Access Control and Privacy Policies (1)


Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS

Security Engineers

According to Bruce Schneier, **security engineers** require a particular **mindset**:

> "Security engineers — at least the good ones — see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it."
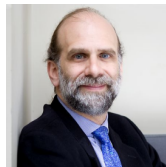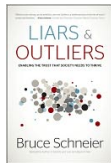
Yes…

> The Guardian (2006): "Chip-and-PIN is so effective in this country that fraudsters are starting to move their activities overseas," said Emile Abu-Shakra, spokesman for Lloyds TSB.

- mag-stripe cards cannot be cloned anymore
- stolen or cloned cards need to be used abroad
- fraud on lost, stolen and counterfeit credit cards was down £60m (24%) on 2004's figure

BUT...

Bank

shop

costumer / you

BUT...

Bank

shop

terminal producer

costumer / you

Chip-and-PIN

- "tamperesitant" terminal playing Tetris on youtube

 (http://www.youtube.com/watch?v=wWTzkD9M0sU)

Chip-and-PIN

- in 2006, Shell petrol stations stopped accepting Chip-and-PIN after £1m had been stolen from customer accounts

- in 2008, hundreds of card readers for use in Britain, Ireland, the Netherlands, Denmark, and Belgium had been expertly tampered with shortly after manufacture so that details and PINs of credit cards were sent during the 9 months before over mobile phone networks to criminals in Lahore, Pakistan
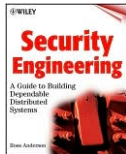
Chip-and-PIN is Broken
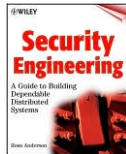
- Man-in-the-middle attacks by the group around Ross Anderson
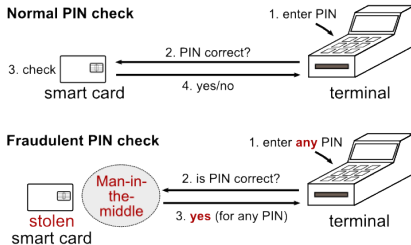
Chip-and-PIN is Really Broken

- same group successfully attacked last this year card readers and ATM machines
- the problem: several types of ATMs generate poor random numbers, which are used as nonces

The Problem...

Bank

shop

terminal producer

costumer / you

- the burden of proof for fraud and financial liability shifted to the costumer

Screwed Again

- **Responsibility**
  "You understand that you are financially
  responsible for all uses of RBS Secure."

  `https://www.rbssecure.co.uk/rbs/tdsecure/terms_of_`
  `use.jsp`