Bringing the Customer into Audit

Steven Murdoch
University of Cambridge

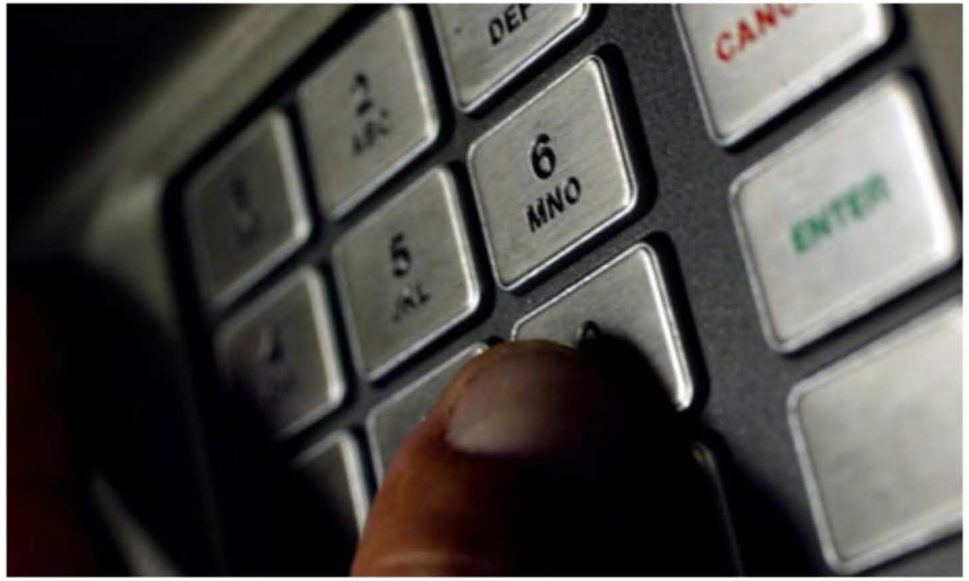
Schloss Dagstuhl seminar 10341, 22—26 August 2010:
Insider Threats: Strategies for Prevention, Mitigation, and Response
http://www.dagstuhl.de/10341

guardian.co.uk

Has chip-and-pin failed to foil fraudsters?

It was supposed to bring an end to unauthorised card transactions, but two years on is chip-and-pin just as fallible as its predecessor?

Danny Bradbury
The Guardian, Thursday 3 January 2008



This is a big week for Alain Job. The 40-year-old football coach is bringing his case against the Halifax bank to court. He says that fraudsters withdrew £2,100 from his account at ATMs, even though he was in possession of his card, and he doesn't want to pay.

Chip-and-pin was supposed to stop disputes like this. First introduced to the UK in 2004, it replaced signatures with chips embedded in bank cards that verify a customer's four-digit pin. Cards also contain a secret key used to validate the card with the bank.

Disputed ATM withdrawal

Card destroyed by bank

Job case

Audit logs destroyed by bank

guardian.co.uk

Has chip-and-pin failed to foil fraudsters?

It was supposed to bring an end to unauthorised card transactions, but two years on is chip-and-pin just as fallible as its predecessor?

Denny Bradbury
The Guardian, Thursday 3 January 2008

A [illegible]

This is a big week for Alain Job. The 40-year-old football coach is bringing his case against the Halifax bank to court. He says that fraudsters withdrew £2,100 from his account at ATMs, even though he was in possession of his card, and he doesn't want to pay.

Chip-and-pin was supposed to stop disputes like this. First introduced to the UK in 2004, it replaced signatures with chips embedded in bank cards that verify a customer's four-digit pin. Cards also contain a secret key used to validate the card with the bank.

We also requested at the time of this claim, supporting documents from [redacted] and were provided a copy of the till receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [redacted] at the time.

Timings and location of these charges are as follows.....

£3000.00 - 20/05/08 - 12.27pm
£4000.00 - 20/05/08 - 12.28pm
£2500.00 - 20/05/08 - 12.30pm

All made at [redacted]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.

Bring

Disputed PoS transactions

Card destroyed by customer

AmEx case

No refund despite known vulnerability

2

We also requested at the time of this claim, supporting documents from [redacted] and were provided a copy of the 10 receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [redacted] at the time.

Timings and location of these charges are as follows....

£3000.00 - 20/05/08 - 12.27pm
£4000.00 - 20/05/08 - 12.28pm
£2500.00 - 20/05/08 - 12.30pm

All made at [redacted]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.

THE TIMES
THE SUNDAY TIMES

From The Times

May 22, 2010

Bank ‘accused me of stealing £10,000 from my fiancée’s account’

Lauren Thompson

A change in the way that banks deal with victims of fraud is being demanded after Santander suggested that a customer was stealing from his fiancée so that it did not have to refund £10,000 in disputed transactions.

The man won his year-long battle to clear his name only after a bank worker was arrested for fraud. Santander then refunded the £10,000, but not before requiring her to sign a confidentiality agreement binding her to secrecy.

The case raises concern that Santander is routinely suggesting that customers are criminals to deny them refunds.

Peter Vicary-Smith, the chief executive of *Which?*, said: “Santander’s behaviour in this case was absolutely shocking. The last thing you need when you discover someone has cleared out your account is for your bank to say it was your fault.

“To claim that chip-and-PIN is infallible is simply not a strong enough argument for accusing a customer of negligence or fraud.

Bring

Disputed ATM withdrawal

Card destroyed by customer

Woolf case

Refund after arrest for fraud

THE TIMES
THE SUNDAY TIMES

Archive Article Please enjoy this article from The Times & The Sunday Times archives. For

From The Times

May 20, 2012

Bank 'accused me of stealing £10,000 from my fiancée's account'

Laurie Thomson

A change in the way that banks deal with victims of fraud is being demanded after Santander suggested that a customer was stealing from his fiancée so that it did not have to refund £10,000 in disputed transactions.

The man won his yearslong battle to clear his name only after a bank worker was arrested for fraud. Santander then refunded the £10,000, but not before requiring her to sign a confidentiality agreement binding her to secrecy.

The case raises concern that Santander is routinely suggesting that customers are criminals to deny them refunds.

Peter Vicary-Smith, the chief executive of Which?, said: "Santander's behaviour in this case was absolutely shocking. The last thing you need when you discover someone has cleared out your account is for your bank to say it was your fault.

"To claim that chip-and-PIN is infallible is simply not a strong enough argument for accusing a customer of negligence or fraud.

Incentives

Poor procedures

Buggy software

Regulatory capture

Internal audit is not working

Poor interpretation

Insufficient auditing

Lack of communication

Bank records:

Below is a list of the dates and times of all transactions performed in [redacted] from 23rd July 2009 onwards. I have also included further computerised records for your information:

Date	Amount	Retailer/ATM	Successful/Unsuccessful
24/07	211.66	[redacted]	Unsuccessful
24/07	3994.56		Successful
24/07	3994.56		Successful
24/07	3187.54		Unsuccessful
24/07	85.56		Unsuccessful

According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

Merchant record:

[redacted]

24/07/1980 11:38

KART NO S.K.T.: 12/10

[redacted]

[redacted]

[redacted]

EMV : A0000000031010/00A0080000/F800

APP LABEL : VISA DEBIT

0x08 = PIN entry required, PIN pad present, but PIN not entered

ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

TESEKKURLER

FORTIS

0x08 = PIN entry required, PIN pad present, but PIN not entered

Disputed ATM withdrawal

Card destroyed by bank

Job case

Audit logs destroyed by bank

Disputed PoS transactions

Card destroyed by customer

AmEx case

No refund despite known vulnerability

Disputed ATM withdrawal

Card destroyed by customer

Woolf case

Refund after arrest for fraud

Help the customer help you!

Incentives

Buggy software

Internal au not worki

Insufficient auditing

Lack of

Help the customer help you!

Do not destroy the card

- Card maintains a transaction counter (ATC)
- Card (optionally) maintains a transaction log

Use these to catch fraud

Cryptographically protect logs

- Maintain hash chain over customer account events
- Print on statement
- Publish top-level of hash tree somewhere else

Prevent log tampering

Make receipts useful for audit

- Have input to cryptographic MAC on receipt
- Force bank to give enough verification data

Verify security properties

Questions?

Internal audit is not working

- Incentives
- Poor procedures
- Buggy software
- Regulatory capture
- Insufficient auditing
- Poor interpretation
- Lack of communication

Bank records:

Below is a list of the dates and times of all transactions performed in [redacted] from 23rd July 2009 onwards. I have also included further computerised records for your information:

Date	Amount	Retailer/ATM	Successful/Unsuccessful
24/07	211.66	[redacted]	Unsuccessful
24/07	3994.56		Successful
24/07	3994.56		Successful
24/07	3187.54		Unsuccessful
24/07	85.56		Unsuccessful

According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

Merchant record:


[redacted]
24/07/1980 11:30
KART NO S.K.T.: 12/10
[redacted]
EMV : A0000000031010/00A0000000/F800
APP LABEL : VISA DEBIT

ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

TESEKKURLER

FORTIS

Do not destroy the card

- Card maintains a transaction counter (ATC)
- Card (optionally) maintains a transaction log

Use these to catch fraud

Cryptographically protect logs

- Maintain hash chain over customer account events
- Print on statement
- Publish top-level of hash tree somewhere else

Prevent log tampering

Make receipts useful for audit

- Have input to cryptographic MAC on receipt
- Force bank to give enough verification data

Verify security properties