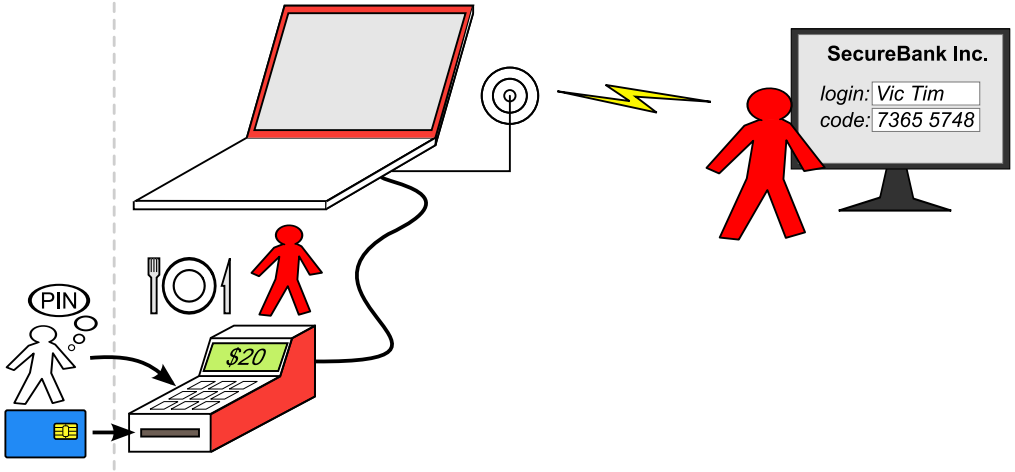
Optimised to Fail: Card Readers for Online Banking



Saar Drimer Steven J. Murdoch Ross Anderson

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

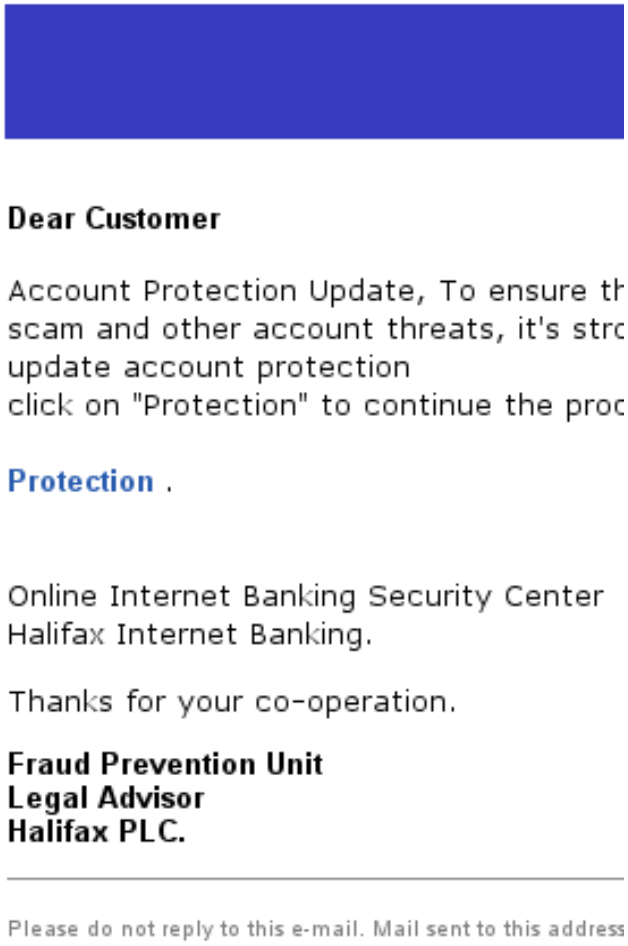
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

Financial Cryptography and Data Security, 23–26 February, Barbados

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.

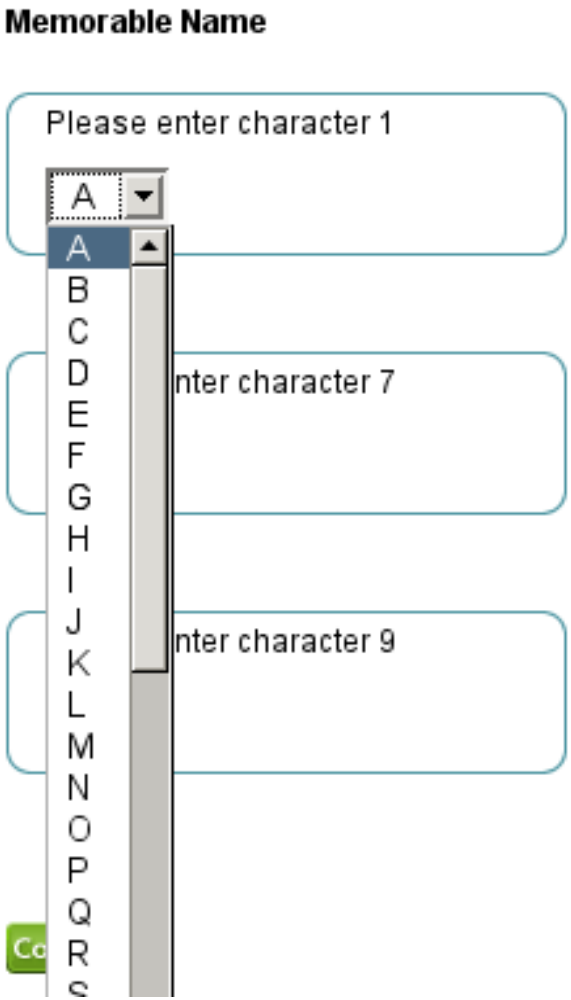
Please do not reply to this e-mail. Mail sent to this address

A variety of solutions have been proposed to resist phishing

- On-screen keyboards
- Picture passwords
- One-time-passwords/iTAN
- Device fingerprinting

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser



A variety of solutions have been proposed to resist phishing

iTAN

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

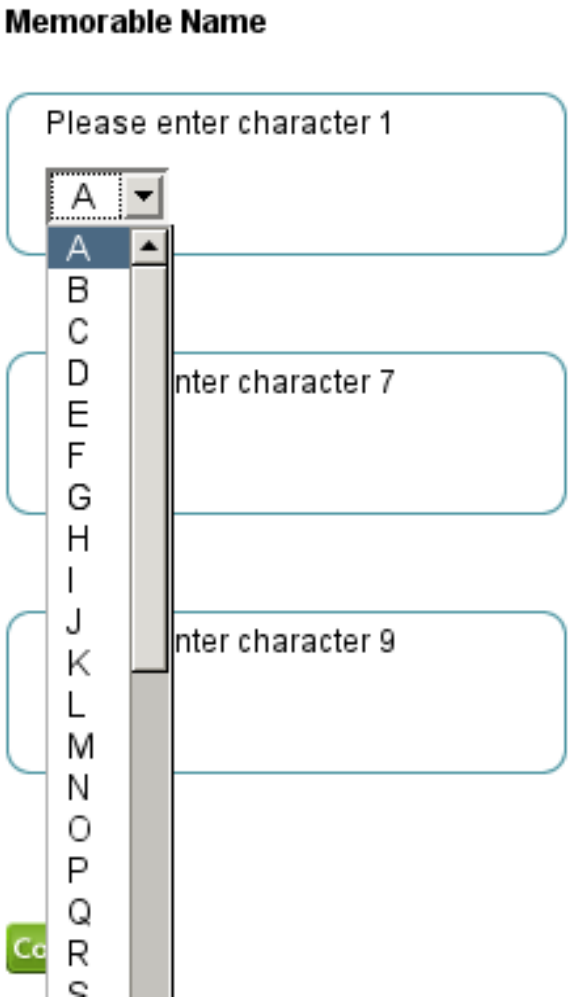
Customer must provide the requested one time password

A variety of solutions have been proposed to resist phishing

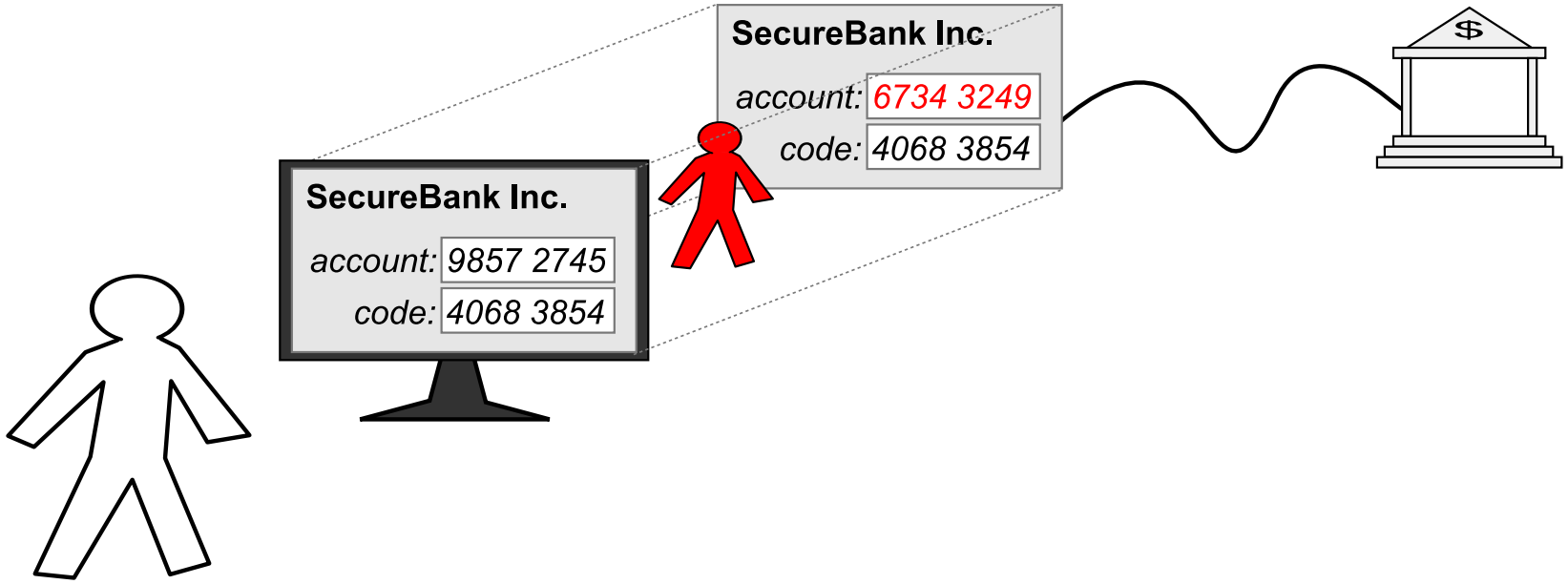
- On-screen keyboards
- Picture passwords
- One-time-passwords/iTAN
- Device fingerprinting

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser



Man in the browser



Malware embeds itself into the browser

Changes destination/amount of transaction in real-time

Any one-time password is valid, and mutual authentication succeeds

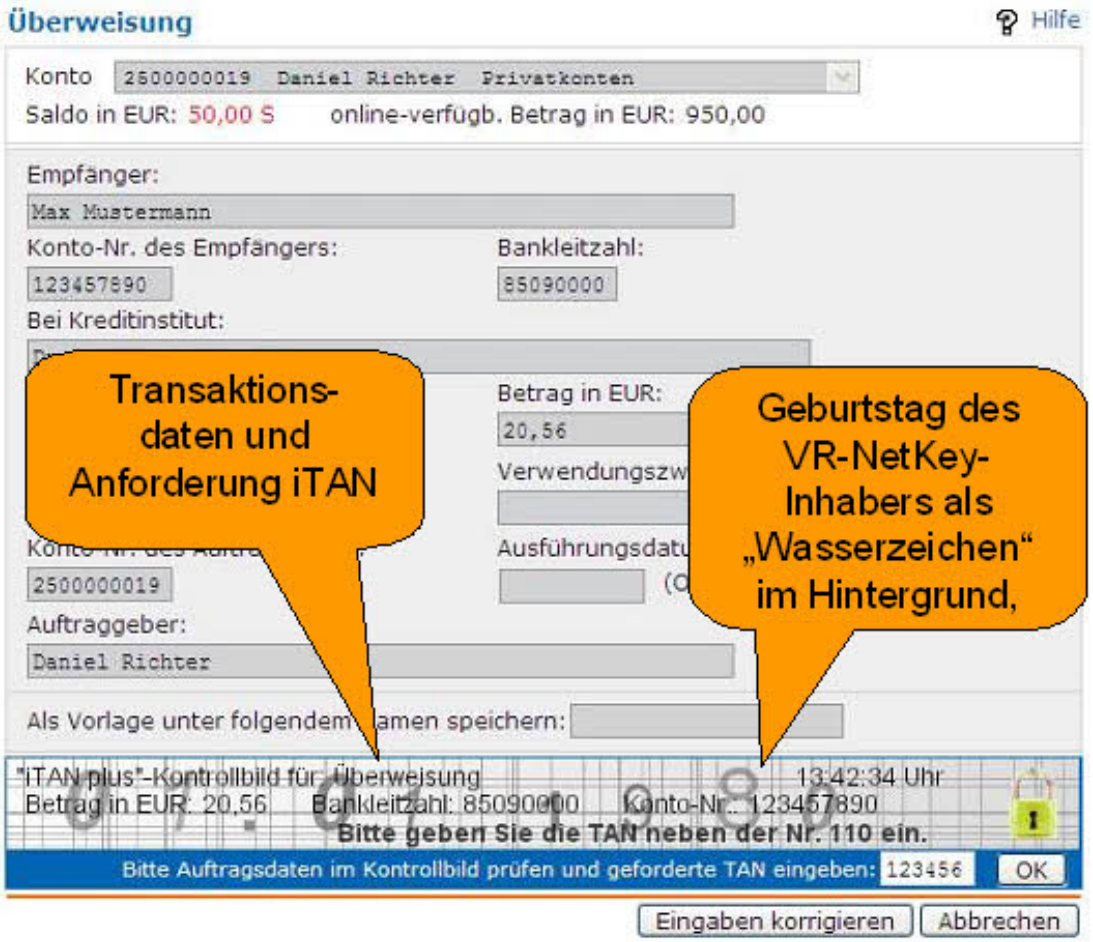
Patches up online statement so customer doesn't know

Somehow the response must be bound to the transaction to be authorised

Embed challenge in a CAPTCHA style image, along with transaction

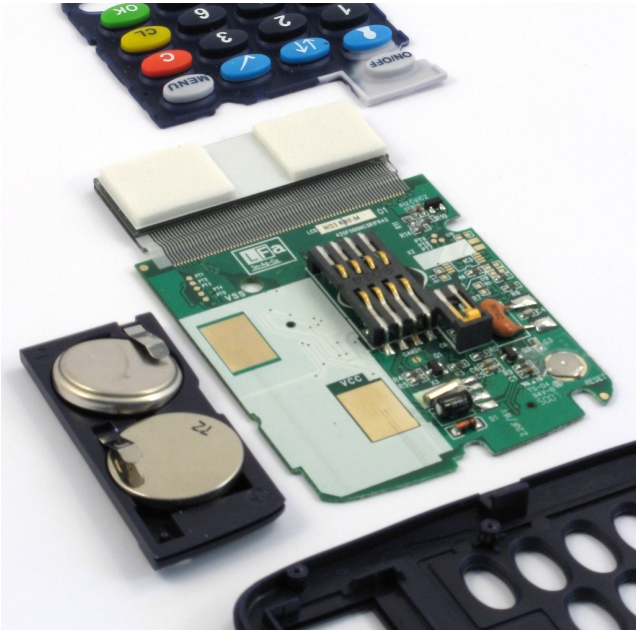
Involving a human can defeat this

May move the fraud to easier banks



Picture: Volksbank Dill eG

Some UK banks have rolled out disconnected smart card readers



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

Reader prompts for input and displays MAC generated by card

- Customer enters PIN
- Card verifies PIN
- Customer enters transaction details (varies between banks)
- Card calculates MAC over:
  - Counter on card
  - Information entered by customer
  - Result of PIN entry
- Reader displays decimal value from:
  - Some bits from the counter
  - Some bits from the MAC

Full details are in the paper

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

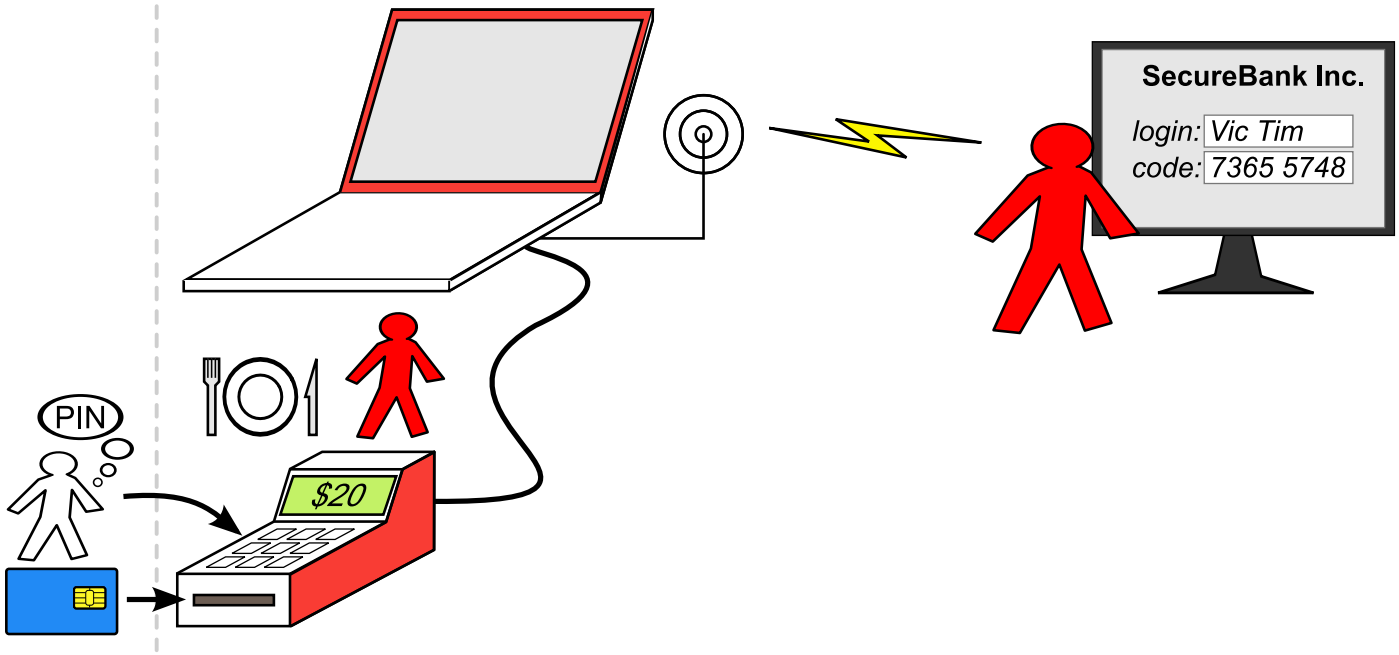
Identify	0000000000000	00000000
Respond	0000000000000	<challenge>
Sign	<amount>	<account number>

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

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

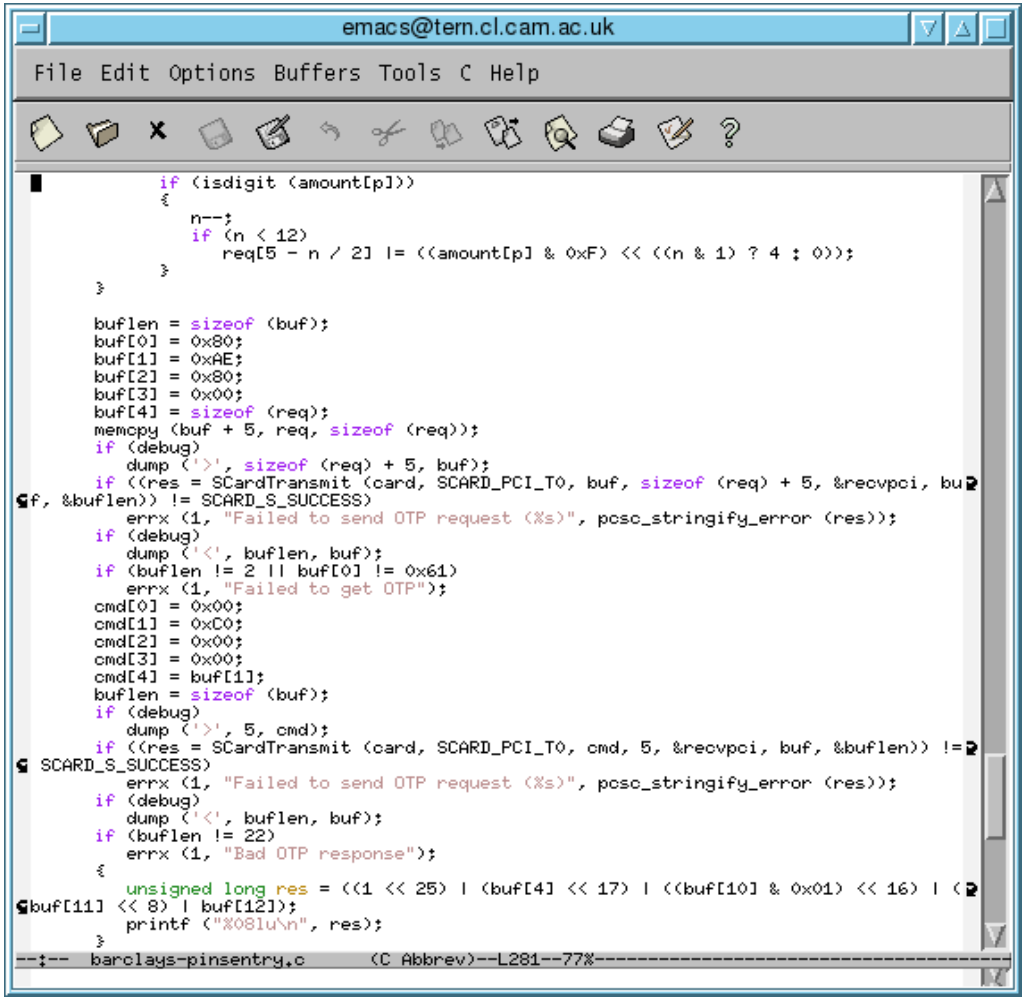
Software implementation of CAP is possible and desirable

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);
      }
```

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

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.

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.

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.

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.

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

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