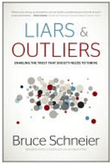
Access Control and Privacy Policies (1)

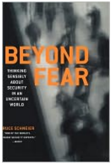
Email:	christian.urban at kcl.ac.uk
Office:	S1.27 (1st floor Strand Building)
Slides:	KEATS

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? What do you think?

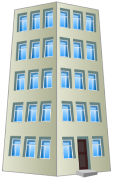
(Some other countries still use the old method.)

Yes...

> "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 (in the Guardian, 2006).

- 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

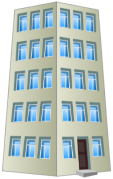
Let's see. . .



Bank

costumer / you

Let’s see. . .



Bank

terminal
producer

costumer / you

Chip-and-PIN

- A “tamperesitant” terminal playing Tetris on youtube.

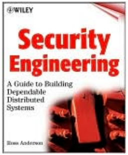
(http://www.youtube.com/watch?v=wWTzkD9M0sU)

Chip-and-PIN

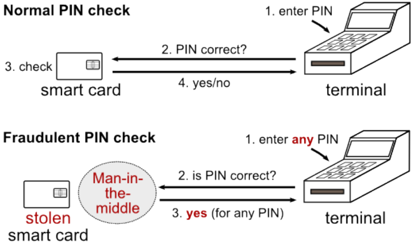
- in 2006, Shell petrol stations stopped accepting Chip-and-PIN after £1m had been stolen from customer accounts

- 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

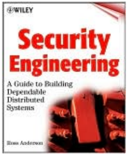


- man-in-the-middle attacks by the group around Ross Anderson



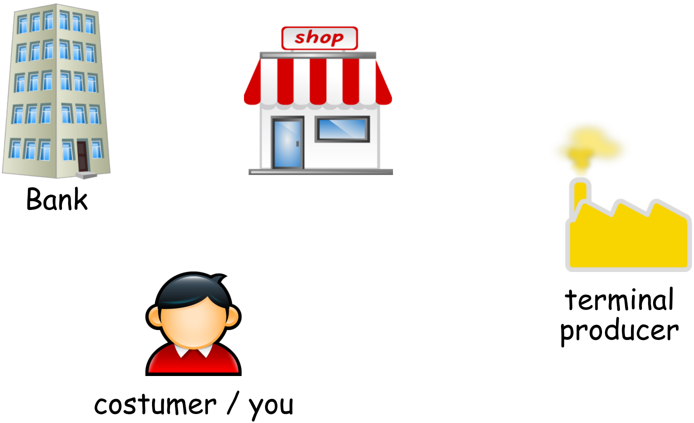
on BBC Newsnight
in 2010 or youtube

Chip-and-PIN is Really Broken



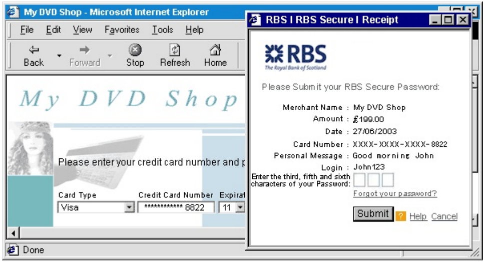
- same group successfully attacked this year card readers and ATM machines
- the problem: several types of ATMs generate poor random numbers, which are used as nonces

The Problem…



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

Screwed Again



Please enter your credit card number and p

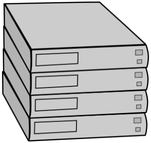
Card Type	Credit Card Number	Expirat
Visa	************ 8822	11

Please Submit your RBS Secure Password:

Merchant Name :	My DVD Shop
Amount :	£199.00
Date :	27/06/2003
Card Number :	XXXX-XXXX-XXXX-8822
Personal Message :	Good morning John
Login :	John123
Enter the third, fifth and sixth characters of your Password:	□□□

- **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?

Scala + Play

```scala
package controllers
import play.api.mvc._

object Application extends Controller {

  // answering a GET request
  val index = Action { request =>

    Ok("Hello world!")
  }

}
```

alternative response:

```scala
Ok("<H1>Hello world!</H1>").as(HTML)
```

```
object Application extends Controller {

  // presenting login form
  val index = Action { request =>

    val form = """<form method="post">
                Login: <input type="text" name="login"><br>
                Password: <input type="password" name="password"><br>
                <input type="submit"></form>"""

    Ok(form).as(HTML)
  }


  // processing the received login data
  val receive = Action { request =>

    val form_data = Form (tuple ("login" -> text, "password" -> text))

    val (login, password) = form_data.bindFromRequest()(request).get

    Ok("Received login: " + login + " and password: " + password)
  }

}
```

Brute Forcing Passwords

- How fast can hackers crack SHA-1 passwords?

Brute Forcing Passwords

- How fast can hackers crack SHA-1 passwords?
- The answer is 2 billion attempts 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

graphics card
ca. £300

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

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.