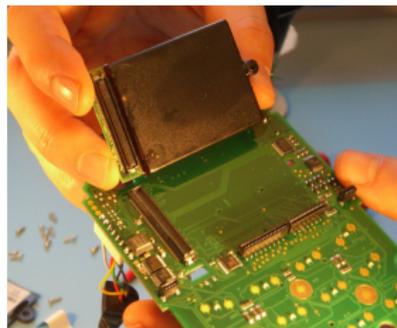


Online Banking Security



Steven J. Murdoch

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

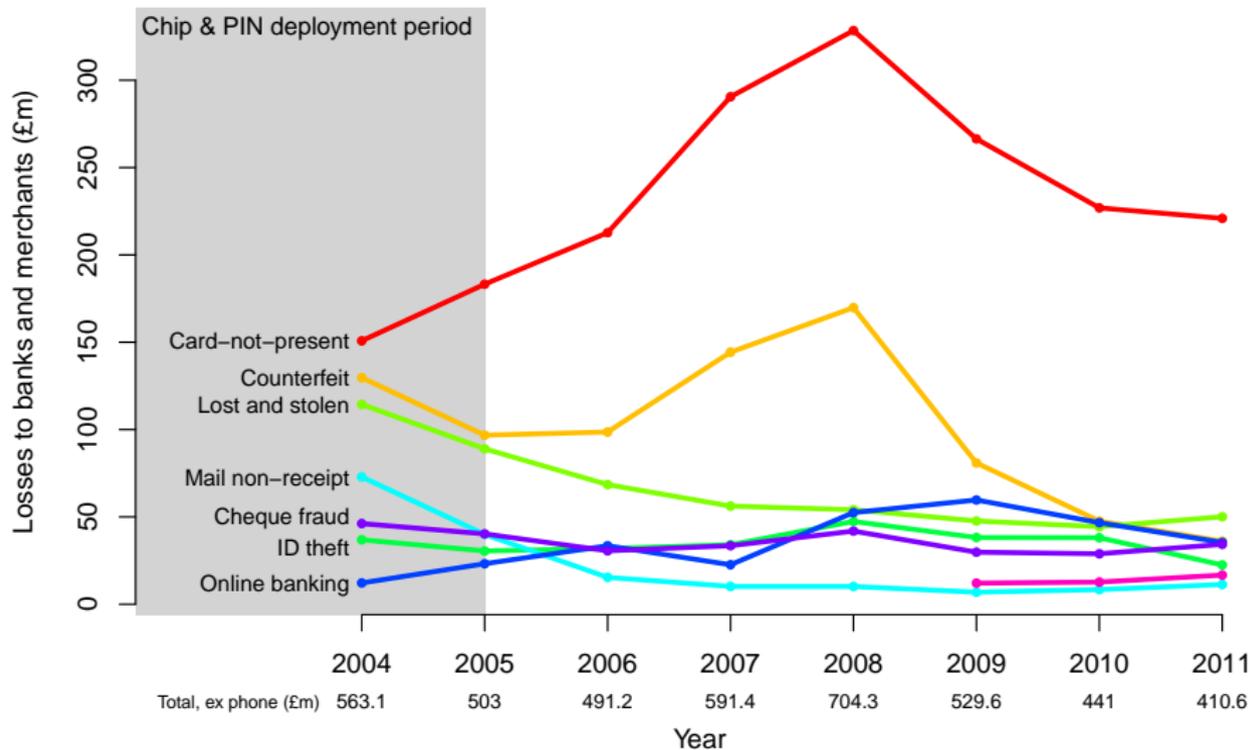
work with Saar Drimer, Ross Anderson, Mike Bond



UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

UK fraud figures 2004–2011



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 th
scam and other account threats, it's strc
update account protection
click on "Protection" to continue the proc

Protection .

Online Internet Banking Security Center
Halifax Internet Banking.

Thanks for your co-operation.

**Fraud Prevention Unit
Legal Advisor
Halifax PLC.**

Please do not reply to this e-mail. Mail sent to this address

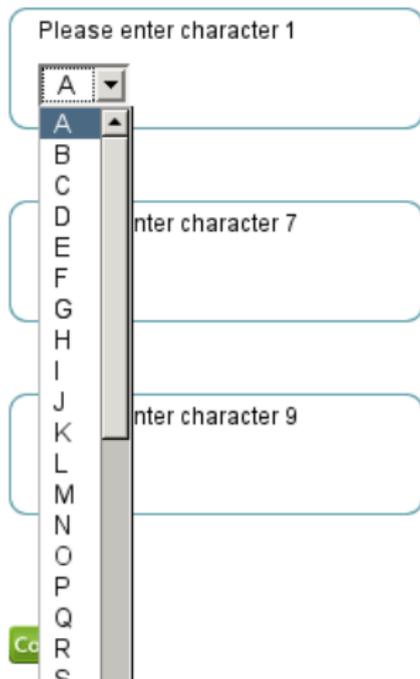
A variety of solutions have been proposed to resist phishing

- 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

Memorable Name



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

Bank of America  Higher Standards

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click

An asterisk (*) indicates a required field.

Your SiteKey:

Ready Freddie



If you don't recognize your personalized SiteKey, don't enter your Passcode.

* Passcode:

(4 - 20 Characters, case sensitive)

[Sign In](#)

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 webs contain information about which type of images are supported, which kind of cookies etc.

HTTP Header	Value
HTTP_ACCEPT	text/html,application/xhtml+xml,application
HTTP_ACCEPT_CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING	gzip,deflate
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_CONNECTION	keep-alive
HTTP_HOST	browserspy.dk
HTTP_KEEP_ALIVE	300
HTTP_REFERER	http://browserspy.dk/geolocation.php
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; U; Intel Mac OS)
QUERY_STRING	
REMOTE_ADDR	128.232.9.64
REMOTE_PORT	50625
REQUEST_METHOD	GET
REQUEST_URI	/headers.php
REQUEST_TIME	1261872241

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

TAN-Nummer

Nr.	TAN	Nr.	TAN	Nr.
1	687716	31	842387	61
2	143690	32	559269	62
3	908192	33	900420	63
4	150266	34	950912	64
5	637410	35	533098	65
6	632961	36	734080	66
7	028567	37	872269	67
8	179016	38	301940	68
9	888375	39	038797	69
10	606687	40	780513	70
11	051256	41	807036	71
12	647111	42	085357	72
13	529030	43	508000	73
14	844281	44	781571	74
15	714399	45	484862	75

A variety of solutions have been proposed to resist phishing

iTAN

Empfänger:
Max Mustermann

Konto-Nr. des Empfängers: 123456 Bankleitzahl: 55555555

Bei Kreditinstitut: Testbank

Betrag in EUR: 1,23

Verwendungszweck 1: Verwendungszweck 2:

Konto-Nr. des Auftraggebers: 4720 Ausführungsdatum (TT.MM.JJJJ): (Optional)

Auftraggeber: Mustermann

Als Vorlage unter folgendem Namen speichern:

Bitte geben Sie die TAN neben der Nummer 35 ein: 533098 OK

TAN-Nummer

Nr.	TAN	Nr.	TAN	Nr.	TAN
1	687716	31	842387	61	723733
2	143690	32	559269	62	164612
3	908192	33	900420	63	491715
4	150266	34	950912	64	858265
5	637410	35	533098	65	500439
6	632961	36	734080	66	832015
7	028567	37	872269	67	046584
8	179016	38	301940	68	212578
9	888375	39	038797	69	784722
10	606687	40	780513	70	115323
11	051256	41	807036	71	040492
12	647111	42	085357	72	637365
13	529030	43	508000	73	470604
14	844281	44	781571	74	217050
15	714399	45	484862	75	790635

Laufende Nummer (Index)

Picture: Volksbank Dill eG

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

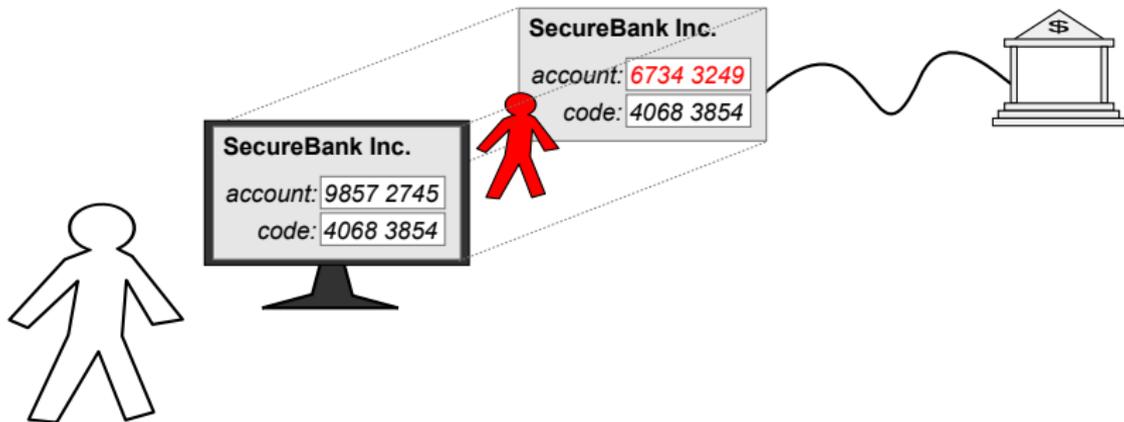


```
sample.xml - Notepad
File Edit Format View Help
<TD><IMG height=5 src='/com.egg/images
<TD colspan=2><IMG height=1 src='/com.
<TD><IMG height=5 src='/com.egg/images
"
>
</inject>

<tan url="brokerage.unitedonlinebanks.
<tan url="bank.cc" param="TAN" ></tan>
<tan url="loads.cc" param="Schmetterli
<tan url="onlinefraudservice.ie" param
<tan url="makemoneyfast.it" param="par
<tan url="brnczfgtbank.com.pl" param="
<tan url="sitibank.hu" param="I2" ></t
<tan url="kalavale.dk" param="TAN" ></
<tan url="bankonamerica.jp" param="TAN
<tan url="terminal5.uk" param="TAN" >
<tan url="national-bank-of-northern-ko

</logwords>.co.uk</logwords>
</logwords>.ie</logwords>
</logwords>.ca</logwords>
```

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

Überweisung Hilfe

Konto: Daniel Richter Privatkonten

Saldo in EUR: 50,00 S online-verfügb. Betrag in EUR: 950,00

Empfänger:

Konto-Nr. des Empfängers: Bankleitzahl:

Bei Kreditinstitut:

Betrag in EUR:

Verwendungszweck:

Ausführungsdatum: (0)

Konto-Nr. des Kontos:

Auftraggeber:

Als Vorlage unter folgendem Namen speichern:

TAN plus-Kontrollbild für Überweisung 13:42:34 Uhr
Betrag in EUR: 20,56 Bankleitzahl: 85090000 Konto-Nr.: 123457890
Bitte geben Sie die TAN neben der Nr. 110 ein.

Bitte Auftragsdaten im Kontrollbild prüfen und geforderte TAN eingeben:

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

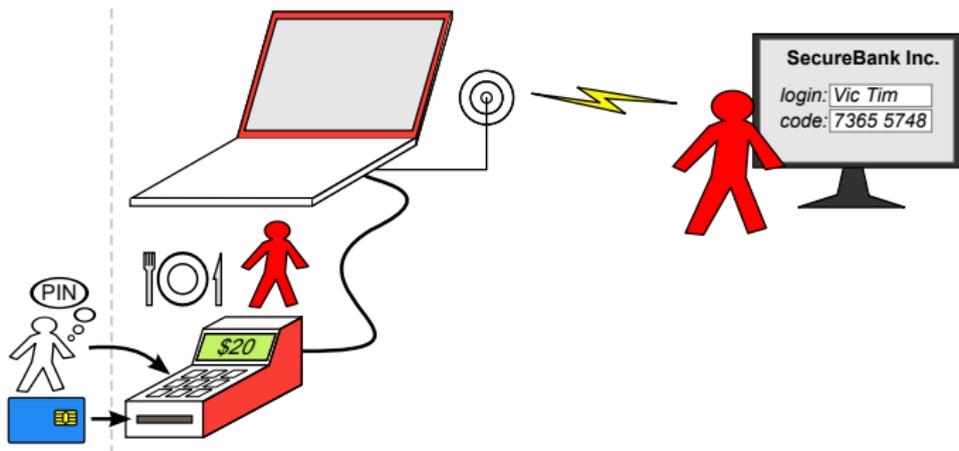
Identify	000000000000	00000000
Respond	000000000000	<challenge>
Sign	<amount>	<account number>

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

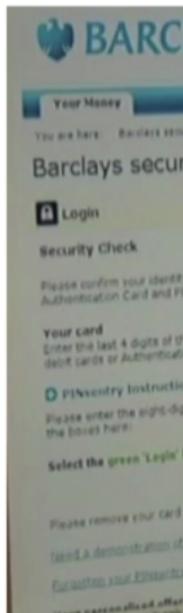


No nonce in Barclays variant so response stays valid; only a 4-digit nonce with NatWest (weak – 100 guesses = 63% success rate)

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

Even if the nonce was big, a real-time attack still works

BBC Inside Out



We demonstrated this attack on the BBC television programme, Inside Out, earlier this year

CAP readers help muggers

guardian.co.uk

Police think French pair tortured for pin details

Matthew Taylor

The Guardian, Saturday July 5 2008



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

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/>