

# Banking Security Architecture



Steven J. Murdoch

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

work with Saar Drimer, Ross Anderson, Mike Bond



UNIVERSITY OF  
CAMBRIDGE

Computer Laboratory

[www.torproject.org](http://www.torproject.org)

## Chip & PIN has now been running in the UK for about 5 years

- Chip & PIN, based on the EMV (EuroPay, MasterCard, Visa) standard, is deployed throughout most of Europe
- In process of roll-out elsewhere
- Customer inserts contact-smart card at point of sale, and enters their PIN
- UK was an early adopter: rollout in 2003–2005; mandatory in 2006
- Chip & PIN changed many things, although not quite what people expected

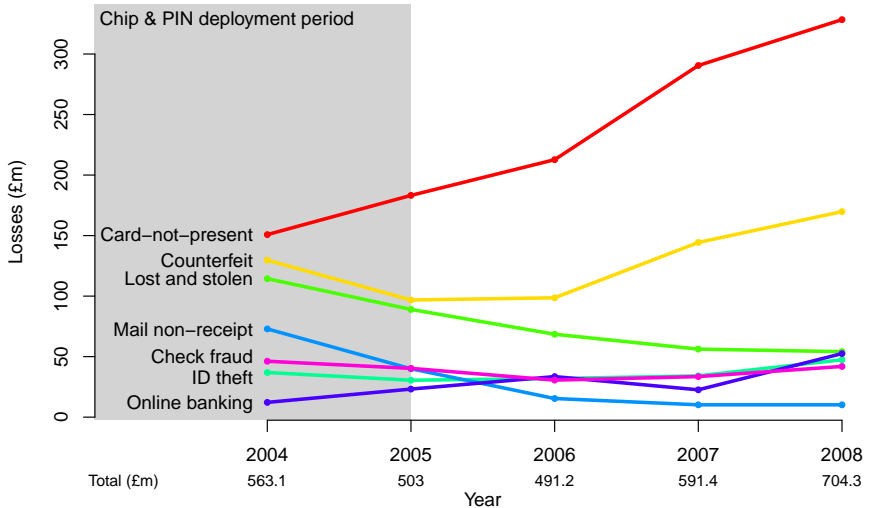


## Card payments in the UK are different from the EU (and elsewhere)

|                          | <b>Before Chip &amp; PIN</b> | <b>After Chip &amp; PIN</b> |
|--------------------------|------------------------------|-----------------------------|
| <b>Cards</b>             | magstrip                     | magstrip and chip           |
| <b>Card verification</b> | magstrip                     | chip if possible            |
| <b>ATM</b>               | PIN used                     | PIN used                    |
| <b>Point-of-sale</b>     | signature used               | PIN used                    |


- No difference between credit and debit cards
- No ID check at point-of-sale (signature rarely checked either)
- Introducing Chip & PIN really made two changes:
  - Chip used for authenticating card (ATM and PoS)
  - PIN used for authenticating customer (only new for PoS)
- The effects of the two changes are often conflated


# UK fraud figures 2004–2008




## Key trends 2004–2008


- Abuse of authentic cards:

- Lost and stolen: **down** 53%  to £54.1m

- Mail non-receipt: **down** 86%  to £10.2m

- Counterfeit: **up** 31%  to £169.8m

- Non-card security:

- Card-not-present: **up** 118%  to £328.4m

- ID theft: **up** 28%  to £47.4m

- Online: **up** 330%  to £52.5m

- Check: **down** 9%  to £41.9m

- **Total**: dip in 2005–2006, but **up** 25%  to £704.3m

## Counterfeit fraud mainly exploited backwards compatibility features

- Upgrading to Chip & PIN was too complex and expensive to complete in one step
- Instead, chip cards continued to have a magstrip
  - Used in terminals without functioning chip readers (e.g. abroad)
  - Act as a backup if the chip failed
- Chip also contained a full copy of the magstrip
  - Simplifies issuer upgrade
  - Chip transactions can be processed by systems designed to process magstrip
- Criminals changed their tactics to exploit these features, and so counterfeit fraud did not fall as hoped
- Fraud against UK cardholders moved outside of the UK

# Criminals could now get cash

Criminals collected:

- card details by a “double-swipe”, or tapping the terminal/phone line
- PIN by setting up a camera, tapping the terminal, or just watching

Cloned magstrip card then used in an ATM (typically abroad)

In some ways, Chip & PIN made the situation worse

- PINs are used much more often (not just ATM)
- PoS terminals are harder to secure than an ATM



Tonight (ITV, 2007-05-04)

## Terminal tamper proofing is supposed to protect the PIN in transit

- In PoS transaction, PIN is sent from PIN entry device (PED) to card for verification
- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD \$25,000 per PED**



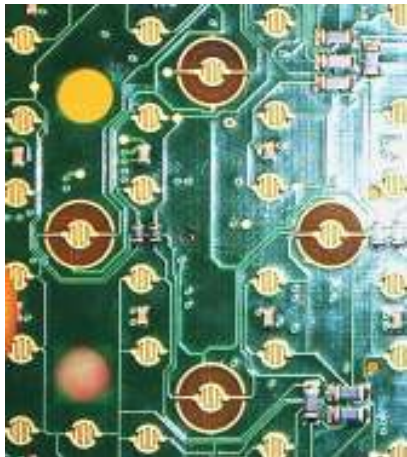


## Protection measures: tamper switches



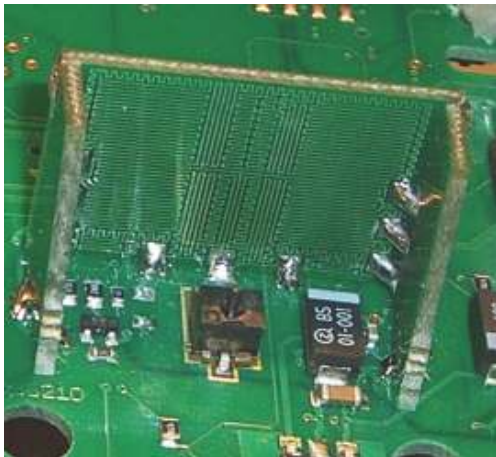
Ingenico i3300

## Protection measures: tamper switches



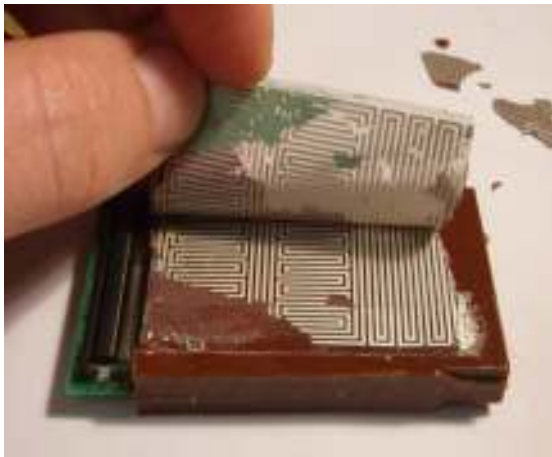
Ingenico i3300

## Protection measures: tamper meshes



Ingenico i3300

## Protection measures: tamper meshes



Ingenico i3300

## BBC Newsnight filmed our demonstration for national TV



BBC Newsnight, BBC2, 26 February 2008

Holes in the tamper mesh allow the communication line to be tapped



An easily accessible compartment can hide a recording device

## This type of fraud is still a serious problem in the UK

Initially (2005), PEDs were tampered on a small scale and installed by someone impersonating a service engineer

PED was collected later, and card details extracted

Now PEDs are being tampered with at or near their point of manufacture

A cellphone module is inserted so it can send back lists of card numbers and PINs automatically



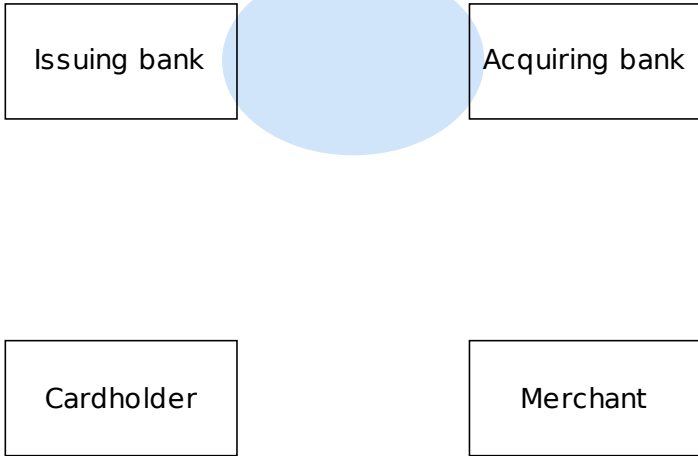
## Chip & PIN vulnerabilities

- Fallback vulnerabilities are not strictly-speaking a Chip & PIN vulnerability
- However, vulnerabilities do exist with Chip & PIN
- To understand these, we need some more background information
- To pay, the customer inserts their smart card into a payment terminal
- The chip and terminal exchange information, fulfilling three goals:
  - **Card authentication:** that the card presented is genuine
  - **Cardholder verification:** that the customer presenting the card is the authorized cardholder
  - **Transaction authorization:** that the issuing bank accepts the transaction



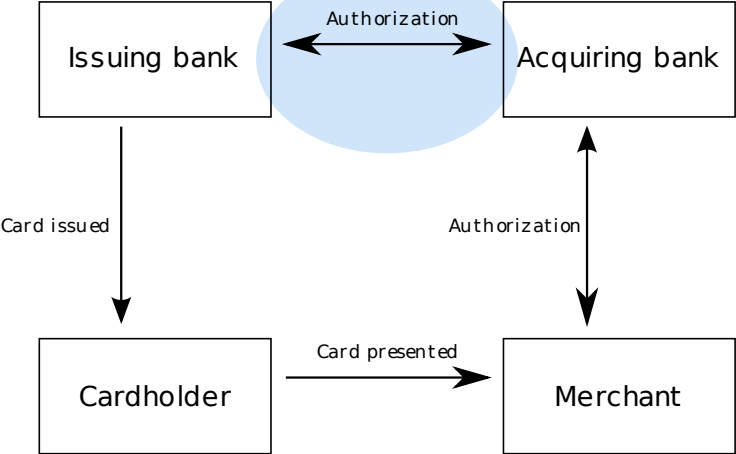
# Terminology

Payment system network  
(MasterCard/Visa/etc.)



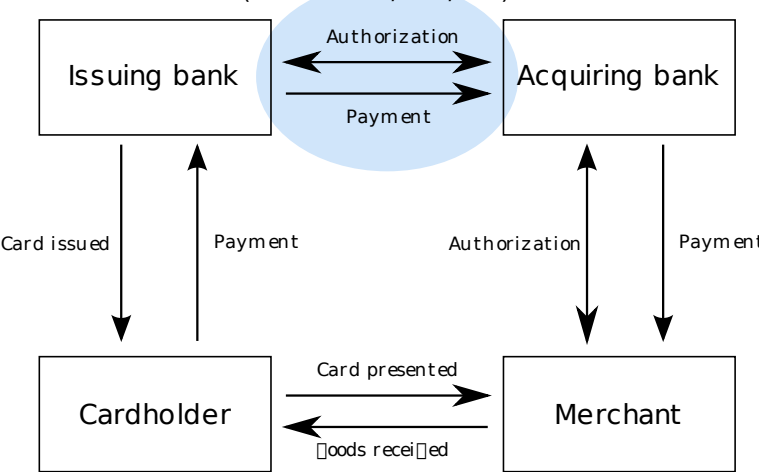
# Terminology

Payment system network  
(MasterCard/Visa/etc.)

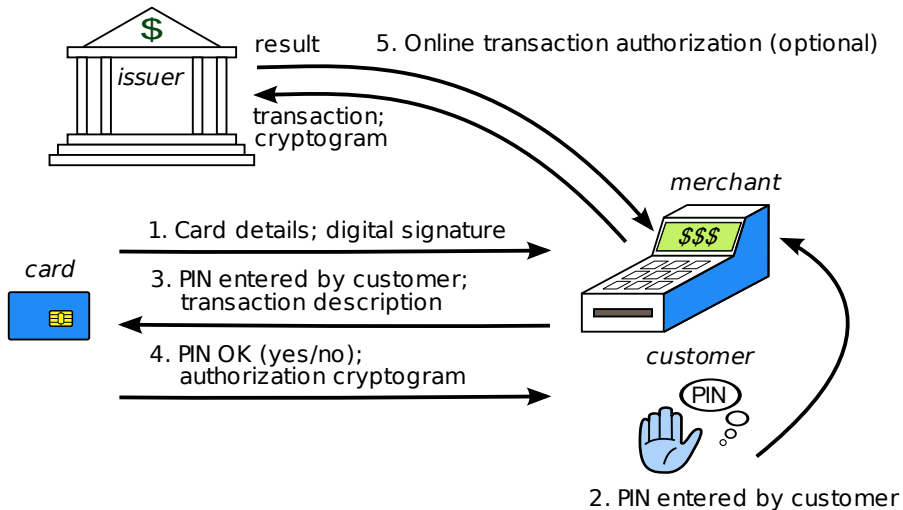


# Terminology

Payment system network  
(MasterCard/Visa/etc.)

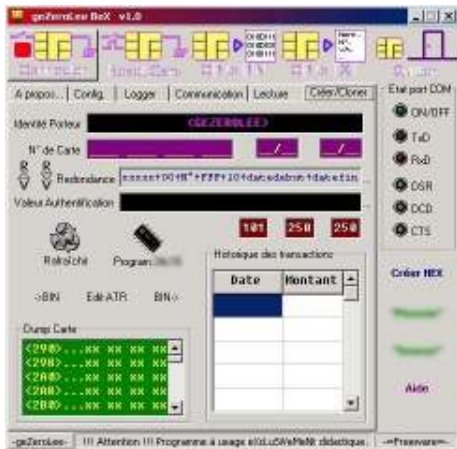


# Simplified Chip & PIN transaction

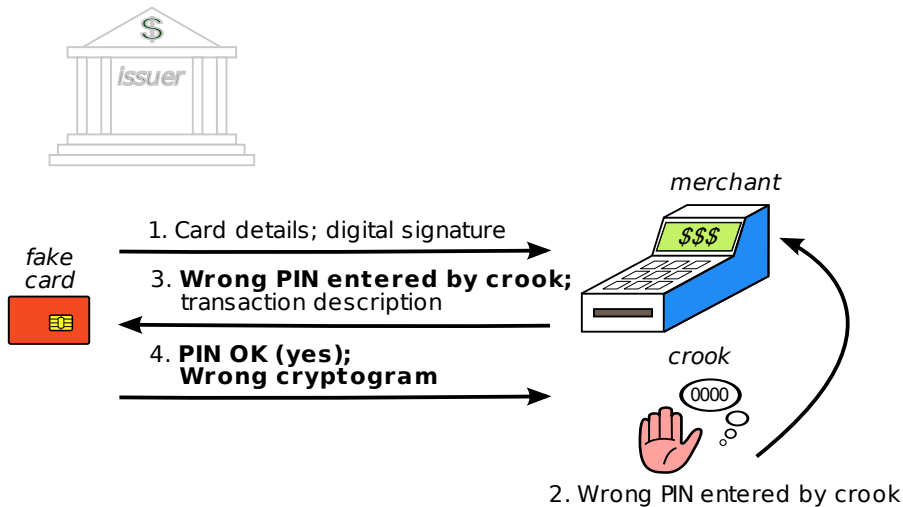


## The YES-card attack

- Criminals can copy EMV chip cards
- This fake card will contain the correct digital signature
- Also, it can be programmed to accept any PIN (hence “YES”)
- However, the fake card can be detected by online transaction authorization



# The YES-card attack



## Defending against the YES-card

- YES-cards are responsible for a relatively small amount of fraud
- Can be detected by **online** transaction authorization
- Can also be detected by more advanced chip cards which can produce a dynamic digital signature
  - **DDA** (dynamic data authentication), as opposed to **SDA** (static data authentication)
  - Previously DDA cards were prohibitively expensive, but now cost about the same as SDA cards
- PIN verification can be performed online too, rather than allowing the card to do so
  - Need to securely send the PIN back to the issuer
  - UK ATMs use **online** PIN verification
  - UK point-of-sale terminals use **offline** PIN verification

Our attack was shown on BBC1's consumer program, in February 2007



*“We got our highest ratings of the run for the story (6.2 million, making it the most watched factual programme of last week)... it’s provoked quite a response from viewers.” – Rob Unsworth, Editor, “Watchdog”*

**Our demonstration helped many cardholders reach a favourable resolution with banks**



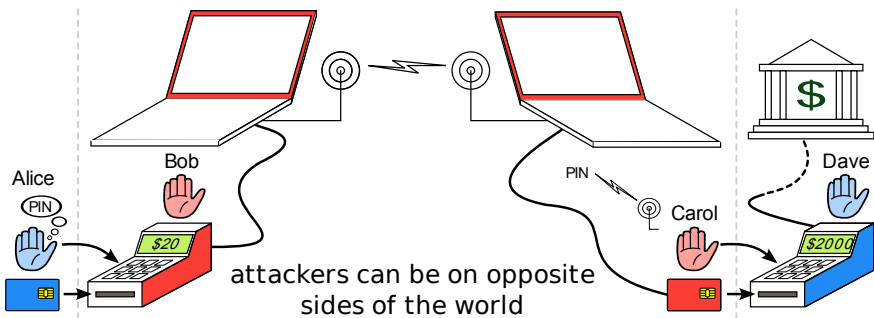
The relay attack: Alice thinks she is paying \$20, but is actually charged \$2 000 for a purchase elsewhere

Alice



Honest cardholder Alice and merchant Dave are unwitting participants in the relay attack

## The relay attack: Alice thinks she is paying \$20, but is actually charged \$2 000 for a purchase elsewhere



Alice inserts her card into Bob's *fake* terminal, while Carol inserts a fake card into Dave's *real* terminal. Using wireless communication the \$2 000 purchase is debited from Alice's account

## The no-PIN attack

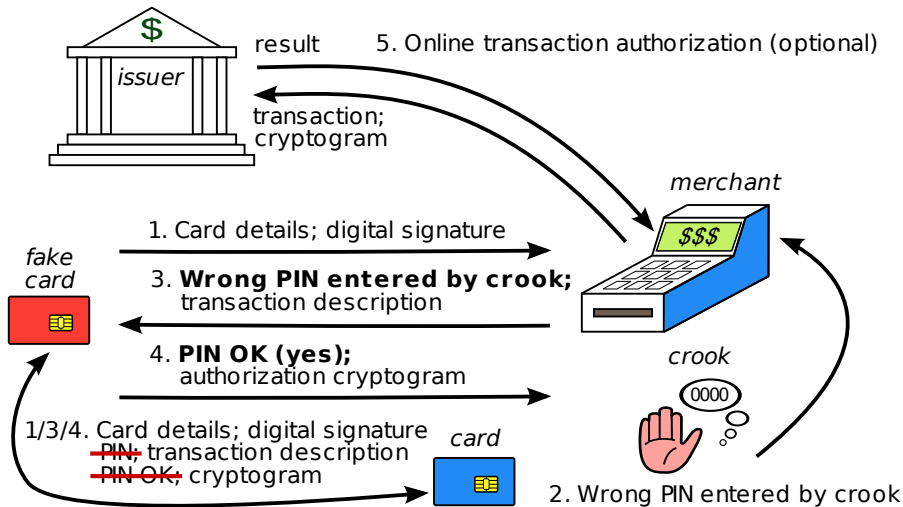
- The no-PIN attack allows criminals to use a stolen card without knowing its PIN
- It requires inserting a device between the genuine card and payment terminal
- This attack works even for **online** transactions, and **DDA** cards



BBC Newsnight filmed our  
demonstration for national TV

BBC Newsnight, BBC2, 11 February 2010

# The no-PIN attack



## Why does this attack work?

- Complexity
  - 4 000 pages of specification!
  - Data needs to be combined from several different sources and specifications (EMV, MasterCard, ISO, APACS)
  - Despite quantity, no specification actually describes the necessary checks
- Bad design of flags
  - Card produces a flag (card verification results – CVR) which says whether PIN verification succeeded
  - But this flag is in an issuer-specific format and so cannot be parsed by the terminal
  - Flag produced by terminal (TVR) is set **either** if PIN verification succeeded **or** terminal skipped check
  - Other flags may exist (country-specific, covered by APACS and ISO), but evidently are not checked in practice
- Implementation problems
  - Since issuers don't check flags, terminals mis-report state

## Current and proposed defences

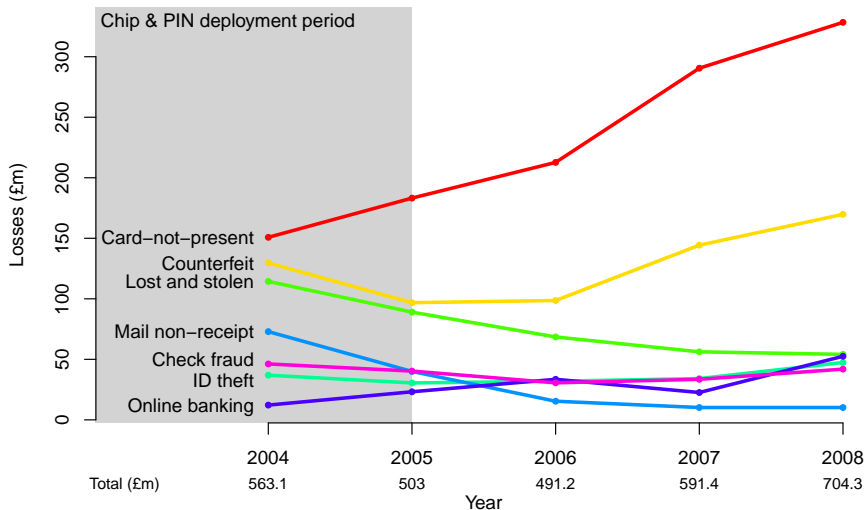
- Skimming
  - iCVV: Slightly modifying copy of magnetic strip stored on chip
  - Disabling fallback: Preventing magnetic strip cards from being used in EMV-enabled terminals
  - Better control of terminals: Prevent skimmers from being installed
- YES-card
  - Dynamic Data Authentication (DDA): Do RSA on card
  - Online authentication: Require that all transactions occur online
- Relay attack
  - Distance bounding protocol between terminal and card
- No-PIN attack
  - Defences currently still being worked on
  - Extra consistency checks at issuer may be able to spot the attack
  - Combined DDA/Application Cryptogram Generation (CDA): Move public key authentication stage to the end

## Effect on consumers

- There was some minor resistance to Chip and PIN
- After deployment, the question of liability became important
- Before Chip and PIN, banks generally refunded victims of fraud, because it was well known that magstrip cards could be cloned and signature forged
- After Chip and PIN, banks took the position that if the chip and PIN were used, the customer must have been negligent and hence liable (level of proof is low)
- The industry does not keep statistics, but a survey from the Consumer Association found that 20% of fraud victims do not get their money bank
- UK costs rules and regulatory regime makes fixing this difficult



# Online banking fraud is a significant and growing problem in the 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 Adviser**  
**Halifax PLC.**

---

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

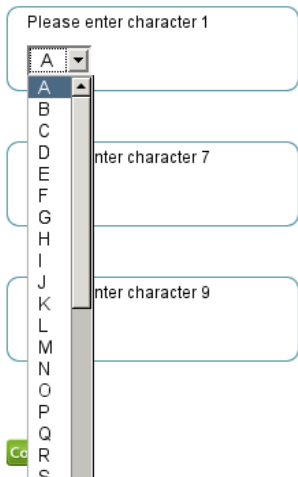
# A variety of solutions have been proposed to resist phishing

- 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

## 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

### 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

The image shows a banking transaction form with a table of iTANs. A box highlights the 35th iTAN, and an arrow points from it to the input field in the form below.

**Empfänger:**  
Rzr. Buchtitel: \_\_\_\_\_  
Konto-Nr. des Empfängers: \_\_\_\_\_ Bankleitzahl: 55555555  
Bei Kreditinstitut: \_\_\_\_\_  
Textbaustein: \_\_\_\_\_  
Betrag in EUR: \_\_\_\_\_  
Kurz: \_\_\_\_\_  
Verwendungszweck 1: \_\_\_\_\_ Verwendungszweck 2: \_\_\_\_\_  
Konto-Nr. des Auftraggebers: \_\_\_\_\_ Ausführungsdatum (TT.MM.YYYY): \_\_\_\_\_  
430) \_\_\_\_\_ (Optional)  
Auftraggeber: \_\_\_\_\_  
Bankleitzahl: \_\_\_\_\_  
Als Vorlage unter folgendem Namen speichern: \_\_\_\_\_

**TAN-Nummer**

| Nr. | TAN    | Nr. | TAN    | Nr. | TAN    |
|-----|--------|-----|--------|-----|--------|
| 1   | 007710 | 31  | 042287 | 61  | 722722 |
| 2   | 143690 | 32  | 550269 | 62  | 164612 |
| 3   | 908190 | 33  | 900420 | 63  | 491715 |
| 4   | 150206 | 34  | 250912 | 64  | 858265 |
| 5   | 637410 | 35  | 533098 | 65  | 500439 |
| 6   | 622961 | 36  | 739080 | 66  | 932015 |
| 7   | 022267 | 37  | 072269 | 67  | 046504 |
| 8   | 178016 | 38  | 301940 | 68  | 212578 |
| 9   | 888375 | 39  | 036797 | 69  | 784722 |
| 10  | 606687 | 40  | 700513 | 70  | 115323 |
| 11  | 053256 | 41  | 007036 | 71  | 040492 |
| 12  | 547111 | 42  | 006257 | 72  | 627265 |
| 13  | 528030 | 43  | 509000 | 73  | 470604 |
| 14  | 044281 | 44  | 701671 | 74  | 217050 |
| 15  | 714399 | 45  | 484862 | 75  | 790635 |

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

Laufende Nummer (Index)

Picture: Volksbank Dill eG

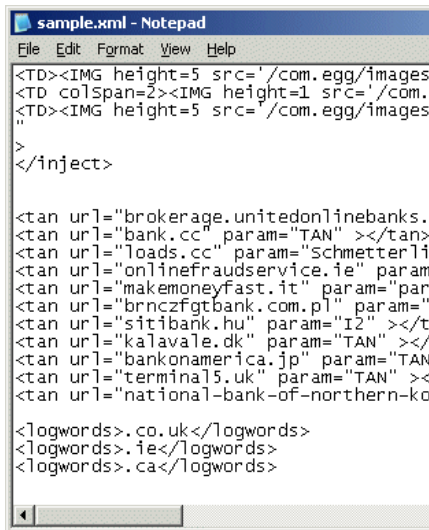
Customer must provide the requested one time password

## 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



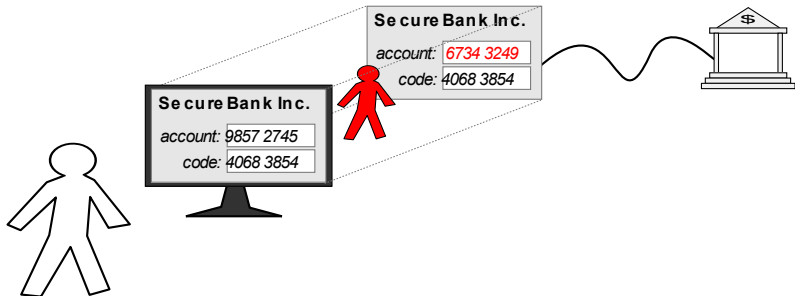
```
sample.xml - Notepad
File Edit Format View Help
<TD><IMG height=5 src='/com.egg/images
<TD colspan=2><IMG height=1 src='/com.
<TD><IMG height=5 src='/com.egg/images
"
>
</inject>

<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

The image shows a screenshot of a German online banking interface for a transfer (Überweisung). The form includes fields for account number, recipient name, account number, and amount. Two orange callout boxes are overlaid on the form:

- The first callout box points to the transaction details and ITAN field, containing the text: "Transaktionsdaten und Anforderung ITAN".
- The second callout box points to the background of the form, containing the text: "Geburtsdatum des VR-NetKey-Inhabers als „Wasserzeichen“ im Hintergrund,".

At the bottom of the form, there is a blue bar with a warning icon and the text: "Bitte auftragsgültig in Kontrollbild prüfen und gefällende TAN eingeben: 123456". Below this bar are buttons for "Eingaben kopieren" and "Abbrechen".

## 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)

Full details are in the paper (linked from the Fahrplan)

## 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

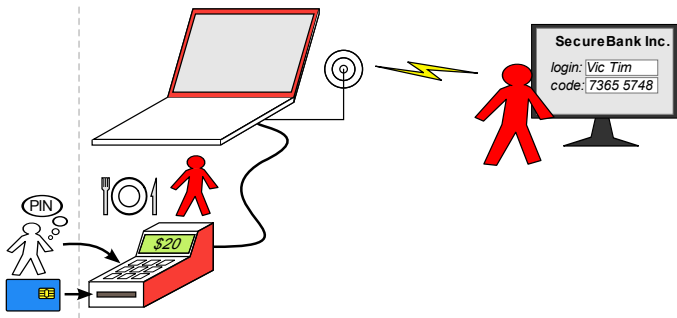
Banks have inconsistent usage

**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**

## 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



## 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 (Java, Blackberry, Android, Symbian, iPhone, etc. . . )
- 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/>