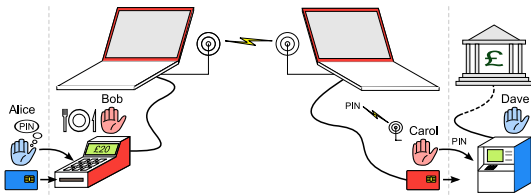


# The Convergence of ATM and Online Transactions



Steven J. Murdoch

<http://www.cl.cam.ac.uk/users/sjm217/>



UNIVERSITY OF  
CAMBRIDGE

Computer Laboratory



CRONTO

[www.cronto.com](http://www.cronto.com)

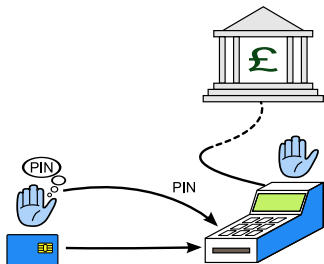
## Card skimming at point of sale

- Previously, PINs were used exclusively at ATMs
- Now they are used at point of sale too
- This opens up the ATM system to attack:
  - Criminals tap communication lines, tamper with terminals and/or install CCTV to watch PIN pads
  - Then collect magnetic strip details and PIN, and use them in ATMs
- Gives criminals cash, rather than goods, and reduces risk of them being caught

Losses of UK customers from their cards being used abroad now total £ 191m in January–June 2008 (up 190% from 2005 figures)

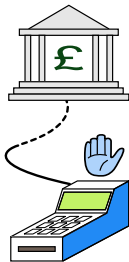
Fraud in the UK is also rising, with retail fraud up by 26% and ATM fraud up by 22%. However these are still lower than the 2005 figures.

## The relay attack against point of sale



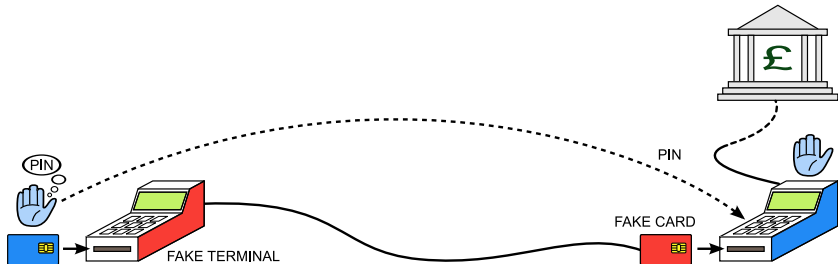
We take a normal Chip and PIN transaction,  
separate the card and the terminal,  
and connect them with a long wire (though this is not very practical)

# The relay attack against point of sale



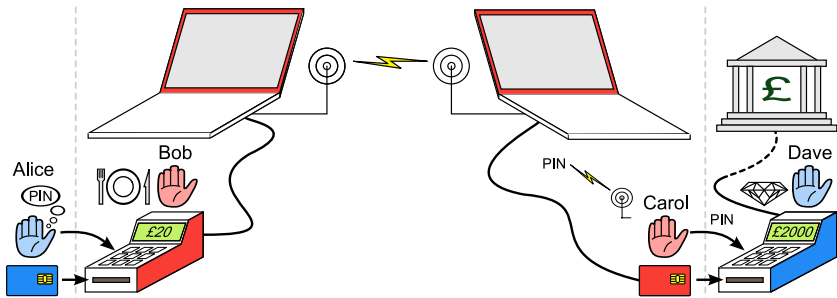
We take a normal Chip and PIN transaction,  
separate the card and the terminal,  
and connect them with a long wire (though this is not very practical)

## The relay attack against point of sale



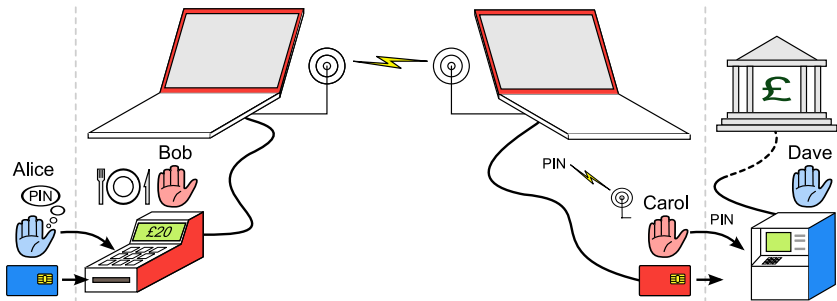
We take a normal Chip and PIN transaction,  
separate the card and the terminal,  
and connect them with a long wire (though this is not very practical)

## The relay attack against point of sale



Alice inserts her card into Bob's *fake* terminal, while Carol inserts a fake card into Dave's *real* terminal. Using wireless communication the £ 2 000 purchase is debited from Alice's account

## The relay attack against ATMs



Same attack will work for an ATM, provided the details on the chip override what is found on the magnetic strip, or the fraudster makes them match beforehand by quickly writing to the magnetic strip

## CAP brings PIN transactions to the home, office and street

- Some banks are rolling out personal card readers, for use in online banking
- If the correct PIN is not entered, the reader will not generate a code
- The bank can verify the one-time password, in the same way as Chip & PIN transactions are
- All UK readers are compatible with all other UK cards





## CAP readers offer muggers an easy way to check card PINs

- Previously, muggers who stole bank cards needed to march the victim to an ATM, to check the PIN
- ATMs are more likely to be located in a busy area, increasing the risk that the mugger will be caught by CCTV or the victim could escape
- Now criminals can use a CAP reader to easily check the PIN on the spot

[guardian.co.uk](http://guardian.co.uk)

### Police think French pair tortured for pin details

**Matthew Taylor**

The Guardian, Saturday July 5 2008



## ATMs are becoming less trustworthy

- Previously, ATMs were in bank branches and heavily protected
- Now they are easily available, and found in shops and on the street
- A further way to collect magnetic strip details, or mount the relay attack, is to set up a fake or tampered ATM
- The owner of the ATM might not even be aware of the attack, if the malicious hardware could be added in the supply chain
- This could be as simple as posting an eBay advert



Categories ▾ Shops eBay Motors

### CASH MACHINE - NCR EASYPOINT 53

Seller of this item? [Sign in](#) for your status



[View larger picture](#)

Starting bid **£500.00**

Your maximum bid: £   
(Enter £500.00)

**Buy It Now** price: **£750.00**

End time: **16-Oct-08 0**

Postage costs: **Free**  
Collection in I  
Service to [Un](#)

Post to: United Kingdo

Item location: Southport, M

History: [0 bids](#)

## Many of these problems could have been prevented with better design

- Chip & PIN card skimming is possible because a copy of the magnetic strip is present on the chip
  - iCVV (removing some details from the chip copy) makes this harder to carry out
  - Swipe and dock readers (which read both the magnetic strip and the chip) are risky
- Obtaining the PIN from a tampered terminal is easy
  - UK cards cannot perform PIN encryption, so the PIN is transmitted unprotected
  - Tamper resistance features of Chip & PIN terminals are trivial to bypass



## Many of these problems could have been prevented with better design

- ATM relay attacks may be a risk in the future
  - ATMs may verify that the magnetic strip details match the chip
  - Currently there are enough non-chip enabled ATMs abroad for criminals to be satisfied
  - If foreign ATM transactions are treated with more suspicion, criminals may adapt
- In some ways, the ATM relay attack is easier to carry out than at point of sale
  - Hanging around the area of an ATM can look less suspicious than an expensive shop
  - There is no staff member who might spot cables on the card
  - Aborting a transaction is not likely to flag an alert because the ATM will see a different card each time

## A different design of CAP could have reduced the mugging risk

- CAP readers only produce a response if the PIN is correct
- In contrast, Racal Watchword and Cronto Transaction Authentication devices just return a different response
- Only the bank can tell the difference

**Step 1 of 3. Payment Details**

To pay someone please enter the details.

**Payee name:**  \*

e.g. Thomas Anderson

**Payee account no.:**  \*

e.g. 11031962


**Payee sort code:**

e.g. 143221

**Amount (EUR):**  .  \*

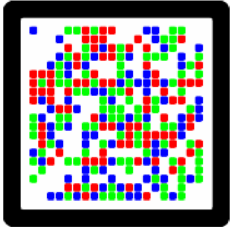
Select Next button to continue

\* - indicates a field required for the demo



## A different design of CAP could have reduced the mugging risk

- CAP readers only produce a response if the PIN is correct
- In contrast, Racal Watchword and Cronto Transaction Authentication devices just return a different response
- Only the bank can tell the difference



**Step 2 of 3. Confirm details**

Payee name:

Payee account no.:

Payee sort code:

Amount:

Please check the transaction details displayed by the Cronto application then enter the authorisation code and click Confirm. [How do I find authorisation code?](#)

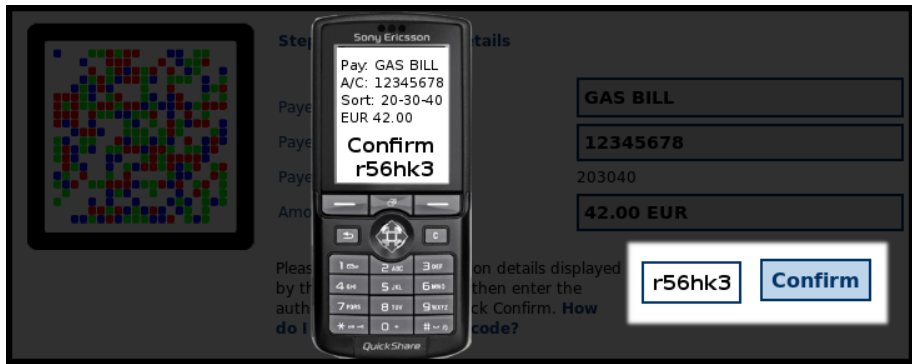
## A different design of CAP could have reduced the mugging risk

- CAP readers only produce a response if the PIN is correct
- In contrast, Racal Watchword and Cronto Transaction Authentication devices just return a different response
- Only the bank can tell the difference



## A different design of CAP could have reduced the mugging risk

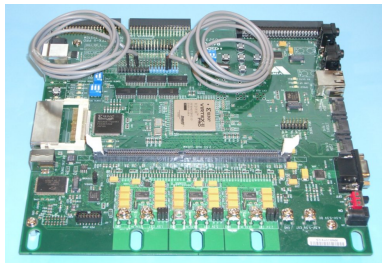
- CAP readers only produce a response if the PIN is correct
- In contrast, Racal Watchword and Cronto Transaction Authentication devices just return a different response
- Only the bank can tell the difference





## Relay attacks can be resisted by distance bounding or trusted display

- Distance bounding gives the ATM a strong assurance that the real card is being used
  - The time it takes for a card to respond is measured
  - If there is a relay attack, the fake card cannot respond in time because information cannot be sent faster than the speed of light



## Relay attacks can be resisted by distance bounding or trusted display

- Alternatively, the ATM or point of sale terminal could have a Near-Field Communications (NFC) interface added
  - Then, the amount to be debited would be shown on the customer's phone, not the untrustworthy ATM
- Distance bounding and NFC both need new ATM hardware (expensive)
- The Cronto transaction authentication system could be used on existing ATMs to generate one-time PINs that are valid only for the amount the customer sees on their phone



## All security solutions need to be regularly tested by experts

- There is often a large gap between planned security and actual security of deployed systems
- Bad news doesn't travel up company hierarchies – if a mechanism doesn't work, management will often not know
- For example, iCVV was supposed to be mandatory by January 2008 to resist skimming attacks
- However, in February, cards were still being issued without this extra security feature, despite media announcements
- Even when security mechanisms work, a system upgrade might break them and nobody will notice
- A “red-team” should be continually testing all security measures
  - Checking that systems reject invalid requests
  - Checking that the bad requests are logged
  - Checking that an alert is triggered on malicious actions

## Conclusions

- ATM security is increasingly bound to retail and online banking
- Chip & PIN at point of sale has led to new opportunities for ATM fraud, and is actively being exploited
- The use of Chip & PIN for online transactions has created new risks for street-crime
- Using separate systems can reduce the problems we now see
- The relay attack is particularly problematic since it cannot be solved with cryptography
- Instead, a trusted display and/or distance bounding mechanism is needed
- Regardless of the mechanism, continuous testing is required for maintaining security