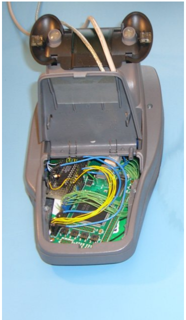
# Chip and Spin



Steven J. Murdoch

www.cl.cam.ac.uk/users/sjm217

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

OpenNet Initiative

www.opennet.net

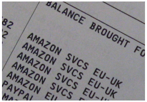
# This talk describes the major methods of card fraud in the UK

Card skimming and fallback: the current problem

Possible future developments in card fraud

The Firm has provide
shows the location a
was 'CHIP' read.
The Firm says that n
yo
'CHIP' read.
Although you questic
provided is in a form
upon. As we have al
Service is not aware

Risks to victims of fraud



BALANCE BROUGHT FO
82
2
AMAZON SVCS EU-UK
AMAZON SVCS EU-UK
AMAZON SVCS EU-UK
AMAZON SVCS EU-U
PAYPAL EU

What can be done to help

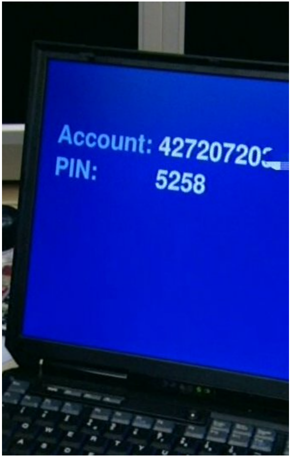
# The easiest way to get card details is to read them from the magnetic stripe

- Your name, account number and all information needed to make a fake card are stored on the card's magnetic stripe
- This includes the "CVV", which banks use to confirm that the card is legitimate (not to be confused with the CVV2 printed on the back)
- A fraudster can use a magnetic stripe reader to perform a "double-swipe"
- The fraudster can watch/film the customer entering their PIN

Tonight (ITV, 2007-05-04)

# Alternatively, the card details and PIN can be intercepted “on the wire”

- In some cases, the magnetic stripe details are also sent along wires and can be intercepted there
- Another place to intercept communications is between the chip and the terminal
- The account number is sent from the chip to the terminal
- The PIN entered is sent from the terminal to the chip for verification
- So all the information needed by fraudsters can be collected from a single point



Account: 427207203
PIN: 5258

Plusminus (ARD, 2006-03-07)

# Once the details have been collected, a fake card can be created

- Even though UK cards have chips, ATMs will accept clones which appear to have a broken chip
- Alternatively, fraudsters can use the card abroad where ATMs do not have chip readers
- There, the cloned cards can be sold, protecting the people who collected the details originally
- Any magnetic stripe card will suffice, even a mobile phone top-up card

ITV News (2006-06-12)

# New security measures will (eventually) make these attacks more difficult

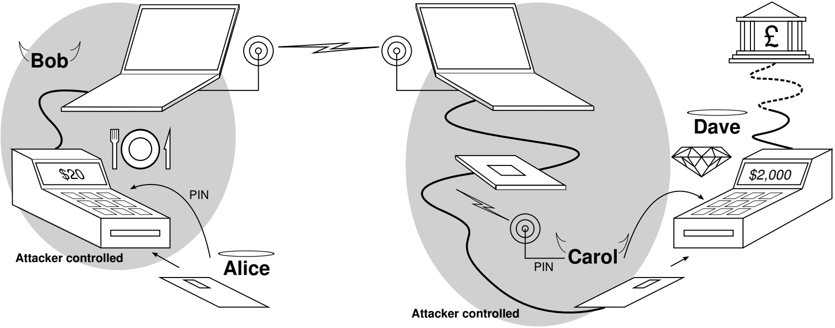
- Slowly, ATMs are being upgraded to refuse cards without a chip
- UK customers might be issued with separate magnetic stripe cards for use abroad
- Chips in UK cards can be cloned, but the clone will be detected if the terminal connects to the bank
- More secure chip cards, as used in other European countries, make cloning much more difficult

# Even then, customers cannot tell whether a terminal has been tampered

- The security of Chip & PIN still depends on the terminal acting in the customer’s best interest
- But customers cannot tell if the terminal is fake, or has been tampered with
- Saar Drimer and I opened up a terminal and replaced the electronics inside
- To a customer it still works as normal, but we have complete control over what it does

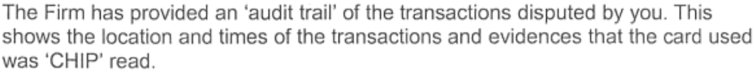
# Relay attacks can defeat even the latest generation of chip cards

Alice thinks she is paying for a meal. Actually, the fraudster Carol is buying diamonds on her card. Information from Alice's card is sent wirelessly to Carol's counterfeit



# If the bank doesn’t believe you, it can be very difficult to get your money back

“

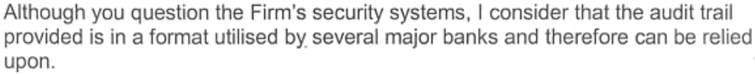


The Firm has provided an ‘audit trail’ of the transactions disputed by you. This shows the location and times of the transactions and evidences that the card used was ‘CHIP’ read.

”

Financial
Ombudsman
Service

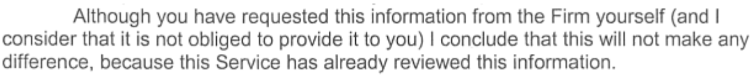
# If the bank doesn't believe you, it can be very difficult to get your money back



“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

# If the bank doesn't believe you, it can be very difficult to get your money back

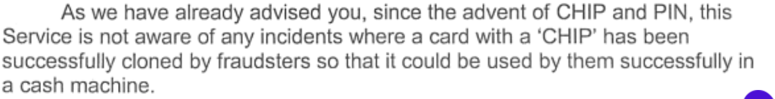


Although you have requested this information from the Firm yourself (and I consider that it is not obliged to provide it to you) I conclude that this will not make any difference, because this Service has already reviewed this information.

Financial
Ombudsman
Service

# If the bank doesn’t believe you, it can be very difficult to get your money back

“



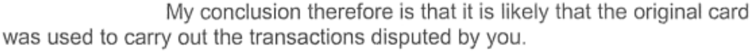
As we have already advised you, since the advent of CHIP and PIN, this Service is not aware of any incidents where a card with a ‘CHIP’ has been successfully cloned by fraudsters so that it could be used by them successfully in a cash machine.

”

Financial
Ombudsman
Service

# If the bank doesn't believe you, it can be very difficult to get your money back

“



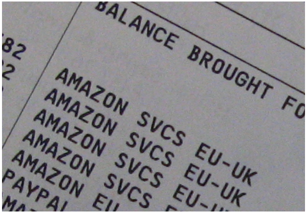
My conclusion therefore is that it is likely that the original card was used to carry out the transactions disputed by you.

”

Financial
Ombudsman
Service

# What can be done

- Check your statements and promptly report anything suspicious
- Don’t write down your PIN or give your bank other excuses to not refund you
- Be persistent if the banks initially don’t believe you



82
2
BALANCE BROUGHT FO
AMAZON SVCS EU-UK
AMAZON SVCS EU-UK
AMAZON SVCS EU-UK
AMAZON SVCS EU-U
PAYPAL EU

For more information:

`http://www.lightbluetouchpaper.org/`

`http://www.cl.cam.ac.uk/research/security/projects/banking`