# 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."
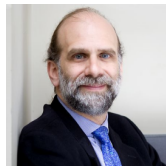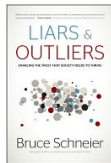
# Chip-and-PIN



- Chip-and-PIN was introduced in the UK in 2004
- before that customers had to sign a receipt
- Is Chip-and-PIN a more secure system?

(Some other countries still use the old method.)

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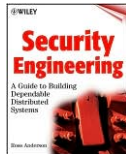
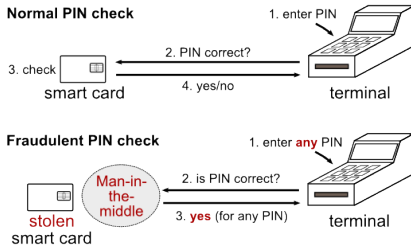  (http://www.youtube.com/watch?v=wWTzkD9M0sU)

# 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
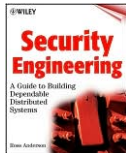
# Chip-and-PIN is Broken



- Man-in-the-middle attacks by the group around Ross Anderson



**Normal PIN check**

3. check — smart card

2. PIN correct?

4. yes/no

1. enter PIN

terminal

**Fraudulent PIN check**

stolen smart card

Man-in-the-middle

2. is PIN correct?

3. **yes** (for any PIN)

1. enter **any** PIN

terminal

# 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
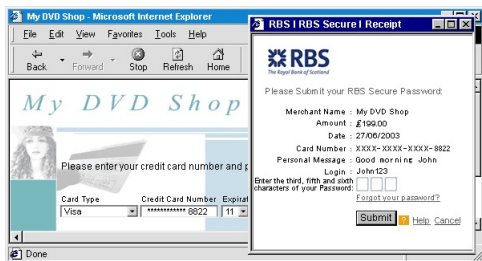
# The Problem…



Bank

shop

terminal producer

costumer / you

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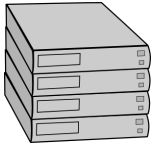
# Screwed Again



- **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`

# Web Applications



Servers from
Dot.com Inc.

Client

- What are pitfalls and best practices?

# Brute Forcing Passwords

- How fast can hackers crack passwords?

# Brute Forcing Passwords

- How fast can hackers crack passwords?
- The answer is 2 billion per second using a Radeon HD 7970

| password length | time |
|---|---|
| 5 letters | 5 secs |
| 6 letters | 500 secs |
| 7 letters | 13 hours |
| 8 letters | 57 days |
| 9 letters | 15 years |

5 letters = $100^5$ = 10 billion combinations
(1 letter ≈ upper case, lower case, digits, symbols)

# Privacy

- Scott McNealy:
  "You have zero privacy anyway. Get over it."

# Passwords

- How do recover from a break in?

# Thinking as a Defender

- What are we trying to protect?
- What properties are we trying to enforce?

- Who are the attackers? Capabilities? Motivations?
- What kind of attack are we trying to protect?
- Who can fix any vulnerabilities?

- What are the weaknesses of the system?
- What will successful attacks cost us?
- How likely are the attacks?

- Security almost always is **not** free!

# The Security Mindset

- How things can go wrong.
- Think outside the box.

The difference between a criminal is to only think about how things can go wrong.