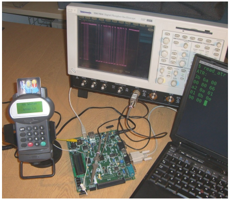
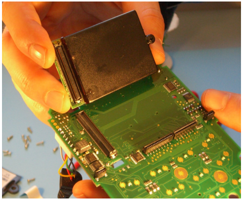
Security vulnerabilities of Chip and PIN

Saar Drimer

www.cl.cam.ac.uk/~sd410

Security Group





UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Show and Tell Event, 30 September 2008

The Security Group

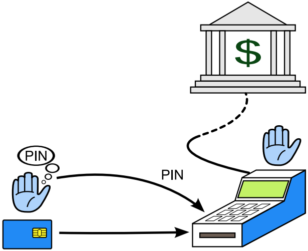
We work on: **hardware and software security, protocols, anonymity, privacy, phishing, forensics, security economics and psychology, banking security, and more...**

Group's page: `http://www.cl.cam.ac.uk/research/security/`

Chip and PIN was touted as “totally secure”

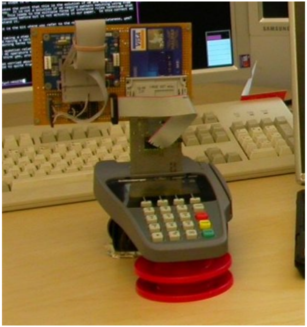
Chip and PIN is fully deployed in the UK since 2006, with banks making grand claims of security;

1066 requires a correct 4 digit PIN input for authorizing transactions (both at ATMs and cash registers);



...no greater motivation for us to look into it!

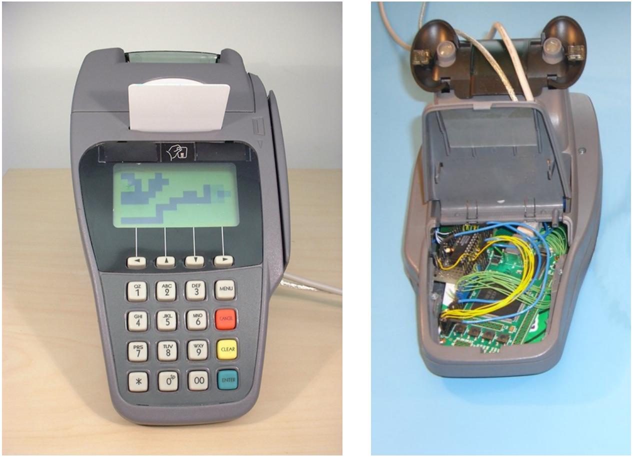
With the “interceptor” we found out more about how the card processes transactions



We found out that data between the card and reader isn’t encrypted during a transaction and that the PIN is sent *in the clear*! **UK banks have chosen to deploy the cheapest smartcards possible.**

Paper: “**Chip and Spin**”, `http://www.chipandspin.co.uk/spin.pdf`
by Ross Anderson, Mike Bond, Steven J. Murdoch

We made a Chip and PIN terminal play Tetris



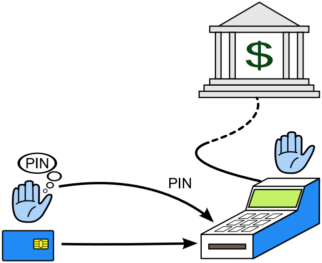
By replacing the internals of the terminal it was completely under our control. **Cardholders have no way of differentiating between a real terminal and a fake or tampered-with one.**

Watch video: `http://www.lightbluetouchpaper.org/2006/12/24/chip-pin-terminal-playing-tetris/`

The chip inside of the smartcard is very hard to clone...

The **relay attack** allows criminals to debit a card with unauthorized transactions without needing to clone the chip

The relay attack: Alice thinks she is paying $20, but is actually charged $2,000 for a purchase elsewhere



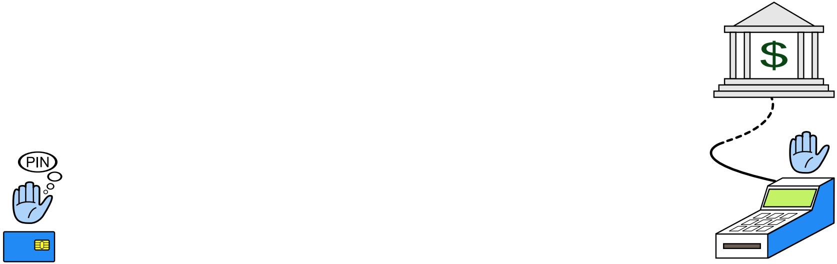
We take a normal Chip and PIN transaction,

separate the card and the terminal,

and connect them with a long wire (though this is not very practical!)

Paper: "**Keep your enemies close: distance bounding against smartcard relay attacks**"
by Saar Drimer, Steven J. Murdoch; USENIX Security Symposium '07 – awarded Best Student Paper

The relay attack: Alice thinks she is paying $20, but is actually charged $2,000 for a purchase elsewhere



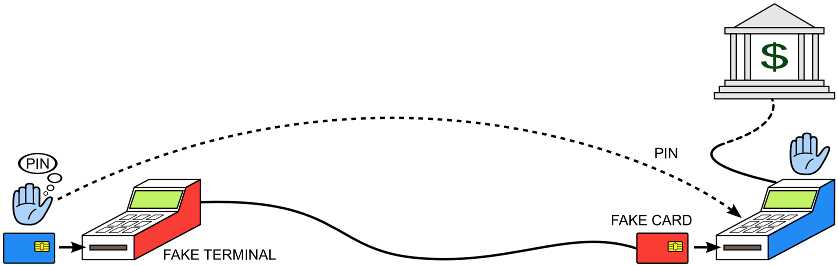
We take a normal Chip and PIN transaction,

separate the card and the terminal,

and connect them with a long wire (though this is not very practical!)

Paper: “**Keep your enemies close: distance bounding against smartcard relay attacks**”
by Saar Drimer, Steven J. Murdoch; USENIX Security Symposium ’07 – awarded Best Student Paper

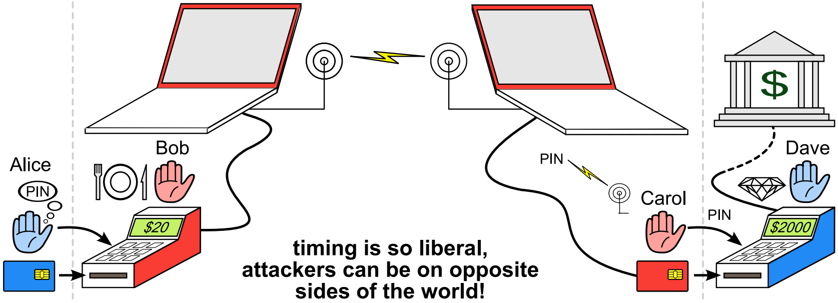
The relay attack: Alice thinks she is paying $20, but is actually charged $2,000 for a purchase elsewhere



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!)

Paper: “**Keep your enemies close: distance bounding against smartcard relay attacks**”
by Saar Drimer, Steven J. Murdoch; USENIX Security Symposium ’07 – awarded Best Student Paper

The relay attack: Alice thinks she is paying $20, but is actually charged $2,000 for a purchase elsewhere



timing is so liberal, attackers can be on opposite sides of the world!

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

Paper: "**Keep your enemies close: distance bounding against smartcard relay attacks**"
by Saar Drimer, Steven J. Murdoch; USENIX Security Symposium '07 – awarded Best Student Paper

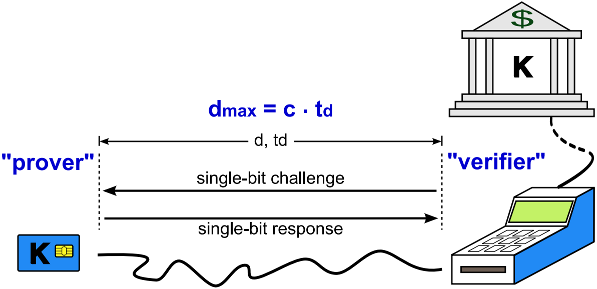
Our attack was shown on BBC1's "Watchdog", February 2007

We showed that this really works between a restaurant and bookstore in Cambridge

> *"We got our highest ratings of the run for the story (6.2 million, making it the most watched factual programme of last week)... it's provoked quite a response from viewers."*
>
> – Rob Unsworth, Editor, "Watchdog"

Watch video: `http://www.youtube.com/watch?v=X7pjUIxKoEc`

We have also implemented a distance bounding defence for the relay attack

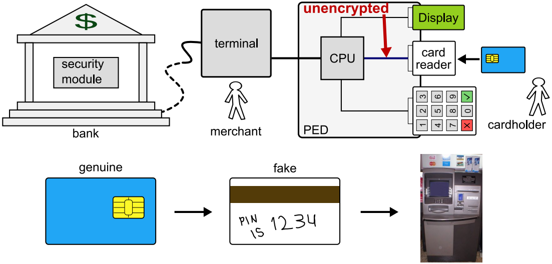


We adapted the Hancke-Kuhn distance bounding protocol* to a wired implementation. With this, the terminal can know the the card is within a few meters radius. **Will banks adopt our solution?**

* Developed in our group by **Gerhard Hancke** and **Markus G. Kuhn**

Paper: "**Keep your enemies close: distance bounding against smartcard relay attacks**"
by Saar Drimer, Steven J. Murdoch; USENIX Security Symposium '07 – awarded Best Student Paper

What if crooks can subvert the PIN Entry Devices (PEDs) we use for transactions?



By “tapping” the communication line between the card and the PED’s processor, criminals can create a magnetic strip version of the card and use at ATMs that do not read smartcards (like in the U.S.)

PEDs use tamper proofing and are certified to prevent criminals from doing this!

Paper: “**Thinking inside the box: system-level failures of tamper proofing**” by Saar Drimer, Steven J. Murdoch, Ross Anderson; IEEE Security and Privacy (Oakland) ’08 – awarded Best Practical Paper

Tamper proofing is required to protect customers' PINs and banks' keys quite well, but...

- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD $25,000 per PED**

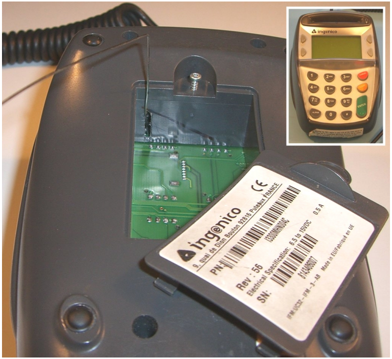
We've shown that these PEDs failed these evaluations miserably

Paper: "**Thinking inside the box: system-level failures of tamper proofing**"
by Saar Drimer, Steven J. Murdoch, Ross Anderson; IEEE Security and Privacy (Oakland) '08 – awarded Best Practical Paper

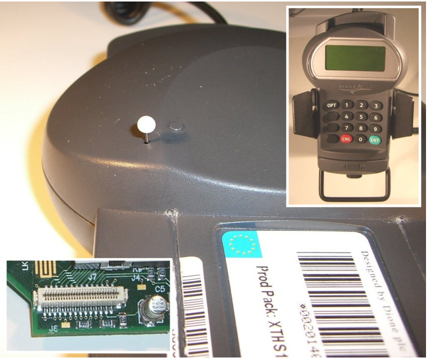
We found serious vulnerabilities in the most popular PEDs used in the UK

We got a few PEDs off of eBay...

Ingenico i3300


ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
Rev : 56
Made in EU/Fabriqué en UE

Dione Xtreme



Criminals just need to know where to drill!

Paper: "**Thinking inside the box: system-level failures of tamper proofing**"
by Saar Drimer, Steven J. Murdoch, Ross Anderson; IEEE Security and Privacy (Oakland) '08 – awarded Best Practical Paper

The PED attack was shown on “Newsnight” in February 2008

> *We believe that the risk remains very low. [This attack] is significantly difficult to industrialise to the numbers of devices that would gain criminals the return they would expect and, therefore, not economically viable to criminals.*
>
> – APACS (UK bank industry body), **February 2008**

Criminals have been tampering with PEDs since at least 2006, and increasingly so today

Watch video: `http://video.google.com/videoplay?docid=7109740591622124830`
Read all responses to our attack: `http://www.cl.cam.ac.uk/research/security/banking/ped/`

See more of what the **Security Group** does!

blog:

`http://www.lightbluetouchpaper.org`

webpage:

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

Thanks to XILINX for funding my research!