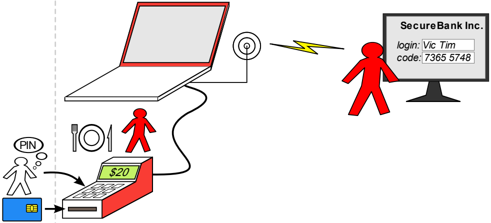
Optimised to Fail:
Card Readers for Online Banking



Saar Drimer   Steven J. Murdoch   Ross Anderson

www.cl.cam.ac.uk/users/{sd410,sjm217,rja14}

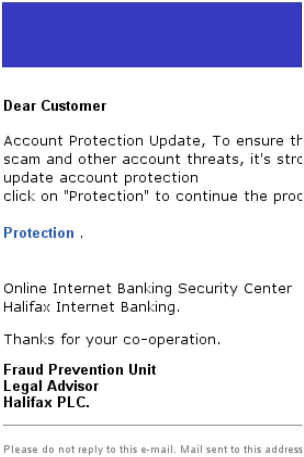
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

26C3, 29 December 2009, Berlin, Germany

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.

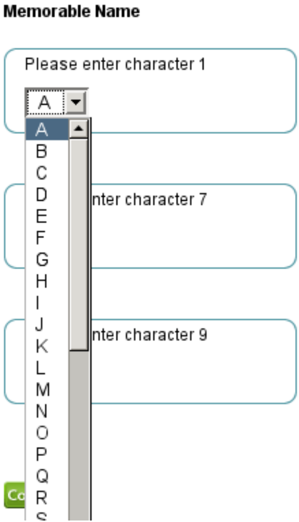
Please do not reply to this e-mail. Mail sent to this address

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

nter character 7

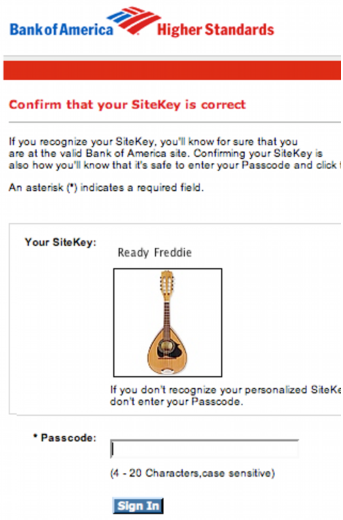
nter character 9

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



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 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:

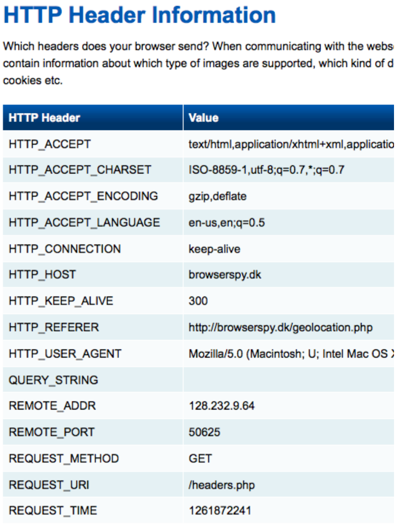
(4 - 20 Characters,case sensitive)

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.

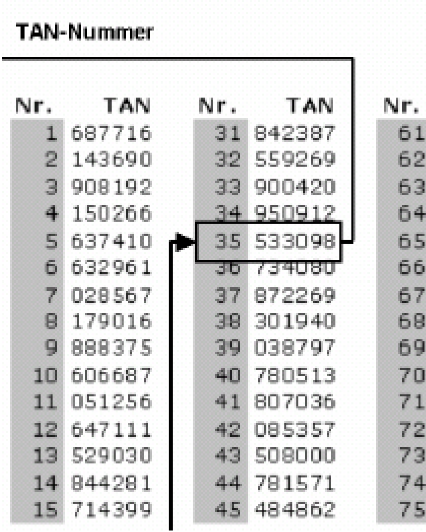
HTTP Header	Value
HTTP_ACCEPT	text/html,application/xhtml+xml,applicatio
HTTP_ACCEPT_CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING	gzip,deflate
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_CONNECTION	keep-alive
HTTP_HOST	browserspy.dk
HTTP_KEEP_ALIVE	300
HTTP_REFERER	http://browserspy.dk/geolocation.php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

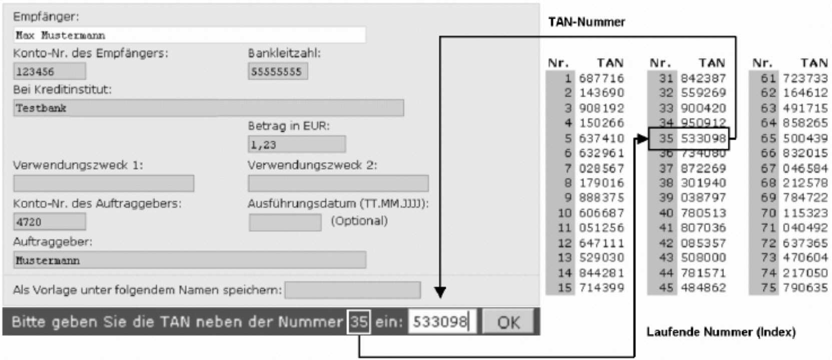


TAN-Nummer

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 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

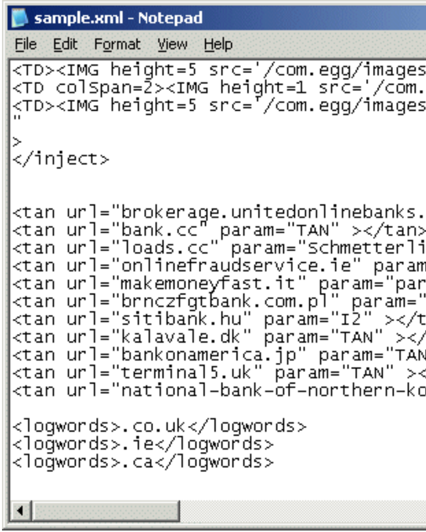
Customer must provide the requested one time password

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



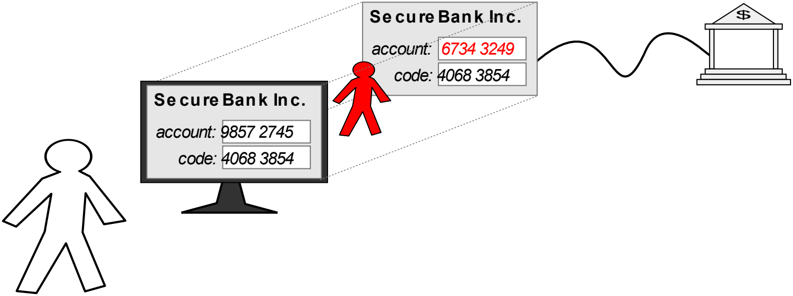
```
<TD><IMG height=5 src='/com.egg/images
<TD colSpan=2><IMG height=1 src='/com.
<TD><IMG height=5 src='/com.egg/images
"

>
</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

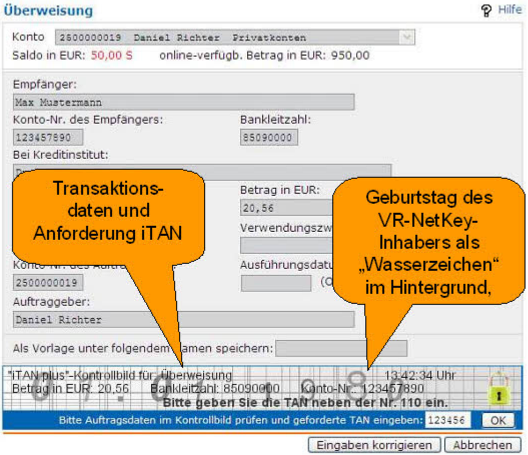
Patches up online statement so customer doesn’t know

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: 2500000019 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

Ausführungsdatu

2500000019

Auftraggeber: Daniel Richter

Als Vorlage unter folgendem amen 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.

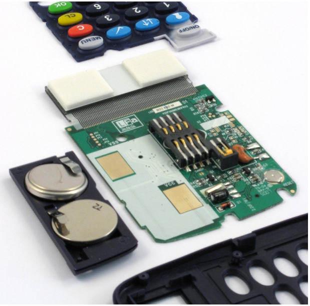
Bitte Auftragsdaten im Kontrollbild prüfen und geforderte TAN eingeben: 123456

Transaktions-daten 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

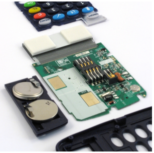


CAP (chip authentication programme) protocol specification secret, but based on EMV (Europay, Mastercard, Visa) open standard for credit/debit cards

Reader prompts for input and displays code generated by card

- Customer enters PIN
- Customer enters transaction details (varies between banks)
- Reader displays decimal authorization code
- Customer enters authorization code into web browser
- Bank verifies authorization code

Security protocol is secret: how does it actually work?



Step 1: Build a smart card snooper

The communications protocol used by smartcards is ISO 7816

- Half duplex (only one side talks at a time)
- Serial (only one communication line)
- Asynchronous (while there is a shared clock, this does not provide synchronization)
- Terminal driven (the terminal initiates all actions; the smartcard just responds to commands)

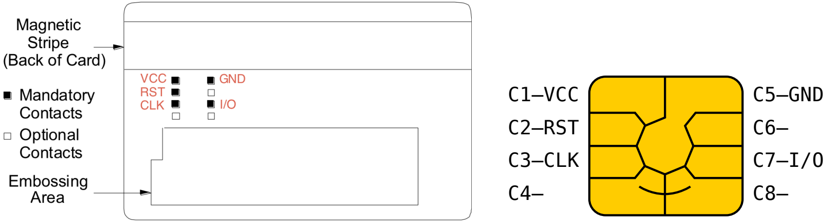


Figure: EMV specification v4.2, Book 1 / Wikipedia

Step 1: Build a smart card snooper

The communications protocol used by smartcards is ISO 7816

- Half duplex (only one side talks at a time)
- Serial (only one communication line)
- Asynchronous (while there is a shared clock, this does not provide synchronization)
- Terminal driven (the terminal initiates all actions; the smartcard just responds to commands)

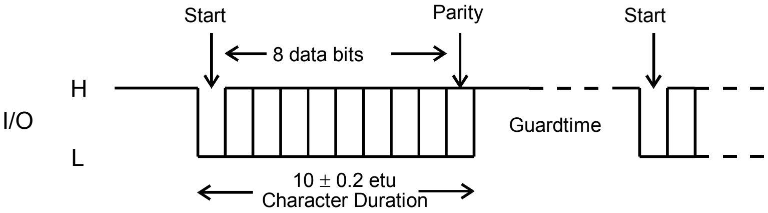
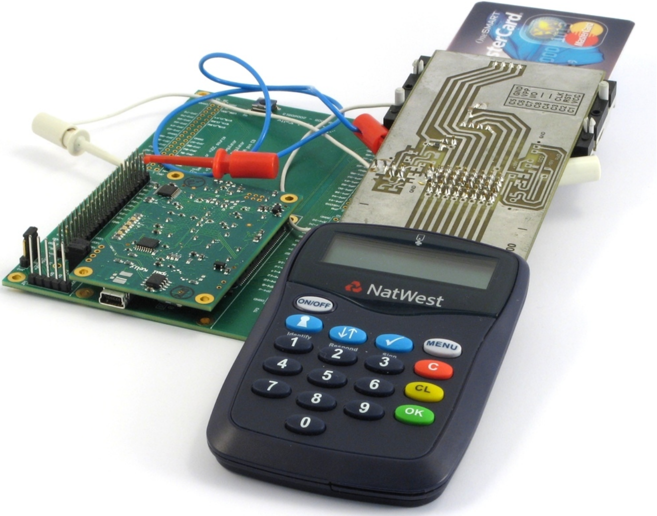


Figure: EMV specification v4.2, Book 1 / Wikipedia

Step 1: Build a smart card snooper

- Based on a Xilinx FPGA development board from Opal Kelly
- Reads I/O line at every etu/8
- Waits for the start bit, then records the 8 bits
- Sends data via USB



Step 1: Build a smart card snooper

What we discovered

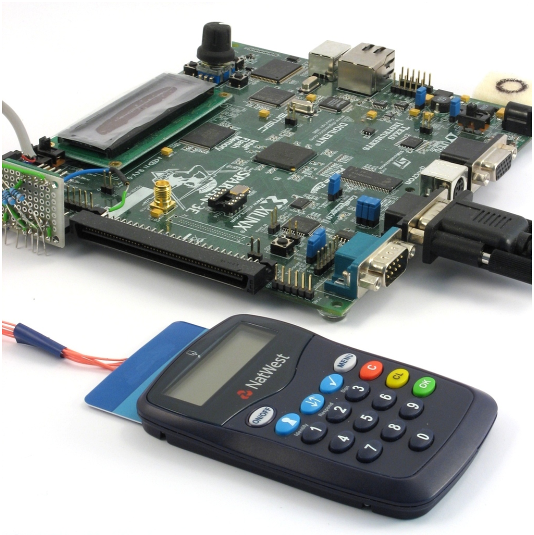
- Protocol **very** similar to EMV (the protocol used for smartcard payments across Europe)
- Looks like a transaction which is initiated, then cancelled at the final stage (as if terminal could not contact the bank)
- Card contains two data items which are not described by the EMV specification:

Tag	Length	Data
9f55	1	a0
9f56	12	00001f00000000000fffff0000000008000

- Likely done to save cost of designing a whole new protocol

Step 2: Start changing some data

- Use hardware developed for relay attack (see my 24C3 talk)
- Send most commands back and forth, unchanged
- Modify a few, and observe the result



Dummy smart card, connected to a PC via a FPGA for RS-232 ↔ ISO 7816 translation

Step 2: Start changing some data

- Use hardware developed for relay attack (see my 24C3 talk)
- Send most commands back and forth, unchanged
- Modify a few, and observe the result

Off-the-shelf smart card reader, connected to the PC over USB

Step 2: Start changing some data

What we discovered

- The authentication code comes from the cryptogram generated by the card at the end of the transaction
- The mysterious tag 9f56 was a ‘bit filter’ which selects which bits from the cryptogram are used for the response
- The filtered cryptogram is then converted to decimal

	CID	**ATC**	**AC**	**IAD**
Card output	80	A52D	AD452EF6BA769E4A	06770A03A48000
Bitmask	00	001F	0000000000FFFFF	00000000008000
Filter	..	..0D	...........69E4A	..........8...
Filter (bin)		01|101 0|1101|0011|1100|1001|010 1		
Filter (hex)			1AD3C95	
Response			28130453	

Step 3: Validate the results

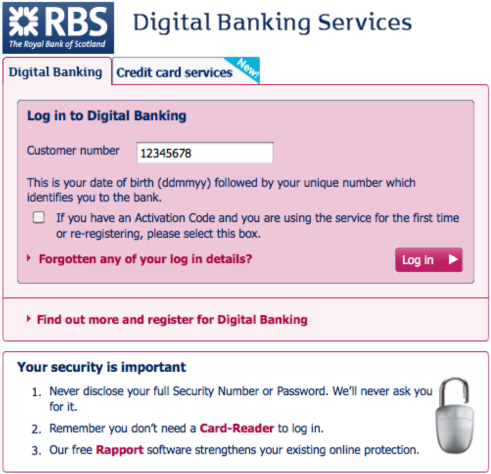
- We implemented the card-reader side in Python, using the PyCSC library
- Generates authentication codes which work with multiple banks' online banking
- Still needs the customer's real card and PIN

Off-the-shelf smart card reader, connected to the PC over USB

Step 3: Validate the results

- We implemented the card-reader side in Python, using the PyCSC library
- Generates authentication codes which work with multiple banks' online banking
- Still needs the customer's real card and PIN

Test with real online banking websites



RBS
The Royal Bank of Scotland

Digital Banking Services

Digital Banking
Credit card services
New!

Log in to Digital Banking

Customer number 12345678

This is your date of birth (ddmmyy) followed by your unique number which identifies you to the bank.

□ If you have an Activation Code and you are using the service for the first time or re-registering, please select this box.

Forgotten any of your log in details?
Log in
Find out more and register for Digital Banking

Your security is important

1. Never disclose your full Security Number or Password. We'll never ask you for it.
2. Remember you don't need a **Card-Reader** to log in.
3. Our free **Rapport** software strengthens your existing online protection.

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

Transaction mode not included in MAC

Input to MAC does not include the selected operation mode

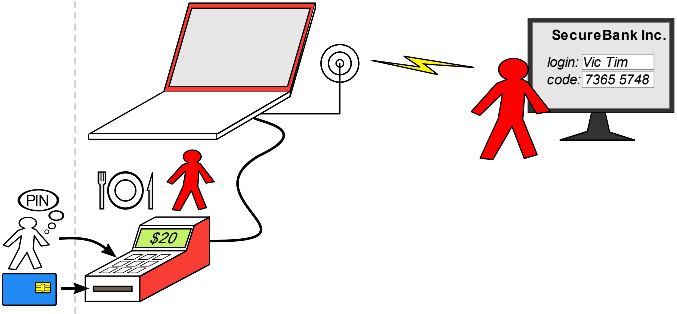
Identify	000000000000	00000000
Respond	000000000000	<challenge>
Sign	<amount>	<account number>

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)

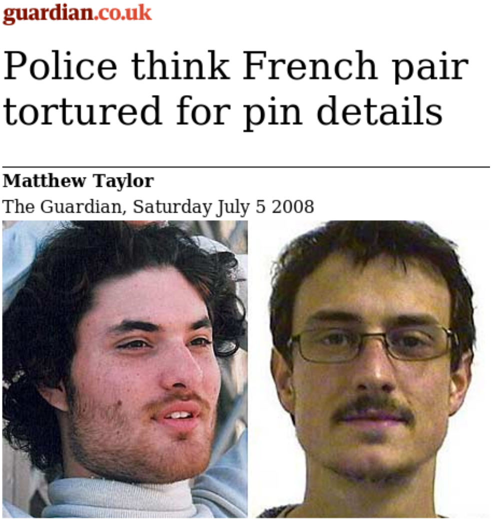
Fake point-of-sale terminal can get response in advance

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

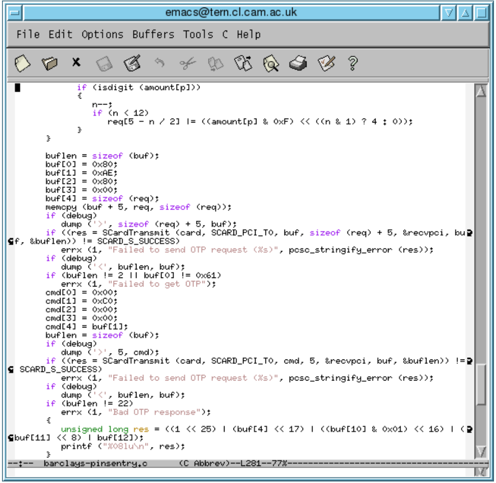
Software implementation of CAP is possible and desirable

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

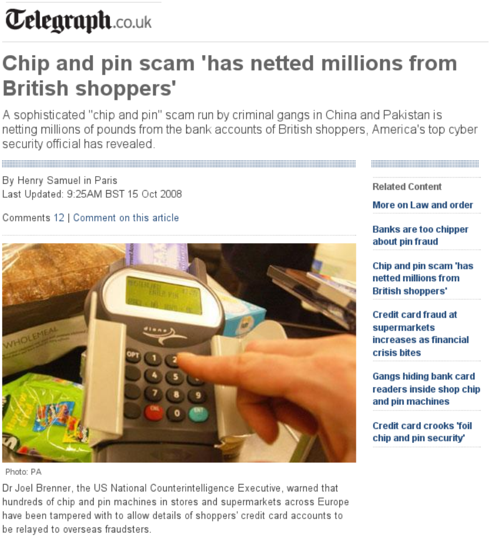
If this software becomes popular, malware will attack it



```
        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%------------------------------
```

Supply chains can be infiltrated



Telegraph.co.uk

Chip and pin scam 'has netted millions from British shoppers'

A sophisticated "chip and pin" scam run by criminal gangs in China and Pakistan is netting millions of pounds from the bank accounts of British shoppers, America's top cyber security official has revealed.

By Henry Samuel in Paris
Last Updated: 9:25AM BST 15 Oct 2008

Comments 12 | Comment on this article

Photo: PA

Dr Joel Brenner, the US National Counterintelligence Executive, warned that hundreds of chip and pin machines in stores and supermarkets across Europe have been tampered with to allow details of shoppers' credit card accounts to be relayed to overseas fraudsters.

Related Content

- More on Law and order
- Banks are too chipper about pin fraud
- Chip and pin scam 'has netted millions from British shoppers'
- Credit card fraud at supermarkets increases as financial crisis bites
- Gangs hiding bank card readers inside shop chip and pin machines
- Credit card crooks 'foil chip and pin security'

Chip & PIN terminals have been found with tapping devices inserted at manufacturer, which send captured details by mobile phone

There is even less control over the supply chain for CAP readers

Criminals could send or sell trojaned readers

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)

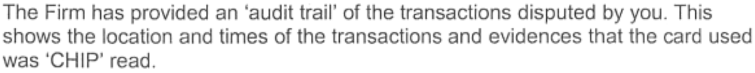
Is this better for customers? Maybe no (at least in the UK)

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)?

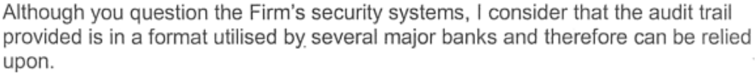
CAP further increases the customer's liability for online fraud



The Firm has provided an 'audit trail' of the transactions disputed by you. This shows the location and times of the transactions and evidences that the card used was 'CHIP' read.

Financial
Ombudsman
Service

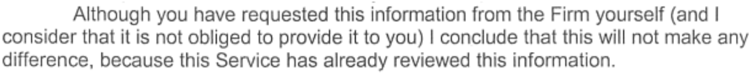
CAP further increases the customer's liability for online fraud



Although you question the Firm's security systems, I consider that the audit trail provided is in a format utilised by several major banks and therefore can be relied upon.

Financial
Ombudsman
Service

CAP further increases the customer's liability for online fraud

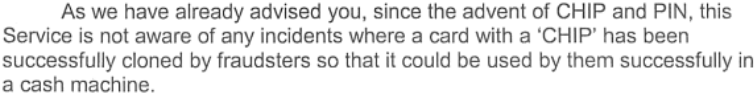


Although you have requested this information from the Firm yourself (and I consider that it is not obliged to provide it to you) I conclude that this will not make any difference, because this Service has already reviewed this information.

Financial
Ombudsman
Service

CAP further increases the customer's liability for online fraud

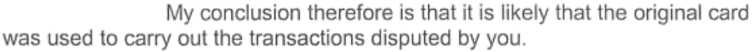
“



As we have already advised you, since the advent of CHIP and PIN, this Service is not aware of any incidents where a card with a ‘CHIP’ has been successfully cloned by fraudsters so that it could be used by them successfully in a cash machine.

Financial
Ombudsman
Service

CAP further increases the customer's liability for online fraud



My conclusion therefore is that it is likely that the original card was used to carry out the transactions disputed by you.

Financial
Ombudsman
Service

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

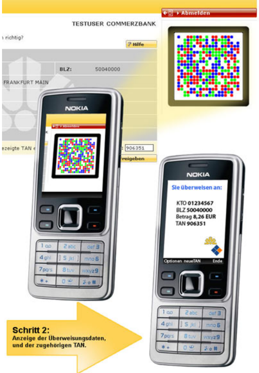
- Many more modes, selected by initial digits of challenge
- Mode number alters the meaningful prompts
- Up to 7 digit nonce for all modes
- Nonce, and mode number, are included in MAC
- PIN verification is optional

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

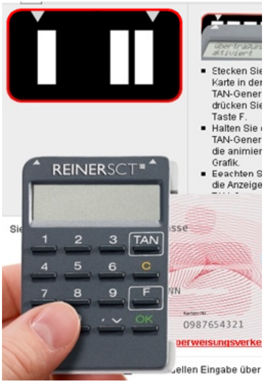
Allows versatility and better security



Sie überweisen an:

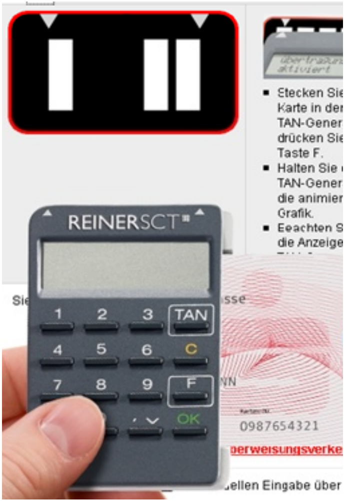
KTO 01234567
BLZ 50040000
Betrag 8,26 EUR
TAN 906351

Schritt 2:
Anzeige der Überweisungsdaten, und der zugehörigen TAN.



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

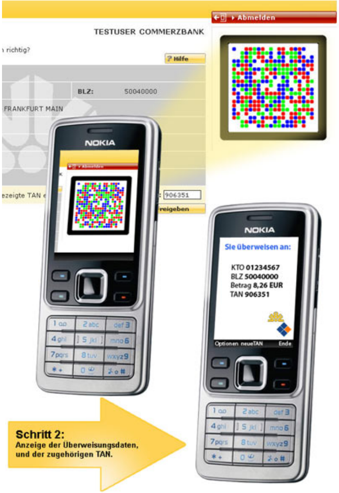


USB connected readers

- 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!



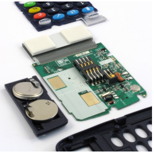
Sie überweisen an:

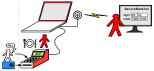
KTO 01234567
BLZ 50040000
Betrag 8,26 EUR
TAN 906351

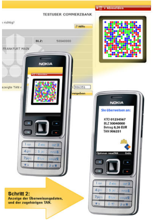
Schritt 2:
Anzeige der Überweisungsdaten,
und der zugehörigen TAN.

Conclusions

- Transaction authentication is necessary to protect against today's fraudsters
- We reverse-engineered the CAP protocol and found that it optimised transaction authentication too far
- CAP suffers from usability and protocol flaws
- Combining point-of-sale and online authentication increases the attack surface
- Usability testing and better security design would have identified these issues
- More bandwidth significantly improves usability and security







Sie überweisen an:
KTO 01234567
BLZ 50040000
Betrag 8,26 EUR
TAN 906351

Schritt 2:
Anzeige der Überweisungsdaten, und der zugehörigen TAN.