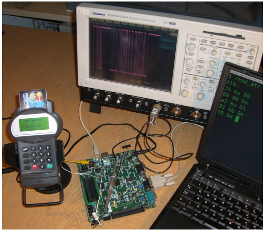
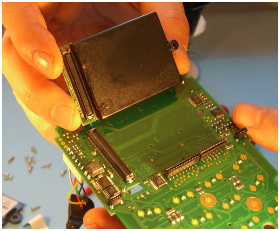
Banking Security: Attacks and Defences





Steven J. Murdoch

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

work with Saar Drimer, Ross Anderson, Mike Bond

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Tor
www.torproject.org

OWASP, March 2013, Leuven, BE

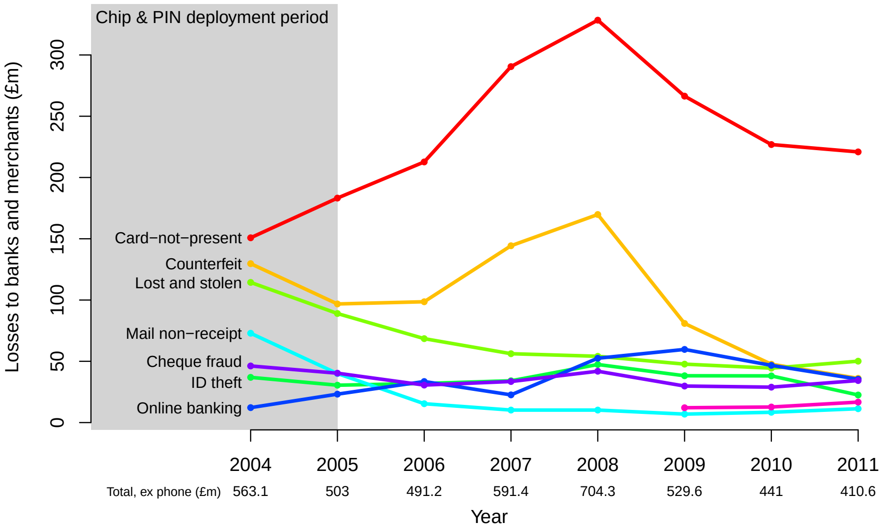
Chip & PIN has now been running in the UK for about 5 years

- 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-smartcard 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

Chip and PIN

EMVCo

UK fraud figures 2004–2011



Source: Financial Fraud Action UK

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

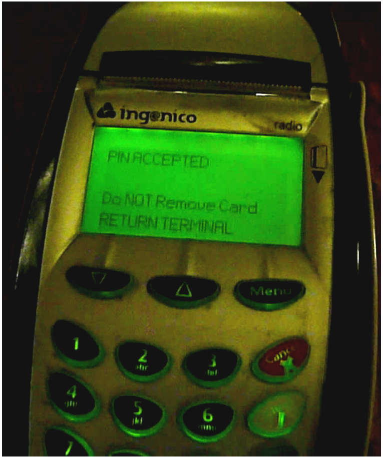
Tonight (ITV, 2007-05-04)

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, fulfiling 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

The no-PIN attack

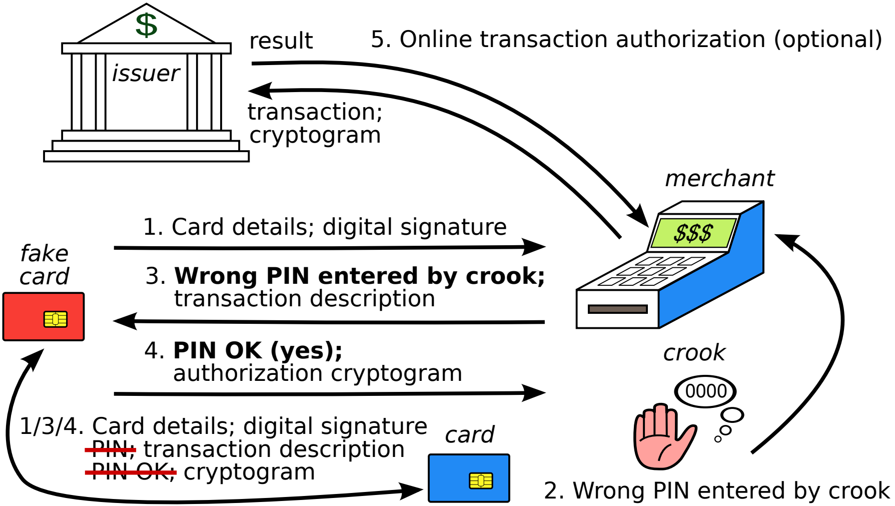
- The no-PIN attack allows criminals to use a stolen card without knowing its PIN
- It requires inserting a device between the genuine card and payment terminal
- This attack works even for online transactions, and DDA cards



BBC Newsnight filmed our demonstration for national TV

BBC Newsnight, BBC2, 11 February 2010

The no-PIN attack



result

5. Online transaction authorization (optional)

transaction;
cryptogram

1. Card details; digital signature

3. **Wrong PIN entered by crook;**
transaction description

4. **PIN OK (yes);**
authorization cryptogram

1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram

2. Wrong PIN entered by crook

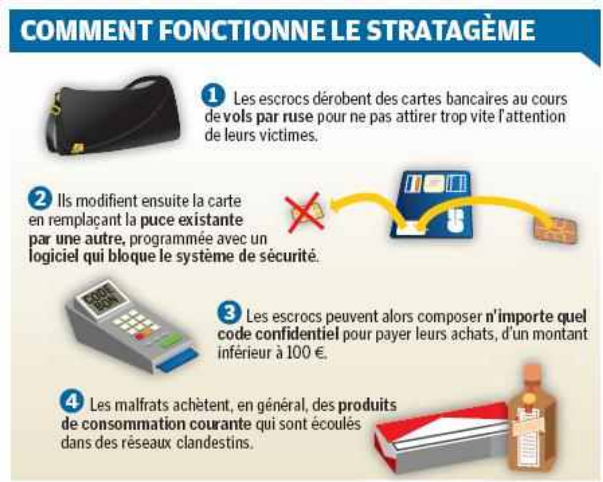
Why does this attack work?

- 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

Response from the banks

> *Scientific researchers from the University of Cambridge (UK), of which the most well known is Professor Ross Anderson, have announced that they have tested a scenario which attacks the EMV chip card. The attack scenario in question has already been analysed by several teams of independent specialists, as well as CBs own experts, with the conclusion that neither the chip in itself, nor the importance and the advantages of the chip in terms of security have been put into question. 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)*

Response from the criminals



COMMENT FONCTIONNE LE STRATAGÈME

1 Les escrocs dérobent des cartes bancaires au cours de **vols par ruse** pour ne pas attirer trop vite l'attention de leurs victimes.

2 Ils modifient ensuite la carte en remplaçant la **puce existante par une autre,** programmée avec un **logiciel qui bloque le système de sécurité.**

3 Les escrocs peuvent alors composer **n'importe quel code confidentiel** pour payer leurs achats, d'un montant inférieur à 100 €.

4 Les malfrats achètent, en général, des **produits de consommation courante** qui sont écoulés dans des réseaux clandestins.

— Le Parisien (January 2012)

Current and proposed defences

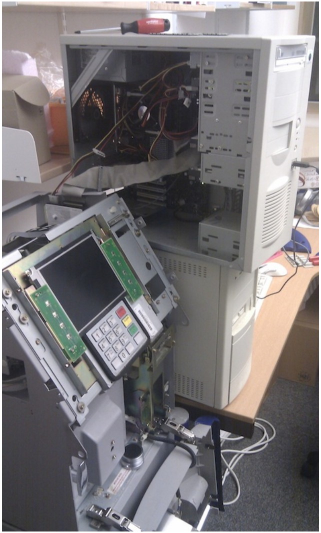
- Skimming
  - iCVV: Slightly modifying copy of magnetic strip stored on chip
  - Disabling fallback: Preventing magnetic strip cards from being used in EMV-enabled terminals
  - Better control of terminals: Prevent skimmers from being installed
- YES-card
  - Dynamic Data Authentication (DDA): Place a public/private keypair on every card
  - Online authorization: Require that all transactions occur online
- 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

Random numbers?

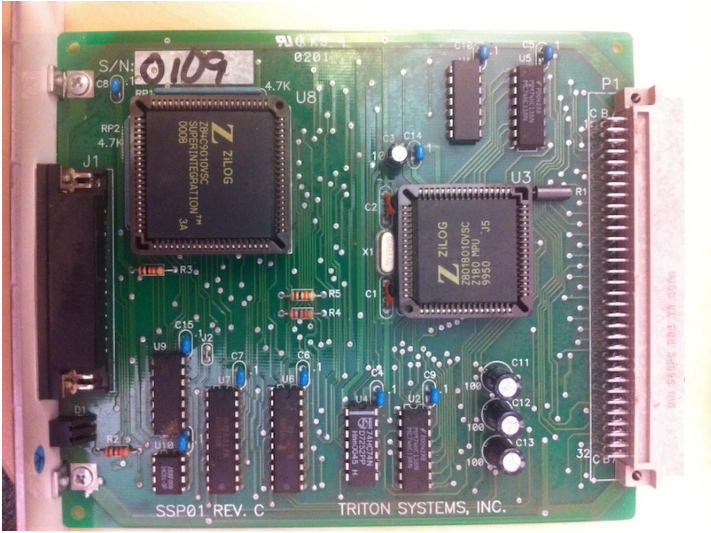
Date	Time	UN
2011-06-29	10:37:24	F1246E04
2011-06-29	10:37:59	F1241354
2011-06-29	10:38:34	F1244328
2011-06-29	10:39:08	F1247348

Reverse engineering

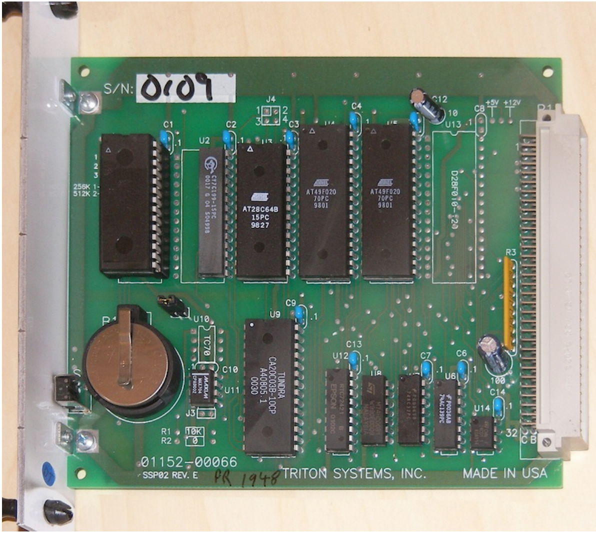
NCR ATM



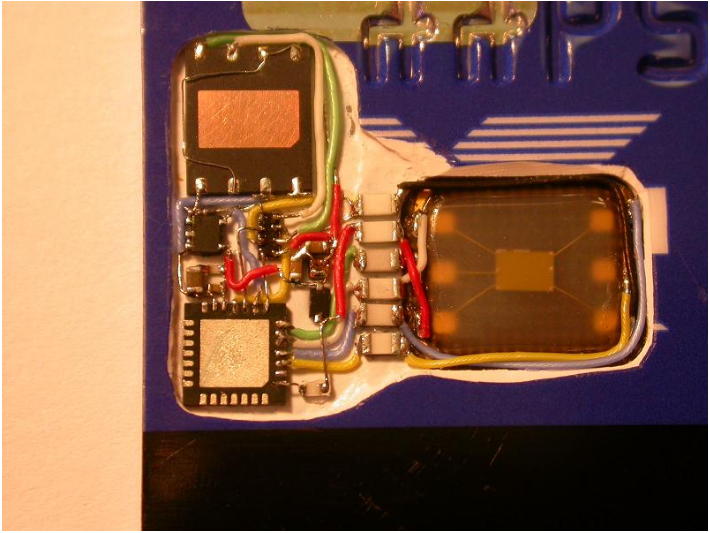
Triton ATM (CPU board)



Triton ATM (DES board)



Surveying the problem



Characteristic C

SRC2 EXP6		SRC2 EXP6B	
0	77028437	0	5D01BBCF
1	0D0AF8F9	1	760273FE
2	5C0E743C	2	730E5CE7
3	4500CE1A	3	380CA5E2
4	5F087130	4	580E9D1F
5	3E0CB21D	5	6805D0F5
6	6A05BAC3	6	530B6EF3
7	74057B71	7	4B0FE750
8	76031924	8	7B0F3323
9	390E8399	9	630166E1

Other ATMs

Counters		Weak RNGs	
ATM4	`eb661db4`	ATM1	`690d4df2`
ATM4	`2cb6339b`	ATM1	`69053549`
ATM4	`36a2963b`	ATM1	`660341c7`
ATM4	`3d19ca14`	ATM1	`5e0fc8f2`
ATM5	`F1246E04`	ATM2	`6f0c2d04`
ATM5	`F1241354`	ATM2	`580fc7d6`
ATM5	`F1244328`	ATM2	`4906e840`
ATM5	`F1247348`	ATM2	`46099187`
		ATM3	`650155D7`
		ATM3	`7C0AF071`
		ATM3	`7B021D0E`
		ATM3	`1107CF7D`

POS terminal

Stronger RNGs	
POS1	013A8CE2
POS1	01FB2C16
POS1	2A26982F
POS1	39EB1E19
POS1	293FBA89
POS1	49868033

Cashing out

- 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

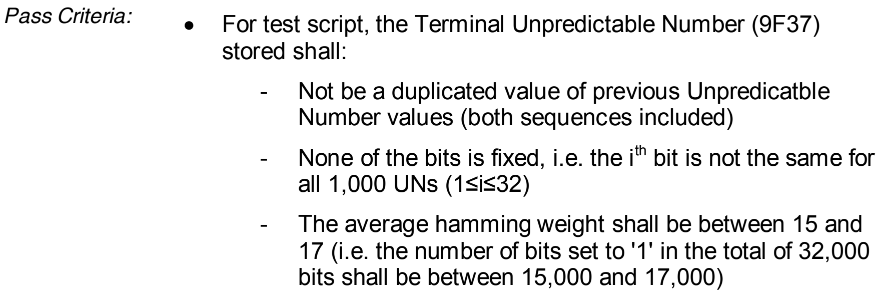
Mitigating the attack

- Detection:
  - Suspicious jumps in transaction counter
  - Lack of issuer authentication
- Prevention:
  - Relying party (issuer) generates the UN
  - Audit trail shows where UNs came from
- Industry response so far has been mixed
  - Details disclosed in early 2012
  - Some surprised by the problem
  - Others less so
  - Some knew of this problem but did not admit it

More information: “Chip and Skim: cloning EMV cards with the pre-play attack”, arXiv:1209.2531

Response from the banks

1,000 tests (was only 4) then:



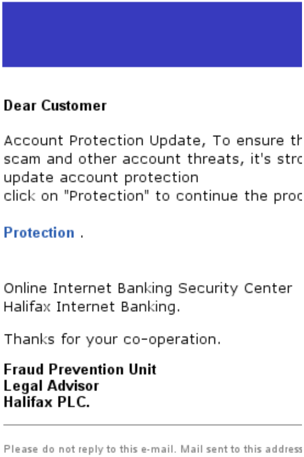
Pass Criteria:

- For test script, the Terminal Unpredictable Number (9F37) stored shall:
  - Not be a duplicated value of previous Unpredicatble Number values (both sequences included)
  - None of the bits is fixed, i.e. the ith bit is not the same for all 1,000 UNs (1≤i≤32)
  - The average hamming weight shall be between 15 and 17 (i.e. the number of bits set to '1' in the total of 32,000 bits shall be between 15,000 and 17,000)

Terminal Level 2 Test Cases: Unpredictable Number testing Update, EMVCo Terminal Approval Bulletin No. 127

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 stro
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.

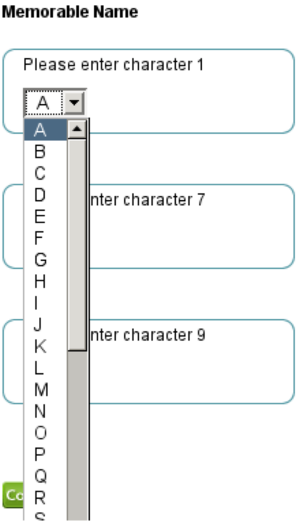
Please do not reply to this e-mail. Mail sent to this address

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

Please enter character 1

A

nter character 7

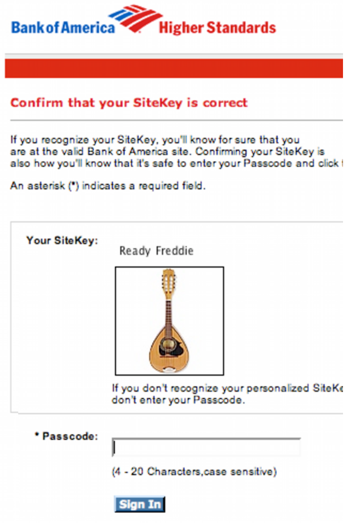
nter character 9

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



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 t

An asterisk (*) indicates a required field.

Your SiteKey: Ready Freddie

If you don't recognize your personalized SiteKe don't enter your Passcode.

* Passcode:

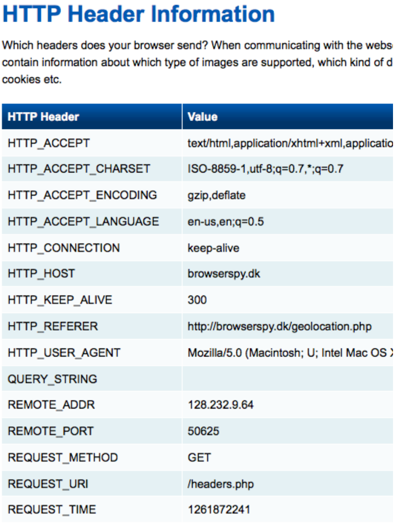
(4 - 20 Characters,case sensitive)

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 d
cookies etc.

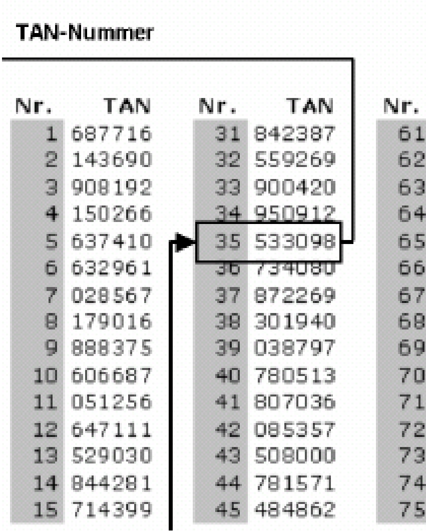
HTTP Header	Value
HTTP_ACCEPT	text/html,application/xhtml+xml,applicatio
HTTP_ACCEPT_CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING	gzip,deflate
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_CONNECTION	keep-alive
HTTP_HOST	browserspy.dk
HTTP_KEEP_ALIVE	300
HTTP_REFERER	http://browserspy.dk/geolocation.php
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; U; Intel Mac OS X
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

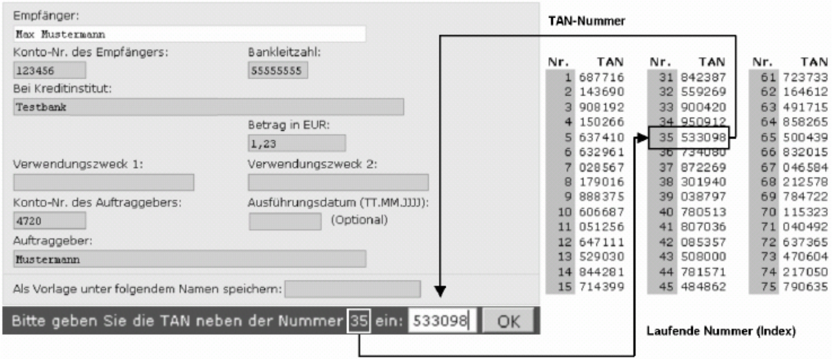


TAN-Nummer

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

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

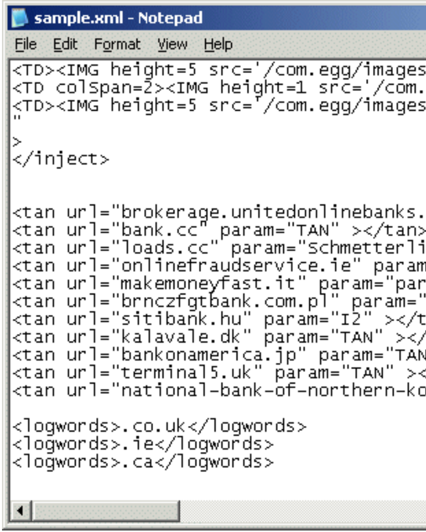
Customer must provide the requested one time password

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



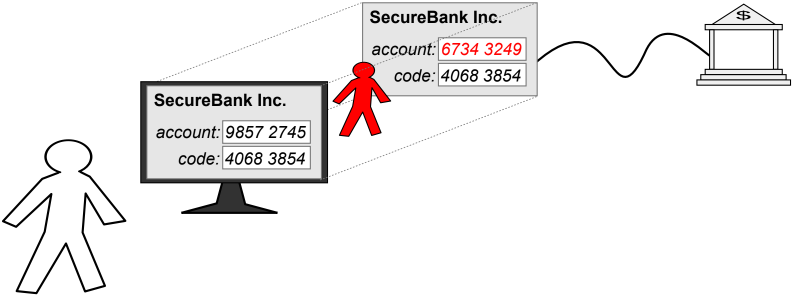
```
<TD><IMG height=5 src='/com.egg/images
<TD colSpan=2><IMG height=1 src='/com.
<TD><IMG height=5 src='/com.egg/images
"

>
</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

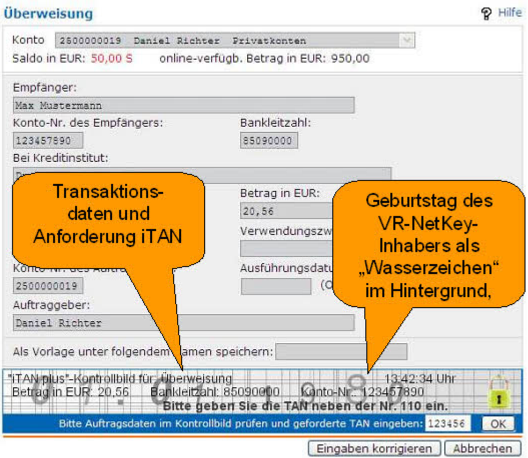
Patches up online statement so customer doesn't know

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

Konto 2600000019 Daniel Richter Privatkonten

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

Empfänger: Max Mustermann

Konto-Nr. des Empfängers: 123457890

Bankleitzahl: 85090000

Bei Kreditinstitut:

Betrag in EUR: 20,56

Verwendungszw

Konto-Nr. des Auftr 2500000019

Ausführungsdatu

Auftraggeber: Daniel Richter

Als Vorlage unter folgendem Namen speichern:

"iTAN 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.

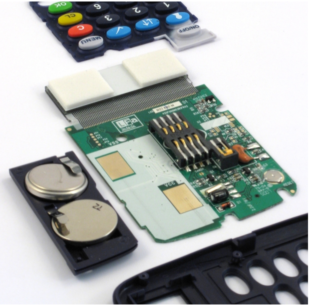
Bitte Auftragsdaten im Kontrollbild prüfen und geforderte TAN eingeben: 123456

Transaktionsdaten und Anforderung iTAN

Geburtstag des VR-NetKey-Inhabers als „Wasserzeichen“ im Hintergrund,

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

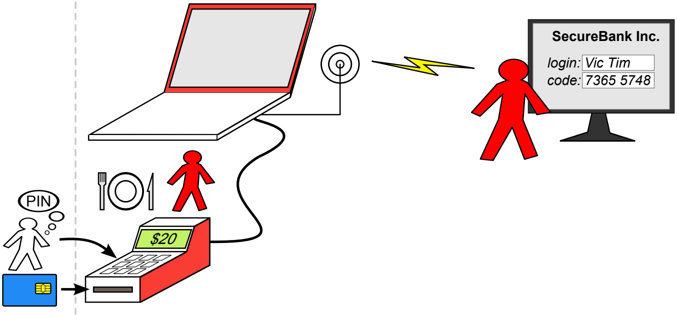
Identify	000000000000	00000000
Respond	000000000000	<challenge>
Sign	<amount>	<account number>

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)

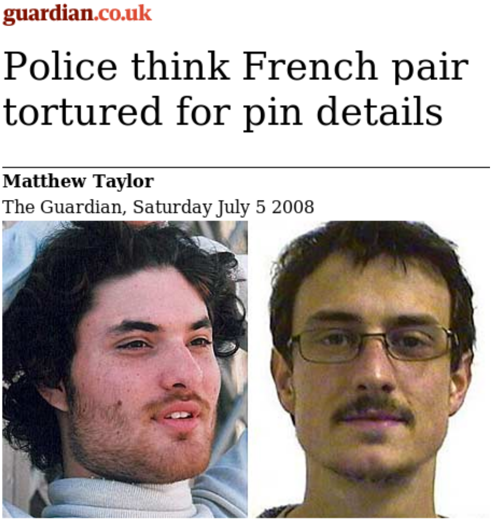
Fake point-of-sale terminal can get response in advance

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

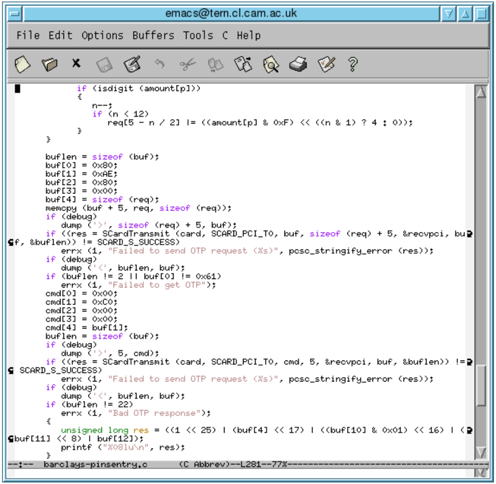
Software implementation of CAP is possible and desirable

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



```
                if (isdigit (amount[p]))
                {
                    n--;
                    if (n < 12)
                        req[5 - n / 2] |= ((amount[p] & 0xF) << ((n & 1) ? 4 : 0));
                }
        }

        buflen = sizeof (buf);
        buf[0] = 0x80;
        buf[1] = 0xAE;
        buf[2] = 0x80;
        buf[3] = 0x00;
        buf[4] = sizeof (req);
        memcpy (buf + 5, req, sizeof (req));
        if (debug)
            dump ('>', sizeof (req) + 5, buf);
        if ((res = SCardTransmit (card, SCARD_PCI_T0, buf, sizeof (req) + 5, &recvpci, bu
f, &buflen)) != SCARD_S_SUCCESS)
            errx (1, "Failed to send OTP request (%s)", pcsc_stringify_error (res));
        if (debug)
            dump ('<', buflen, buf);
        if (buflen != 2 || buf[0] != 0x61)
            errx (1, "Failed to get OTP");
        cmd[0] = 0x00;
        cmd[1] = 0xC0;
        cmd[2] = 0x00;
        cmd[3] = 0x00;
        cmd[4] = buf[1];
        buflen = sizeof (buf);
        if (debug)
            dump ('>', 5, cmd);
        if ((res = SCardTransmit (card, SCARD_PCI_T0, cmd, 5, &recvpci, buf, &buflen)) !=
 SCARD_S_SUCCESS)
            errx (1, "Failed to send OTP request (%s)", pcsc_stringify_error (res));
        if (debug)
            dump ('<', buflen, buf);
        if (buflen != 22)
            errx (1, "Bad OTP response");
        {
            unsigned long res = ((1 << 25) | (buf[4] << 17) | ((buf[10] & 0x01) << 16) | (
buf[11] << 8) | buf[12]);
            printf ("%08lu\n", res);
        }
--:--  barclays-pinsentry.c      (C Abbrev)--L281--77%------------------------------------
```

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

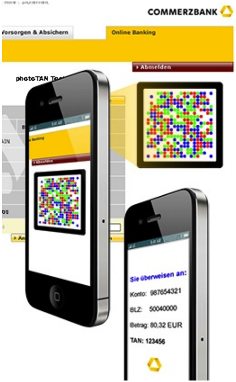
- Many more modes, selected by initial digits of challenge
- Mode number alters the meaningful prompts
- Up to 7 digit nonce for all modes
- Nonce, and mode number, are included in MAC
- PIN verification is optional

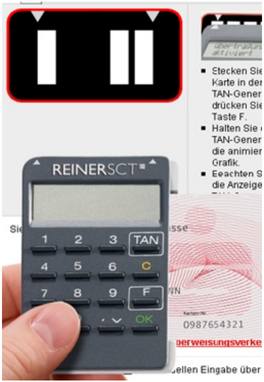
RSA SecurID and Racal Watchword do PIN verification on server, and permit a duress PIN

More improvements require higher unidirectional bandwidth

For usability, customer should not have to type in full challenge

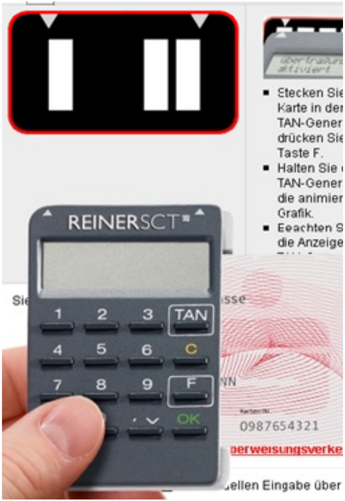
Allows versatility and better security





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

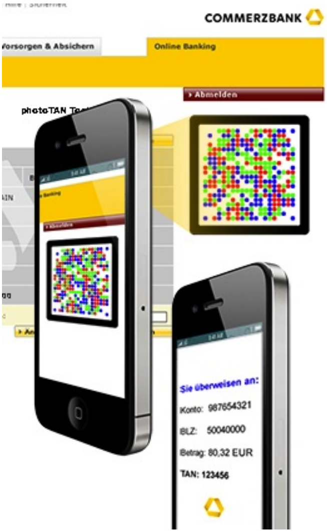


USB connected readers

- 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!



Sie überweisen an:

Konto: 987654321

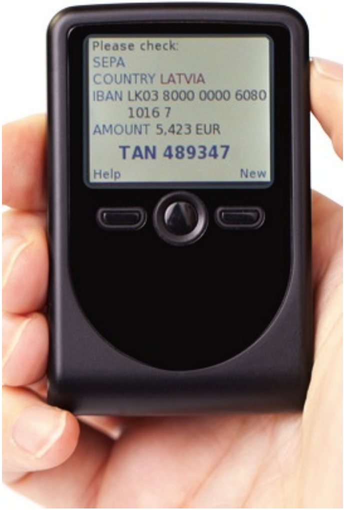
BLZ: 50040000

Betrag: 80,32 EUR

TAN: 123456

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!



Please check:
SEPA
COUNTRY LATVIA
IBAN LK03 8000 0000 6080
1016 7
AMOUNT 5,423 EUR
TAN 489347

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/`