Why Cryptosystems Still Fail

Ross Anderson

Cambridge

Cosade, Berlin, 2015

Why Cryptosystems Fail

- "Why Cryptosystems Fail" describes work I did while a research student
- Acted as expert witness in case where 2000 people sued 13 banks for £2m in refunds
- Banks made many bad design choices, such as
  - writing encrypted PIN on mag strip (without salting it with the account number)
  - printing full account number on receipt (so the bad guys could shoulder surf)

Why cryptosystems fail (2)

- Implementation and operations were worse!
  - Clerical insiders issuing extra cards
  - Technical insiders using test equipment to steal
  - Postal interception
  - Lebanese loop
- the banks usually managed to blame the customers for fraud!
- Even after Andrew Stone went to jail for 6 ½ years, most customers never got a refund

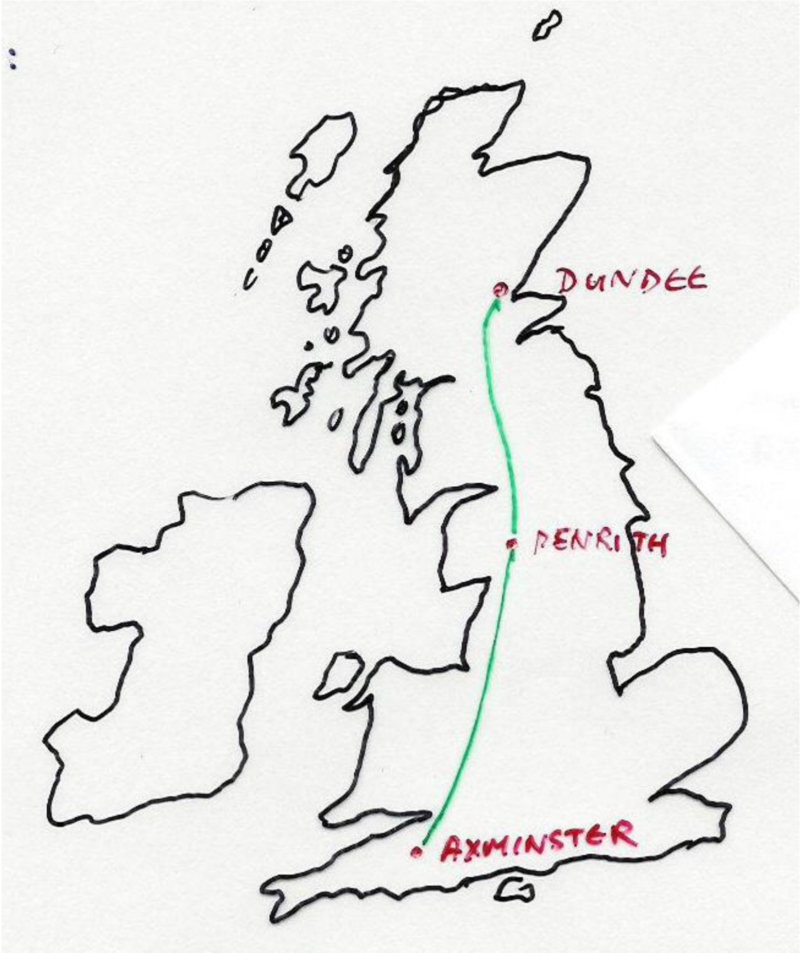
Prepayment meters

Fraud

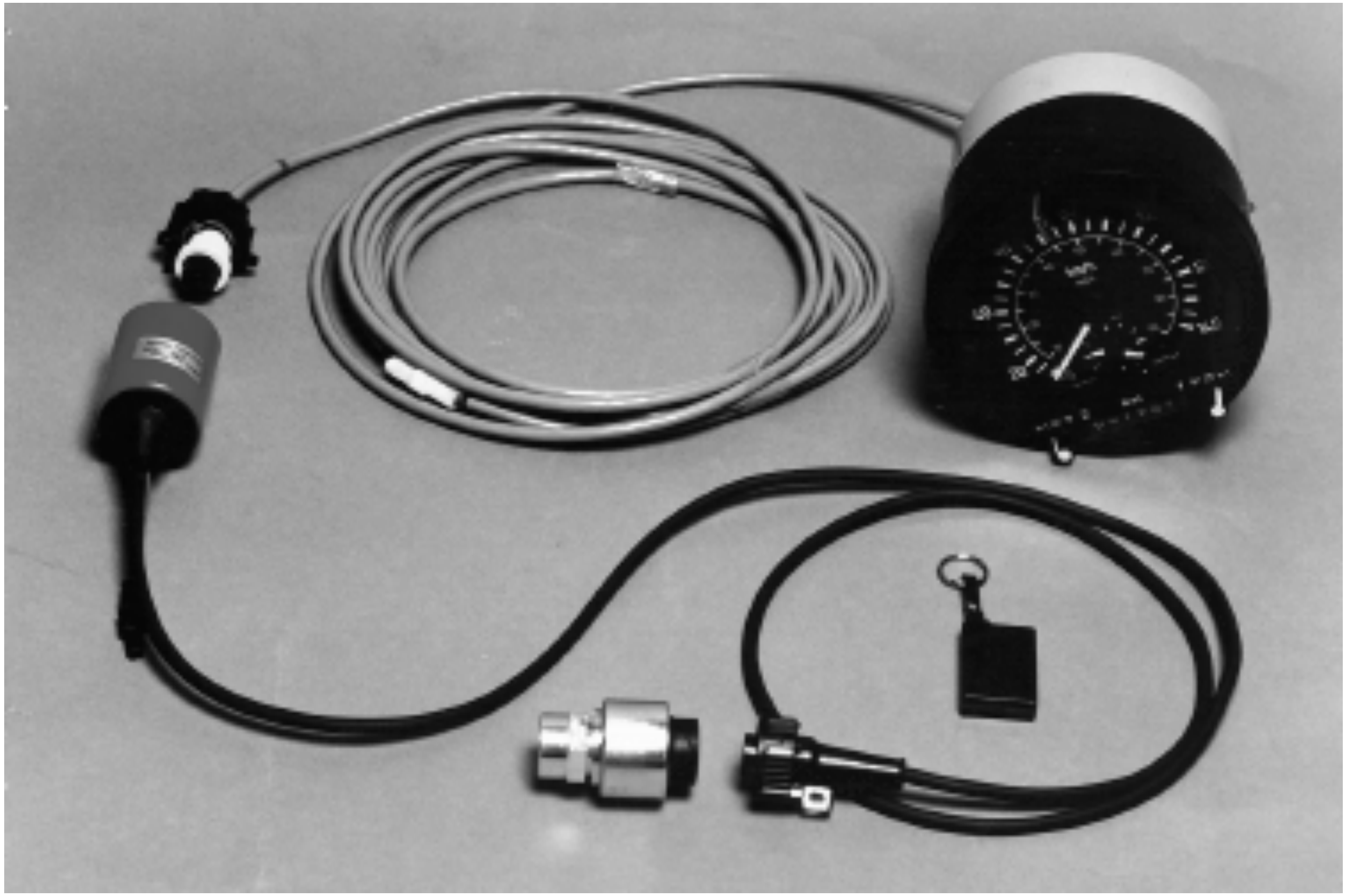
- First-generation crypto-based prepayment meters introduced from late 80s early 90s. Lessons:
  - Bugs – brownout, feature interaction
  - Fraud by intermediaries such as token resellers
  - But it can be cheap: 5% of revenue
- Fraud by utilities too, e.g broken clocks not fixed unless on cheap rate
- No entirely trustworthy player!
- Took several iterations to get it right
- And once we have complex smart meters?

Embedded systems

- I analysed tachograph fraud in 1998
- Procedural exploits were 68% of all driver offences, 71% of all operator offences
- Typical method: collusion between drivers and employers
- The move to digital made it worse



Alice, Bob and Charlie



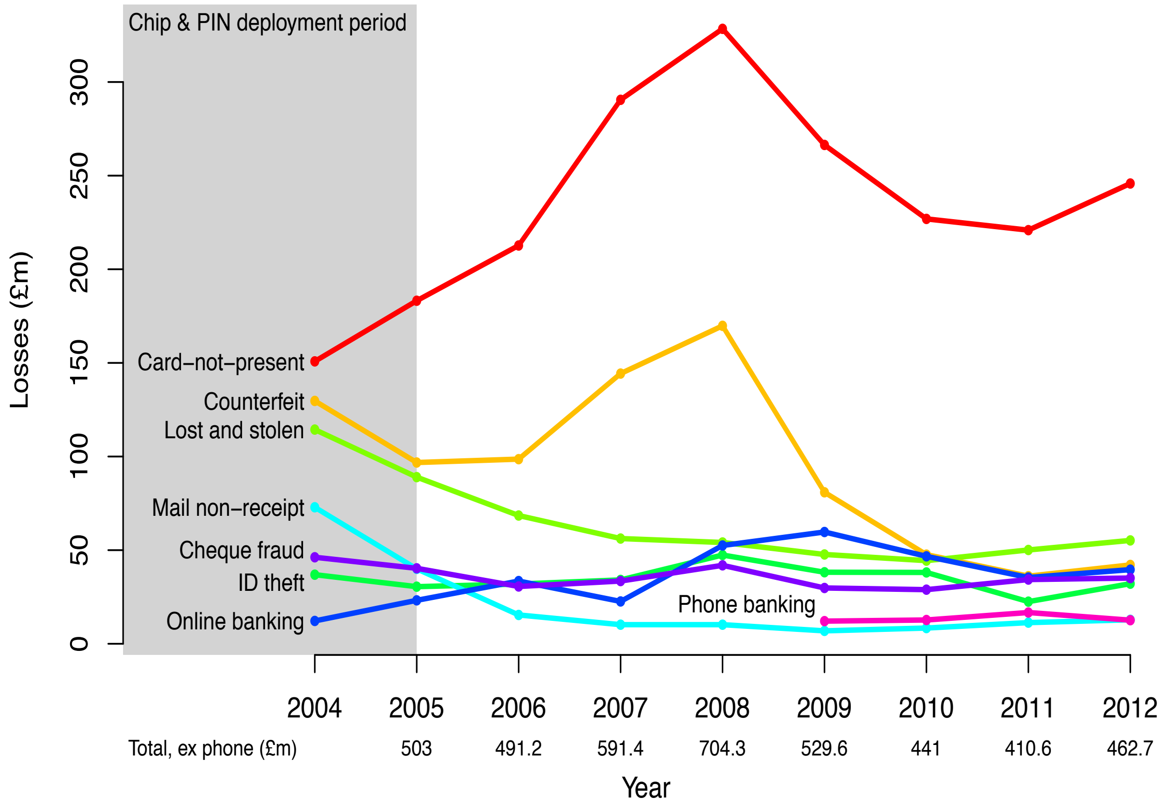
The EMV protocol suite

- Named for Europay-MasterCard-Visa; also known as ‘chip and PIN’
- Developed late 1990s; deployed in UK ten years ago (2003–5; mandatory 2006)
- Europe, Canada followed
- About to be deployed in the USA (by 2015)
- Fascinating story of failures and frauds
- Many lessons for security engineers!

Concept of operations

- Make forgery harder by replacing the mag strip with a chip, which authenticates card
- Make authentication of cardholder stronger by replacing the signature with a PIN
- Keep verifying PINs online at ATMs, but verify on the chip at merchant terminals
- Encourage deployment by making the merchant liable if PIN not used (‘liability shift’)

Fraud history, UK



- Cardholder liable if PIN used
- Else merchant pays
- Banks hoped fraud would go down
- It went up …
- Then down, then up again

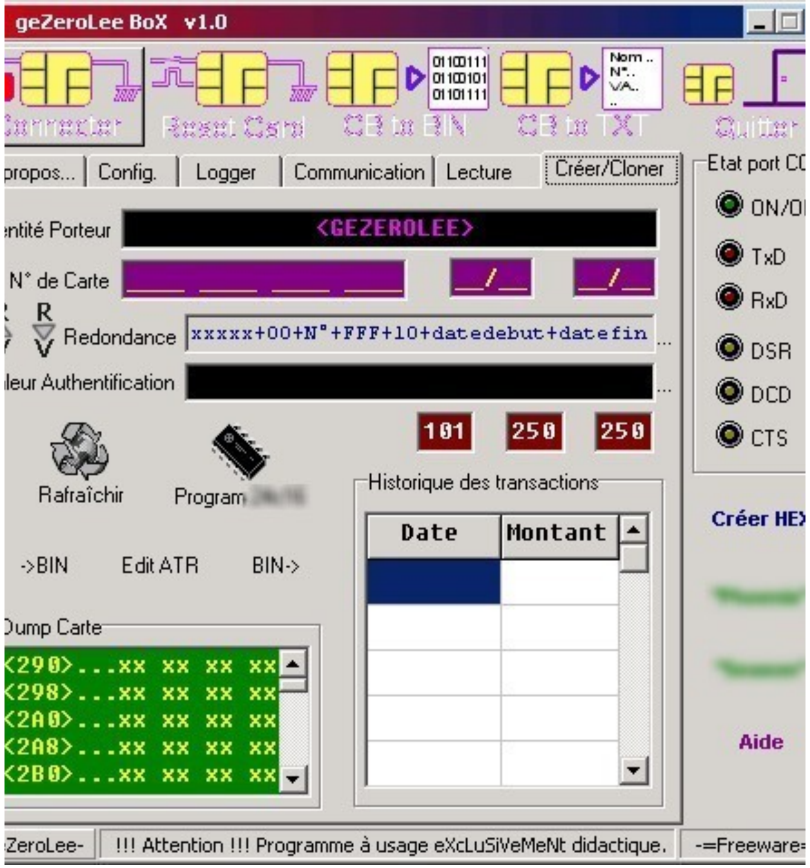
EMV shifted the landscape…

- Like bulldozing a floodplain, it caused the fraud to find new channels
- Card-not-present fraud shot up rapidly
- Counterfeit took a couple of years, then took off once the crooks realised:
  - It's easier to steal card and PIN details once PINs are used everywhere
  - You can still use mag-strip fallback overseas
  - Tamper-resistance doesn't work

Attack the crypto

- EMV broke all the cryptographic hardware security modules in the world!
- A transaction specified by VISA to send an encrypted key to a smartcard leaked keys instead
- See 'Robbing the bank with a theorem prover', Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ronald L Rivest, Ross Anderson, SPW 2007
- Ben now works for Square, Jol for Deutsche…

Attack the optimisations



ntité Porteur <GEZEROLEE>

N° de Carte ____ ____ ____ ____ __/__ __/__

Redondance xxxxx+00+N°+FFF+10+datedebut+datefin

leur Authentification

101 250 250

Historique des transactions

Date	Montant

Dump Carte

```
<290>...xx xx xx xx
<298>...xx xx xx xx
<2A0>...xx xx xx xx
<2A8>...xx xx xx xx
<2B0>...xx xx xx xx
```

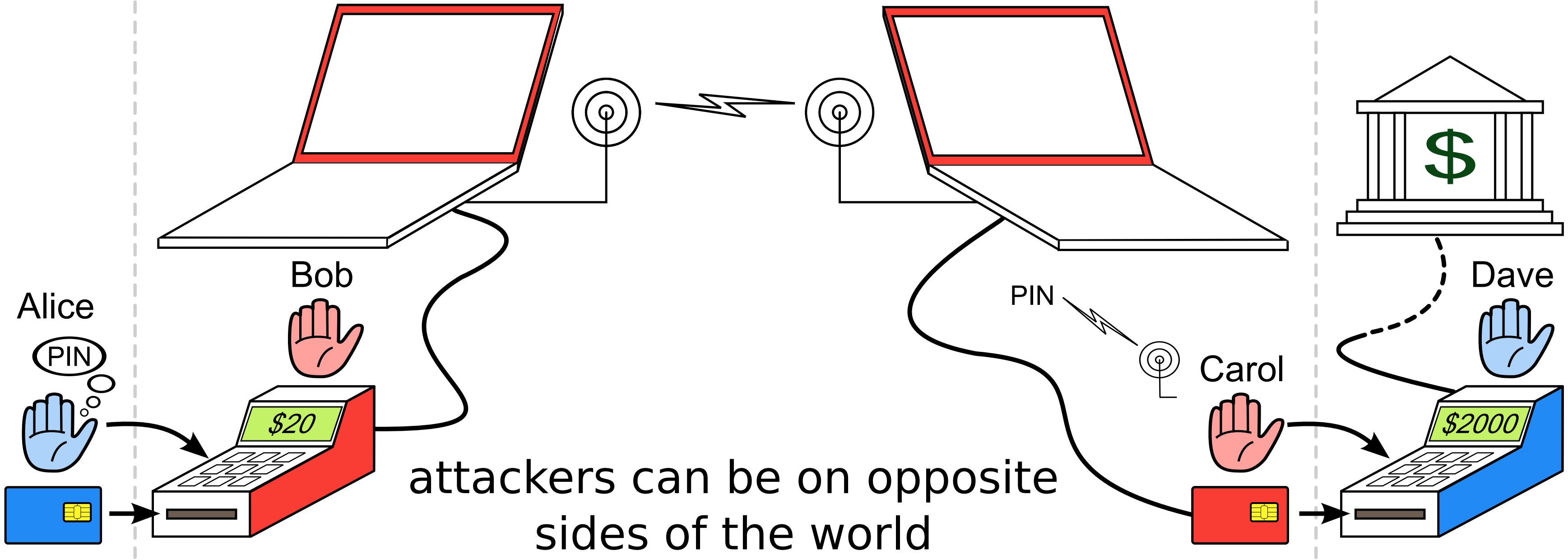
ZeroLee- | !!! Attention !!! Programme à usage eXcLuSiVeMeNt didactique. | -=Freeware=

- Cheap cards are SDA (no public key capability, so static certificate)
- A 'yes card' can impersonate in an offline terminal
- Fairly easy to do, but not seen much

What about a false terminal?

- Replace a terminal’s insides with your own electronics
- Capture cards and PINs from victims
- Use them to do a man-in-the-middle attack in real time on a remote terminal in a merchant selling expensive goods

The relay attack (2007)



attackers can be on opposite sides of the world

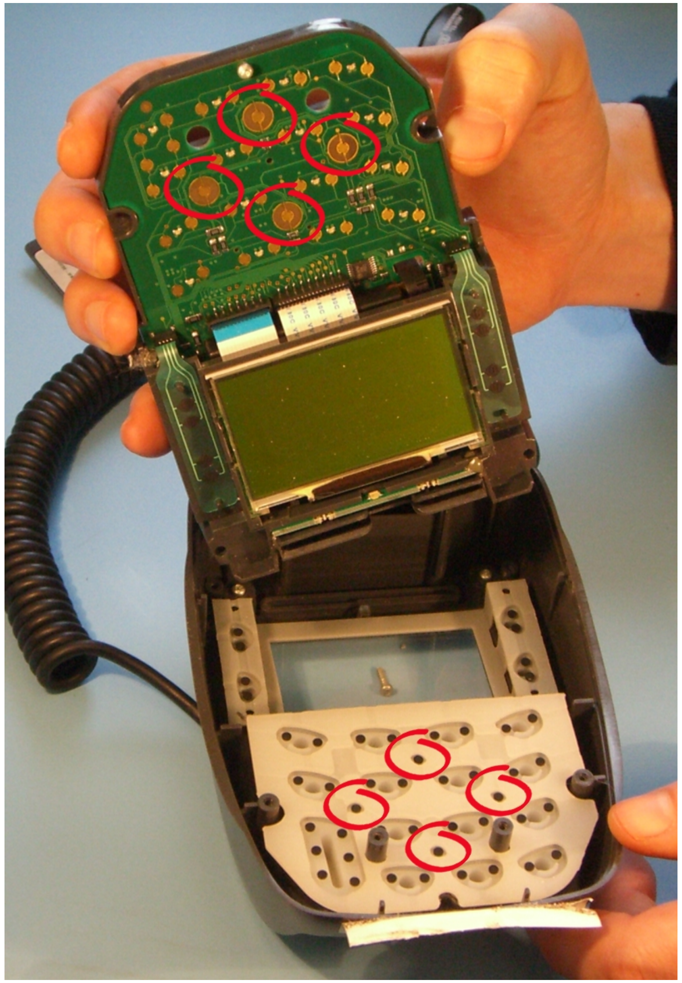
Attacks in the real world

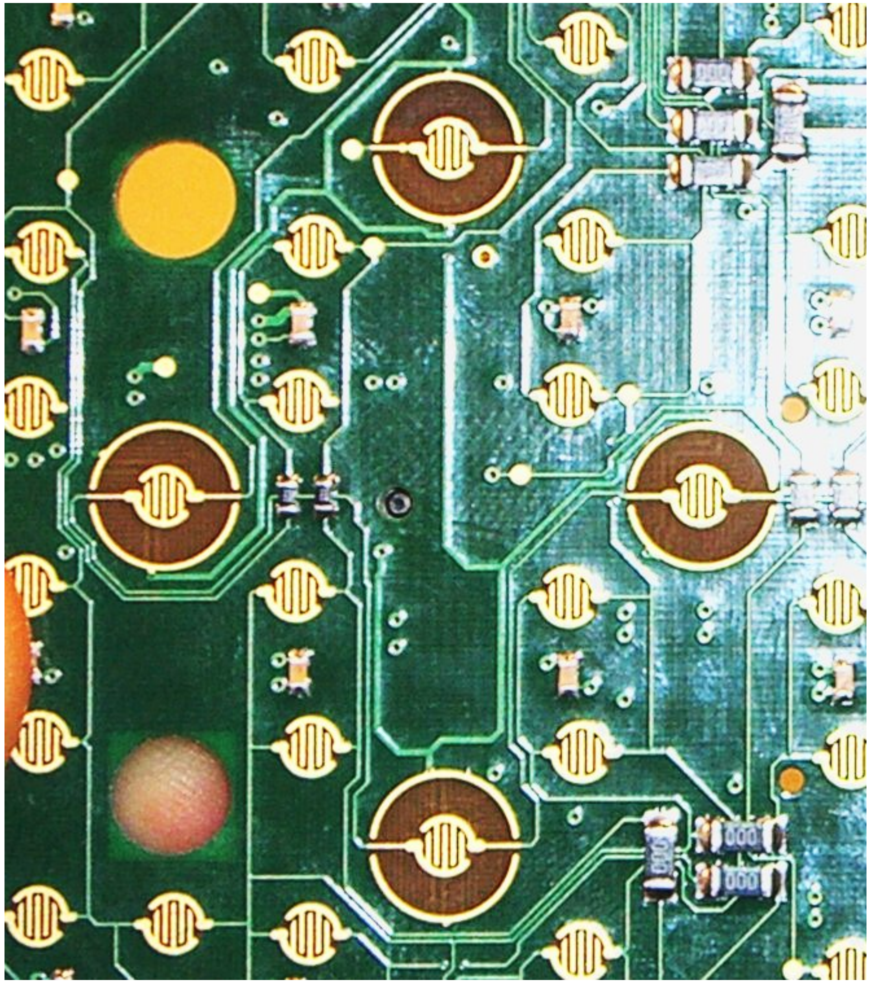
- The relay attack is almost unstoppable, and we showed it in TV in February 2007
- But it seems never to have happened!
- So far, mag-strip fallback fraud has been easy
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier was blamed)
- Then ‘Tamil Tigers’
- After fraud at BP Girton, we investigate

Tamper-proofing of the PED

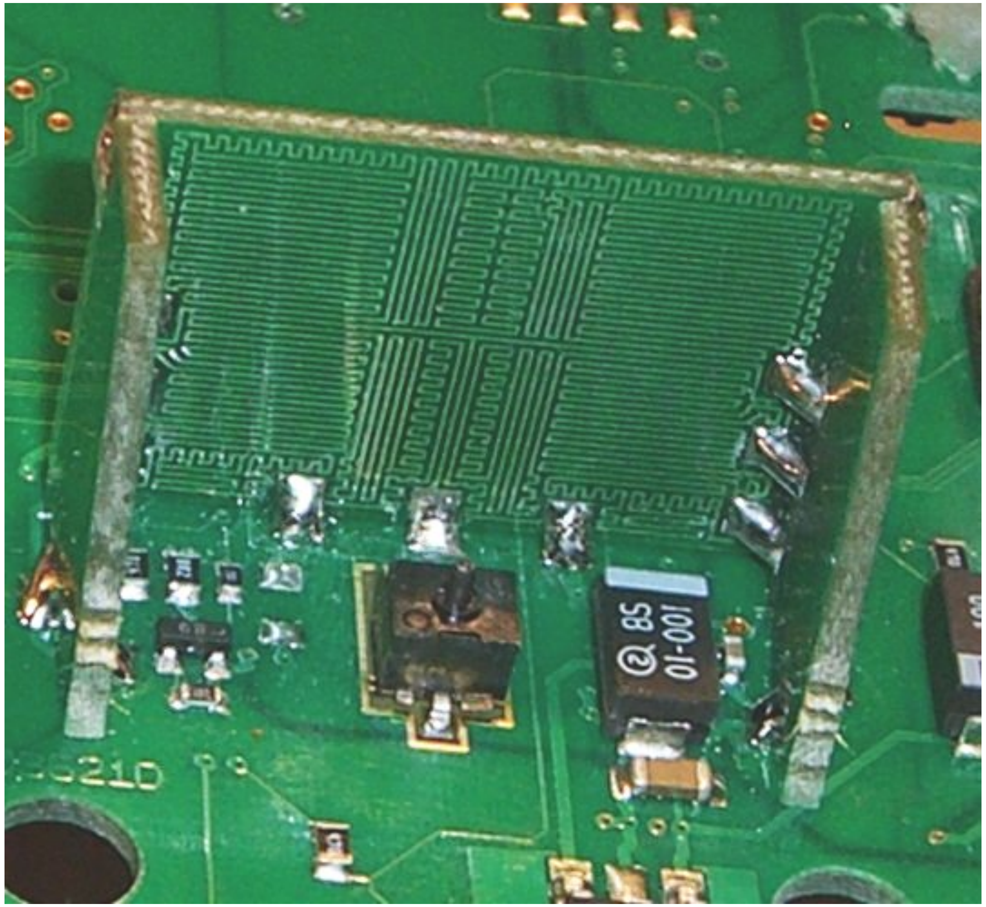
- In EMV, PIN sent from PIN Entry Device (PED) to card
- Card data flow the other way
- PED supposed to be tamper resistant according to VISA, APACS (UK banks), PCI
- ‘Evaluated under Common Criteria’
- Should cost $25,000 per PED to defeat

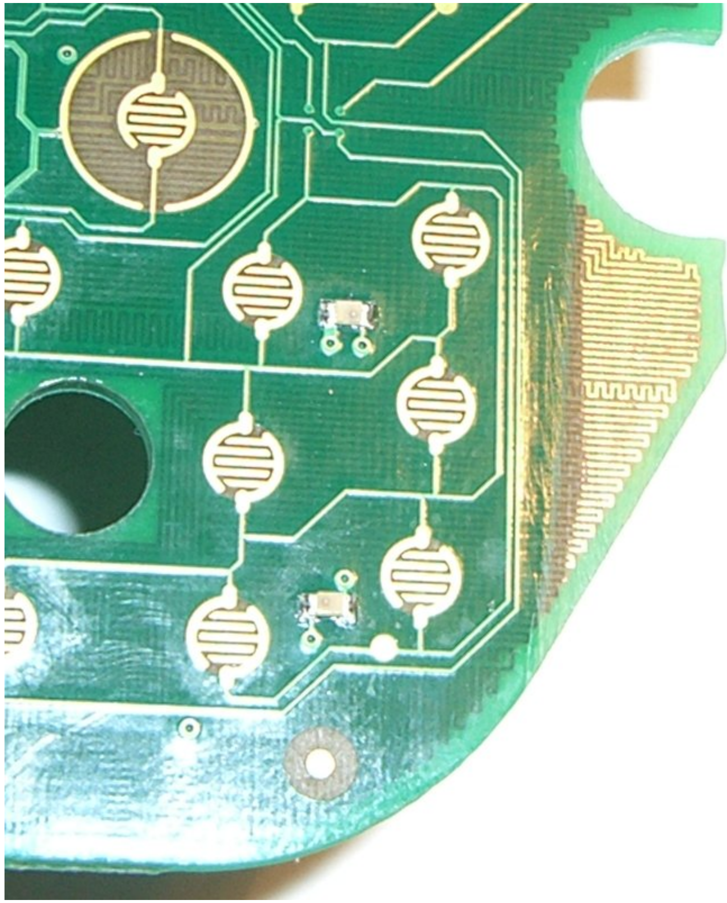
Tamper switches (Ingenico i3300)



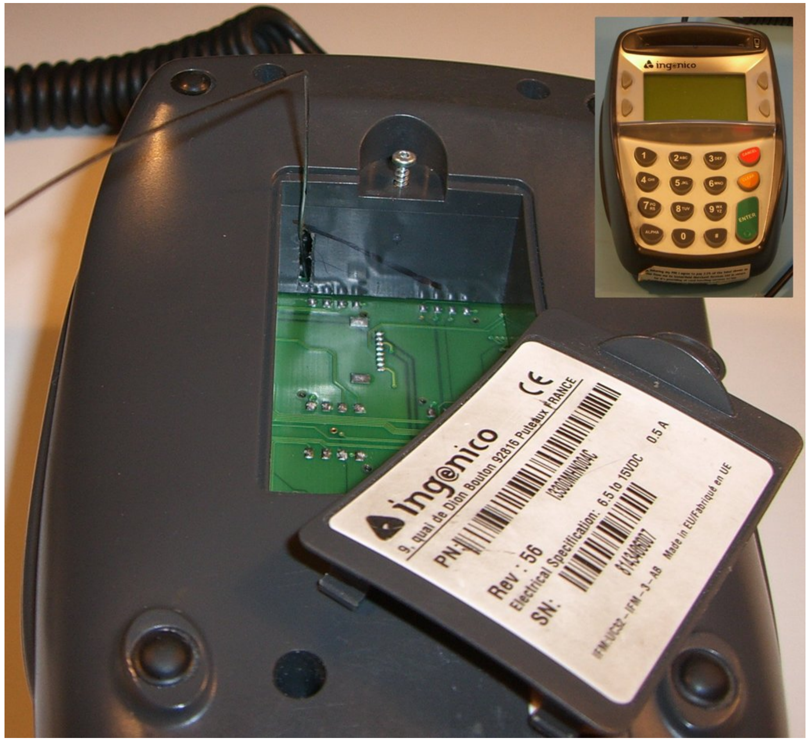


… and tamper meshes too





TV demo: Feb 26 2008

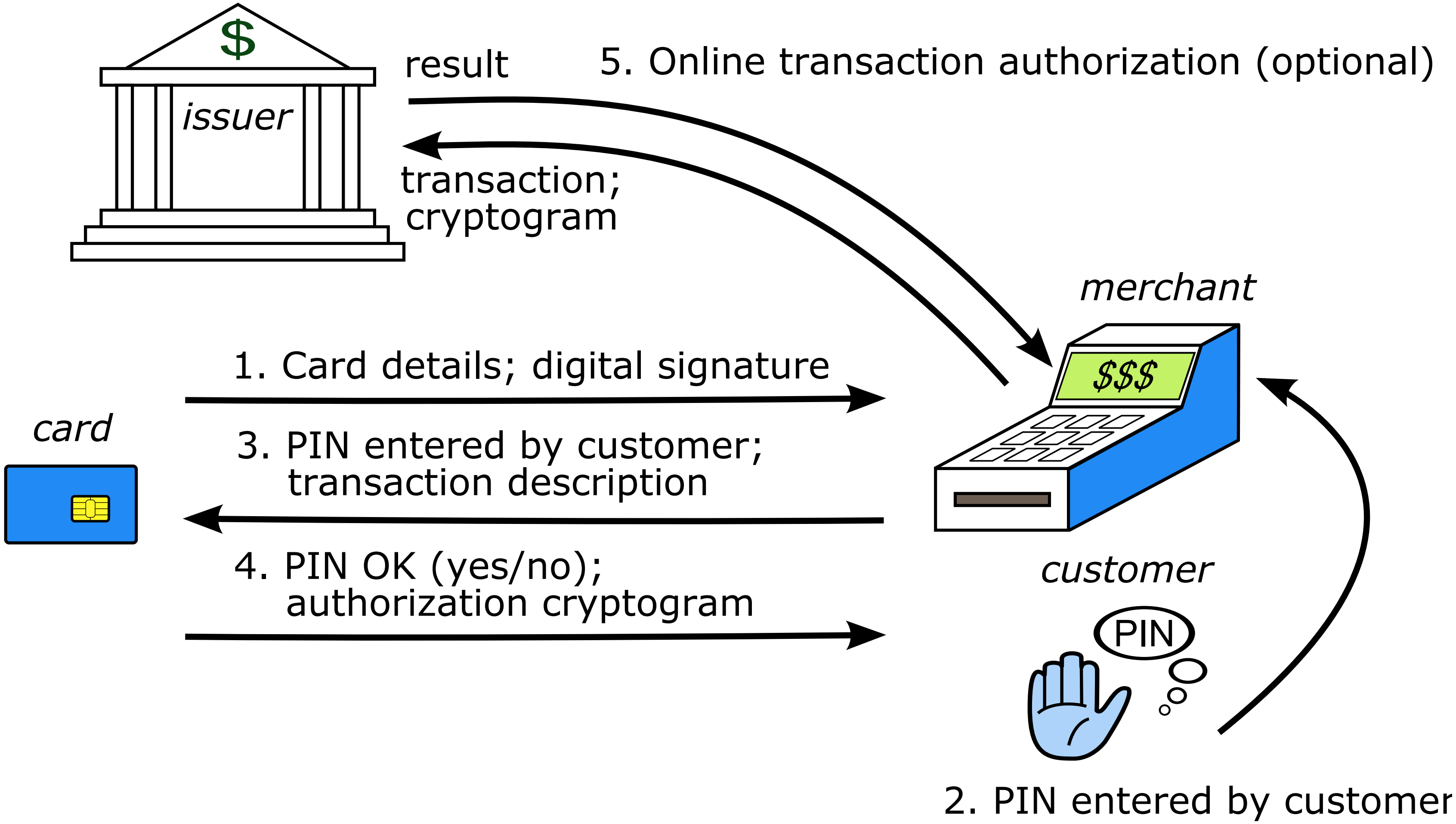

ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
PN:
Rev : 56
Electrical Specification: 6.5 to 15VDC 0.5 A
SN:
Made in EU/Fabriqué en UE
ENTER

- PEDs ‘evaluated under the Common Criteria’ were trivial to tap
- Acquirers, issuers have different incentives
- GCHQ wouldn’t defend the CC brand
- APACS said (Feb 08) it wasn’t a problem…
- Khan case (July 2008)

The ‘No-PIN’ attack

- How could crooks use a stolen card without knowing the PIN?
- We found: insert a device between card & terminal
- Card thinks: signature; terminal thinks: pin
- TV: Feb 11 2010

A normal EMV transaction



issuer

merchant

card

customer

result

5. Online transaction authorization (optional)

transaction;
cryptogram

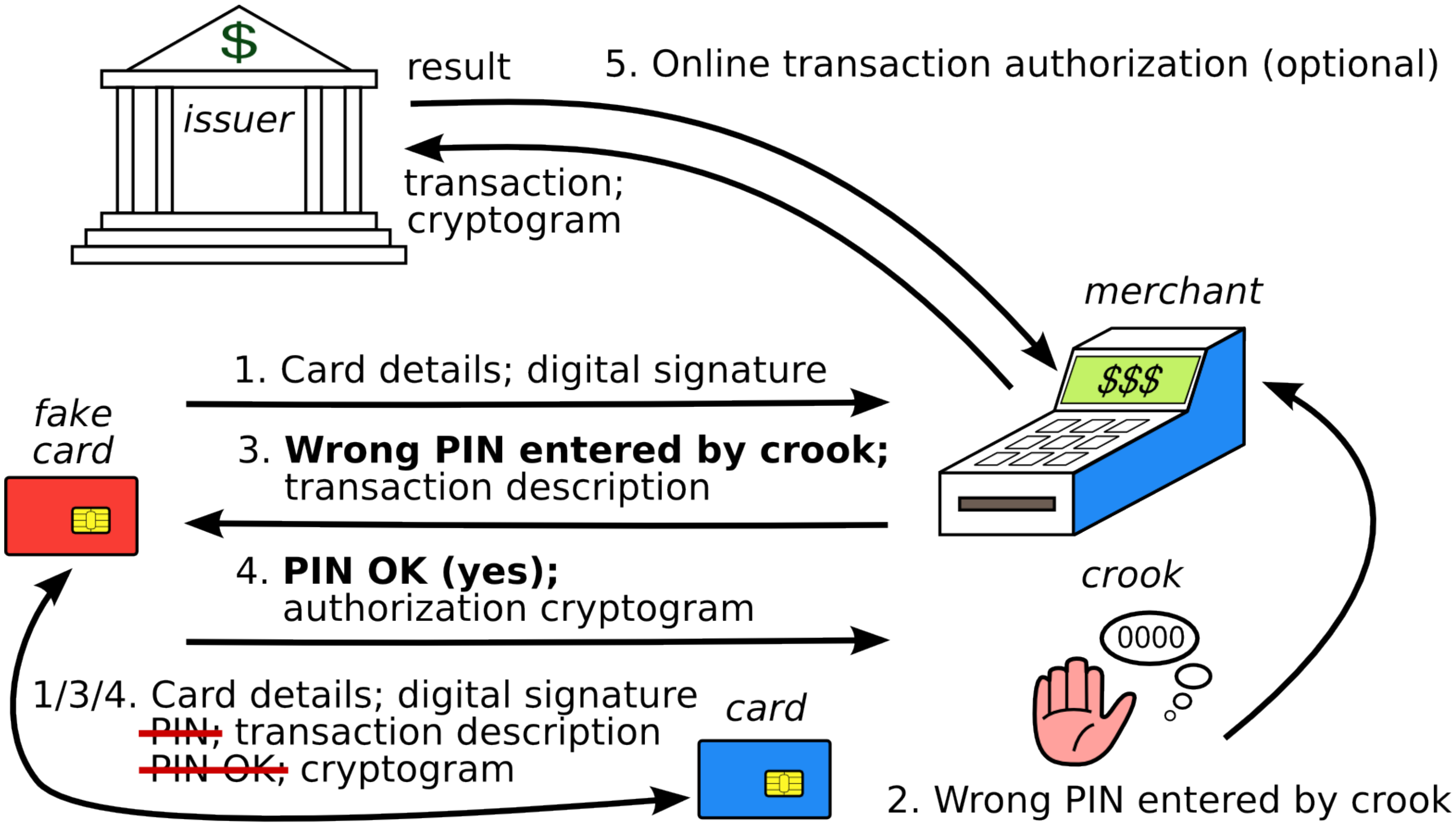
1. Card details; digital signature

3. PIN entered by customer;
transaction description

4. PIN OK (yes/no);
authorization cryptogram

2. PIN entered by customer

A ‘No-PIN’ transaction



issuer
$
result
5. Online transaction authorization (optional)
transaction;
cryptogram
merchant
$$$
1. Card details; digital signature
fake
card
3. **Wrong PIN entered by crook;**
transaction description
4. **PIN OK (yes);**
authorization cryptogram
crook
0000
1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram
card
2. Wrong PIN entered by crook

Blocking the ‘No-PIN’ attack

- In theory: might block at terminal, acquirer, issuer
- In practice: may have to be the issuer (as with terminal tampering, acquirer incentives are poor)
- Barclays blocked it July 2010 until Dec 2010
- Real problem: EMV spec vastly too complex
- With 100+ vendors, 20,000 banks, millions of merchants … a tragedy of the commons!
- Later bank reaction: wrote to university PR department asking for Omar Chaudary’s thesis to be taken down from the website
- Currently only HSBC seems to block it in the UK!

EMV and Random Numbers

- In EMV, the terminal sends a random number N to the card along with the date d and the amount X
- The card computes an authentication request cryptogram (ARQC) on N, d, X
- What happens if I can predict N for d?
- Answer: if I have access to your card I can precompute an ARQC for amount X, date d

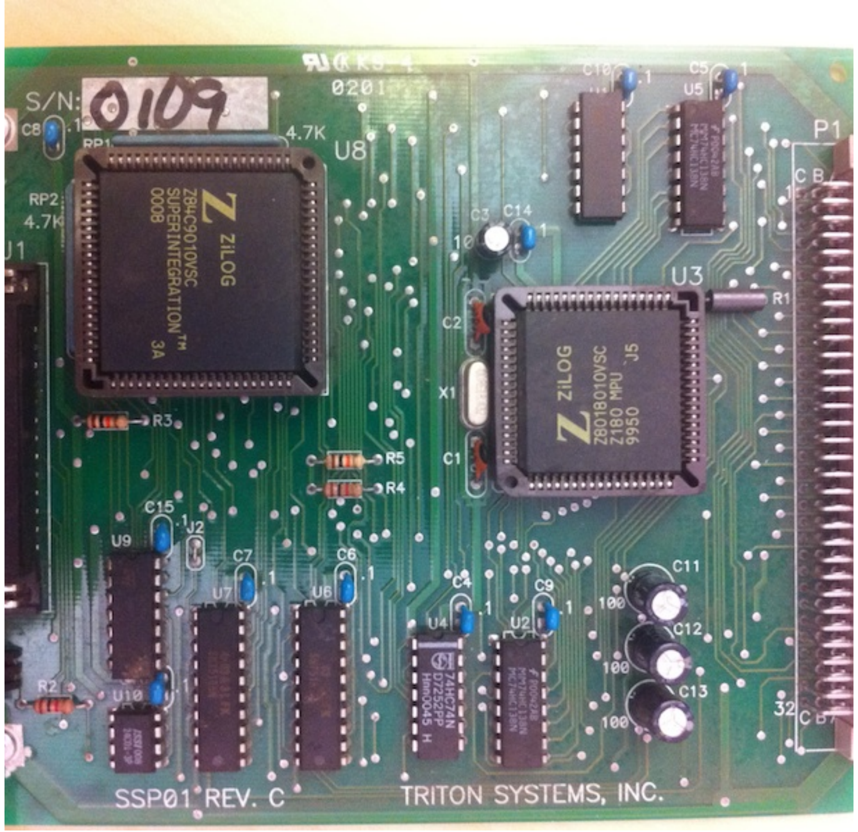
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

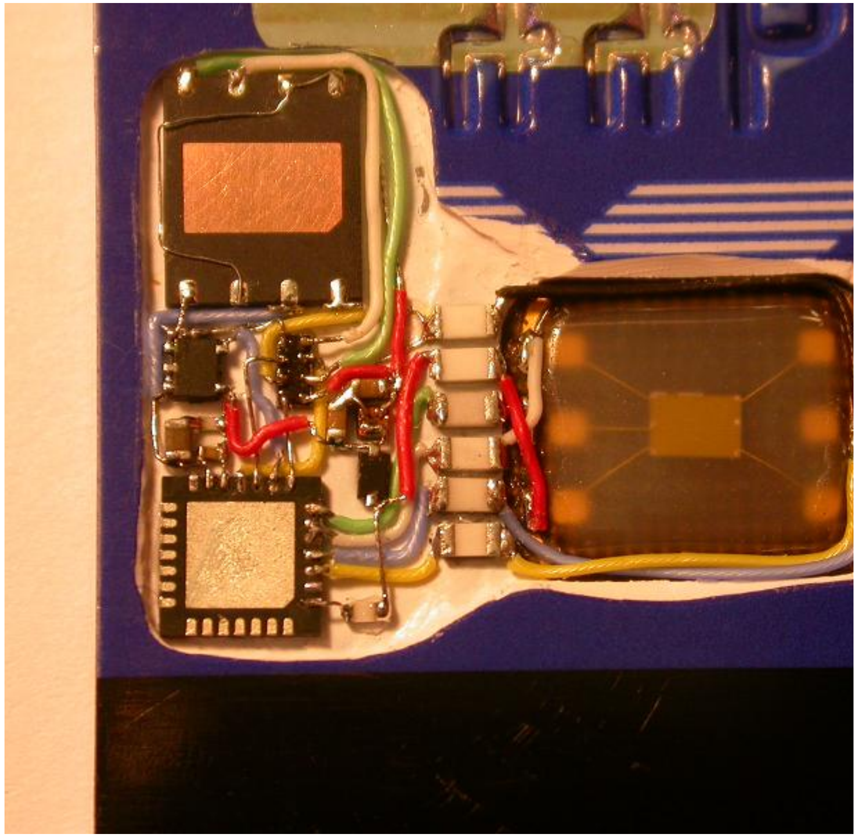
```
2011-06-28          10:37:24          F1246E04
2011-06-28          10:37:59          F1241354
2011-06-28          10:38:34          F1244328
2011-06-28          10:39:08          F1247348
```

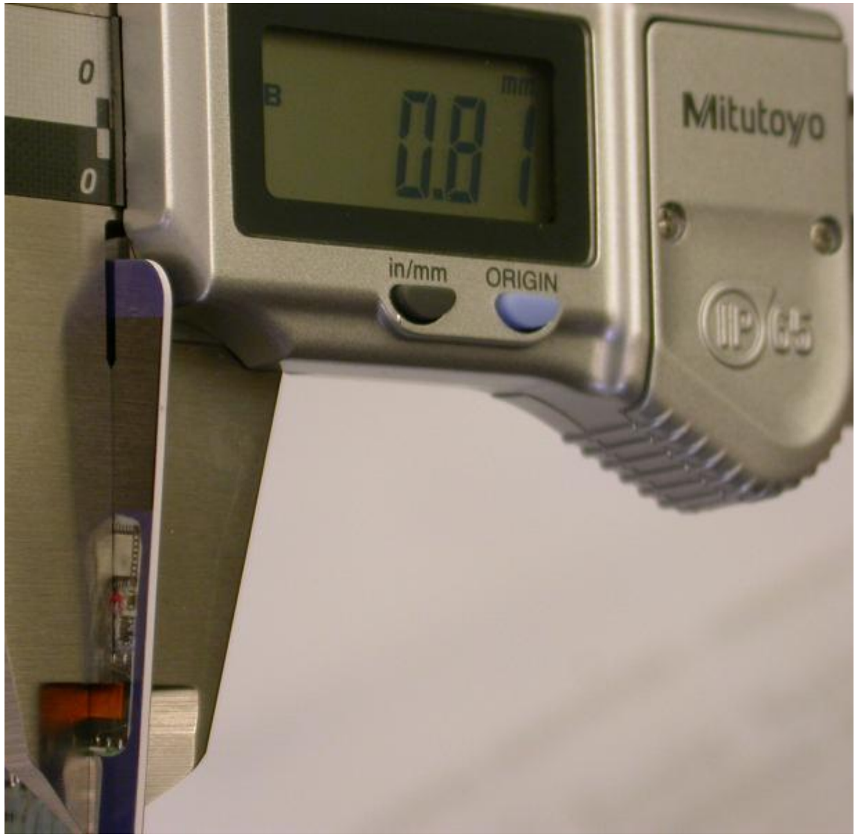
- N is a 17 bit constant followed by a 15 bit counter cycling every 3 minutes
- We test, & find half of ATMs use counters!

ATMs and Random Numbers (3)



ATMs and Random Numbers (4)

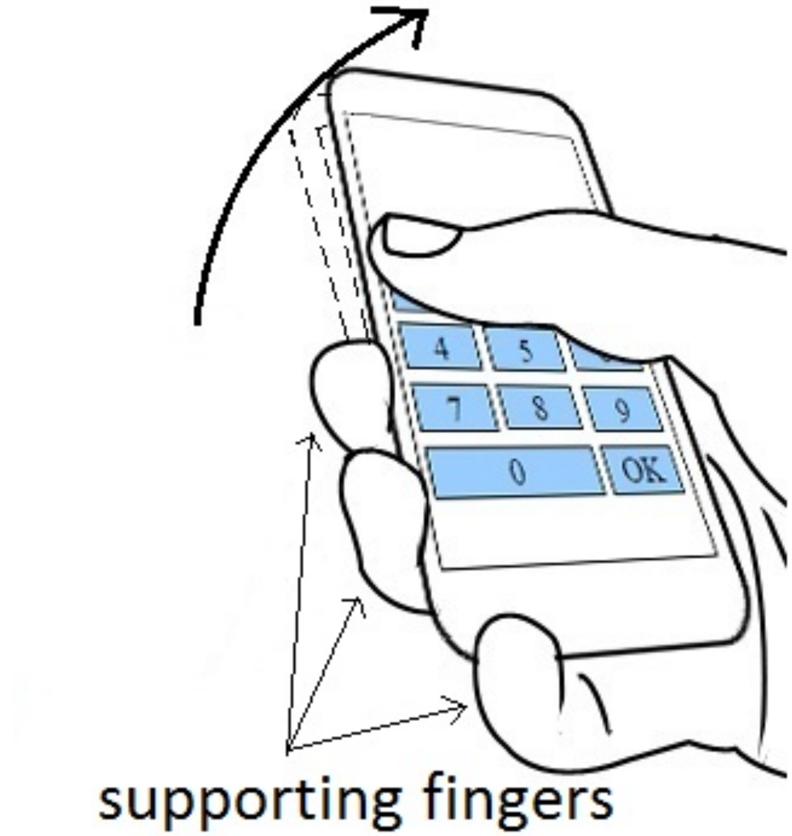




The preplay attack

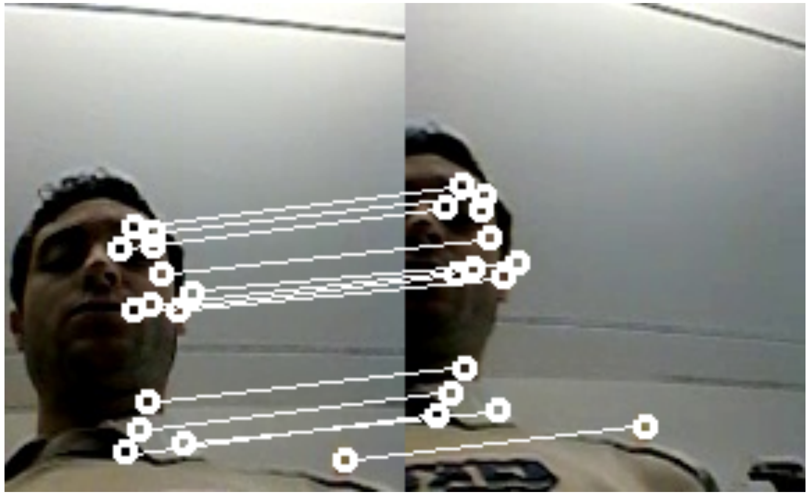
- Collect ARQCs from a target card
- Use them in a wicked terminal at a collusive merchant, which fixes up nonces to match
- Paper at IEEE S&P 2014
- Since then, we won a key case…
- Sailor spent €33 on a drink in a Spanish bar. He got hit with ten transactions for €3300, an hour apart, from one terminal, through three different acquirers, with ATC collisions

Mobile phone PIN stealing



- Is there a side channel from a trusted OS (Knox, TrustZone) that can leak bank PINs?
- Previous work: can use accelerometer, gyro

Mobile phone PIN stealing (2)



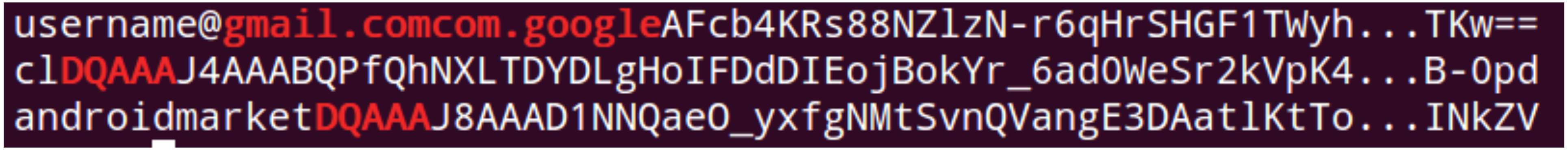
- In “PIN Skimmer” Laurent Simon and I showed the video camera works too
- Also the still camera in burst mode (which works in background)

Latest: attacks on factory reset

- More and more phones sold second-hand
- When you buy a phone, you want to make sure there's no malware
- When you sell a phone, you want to sanitize all your personal data
- Resellers' contracts make you liable for this!
- So: it's important that factory reset works
- Does it?

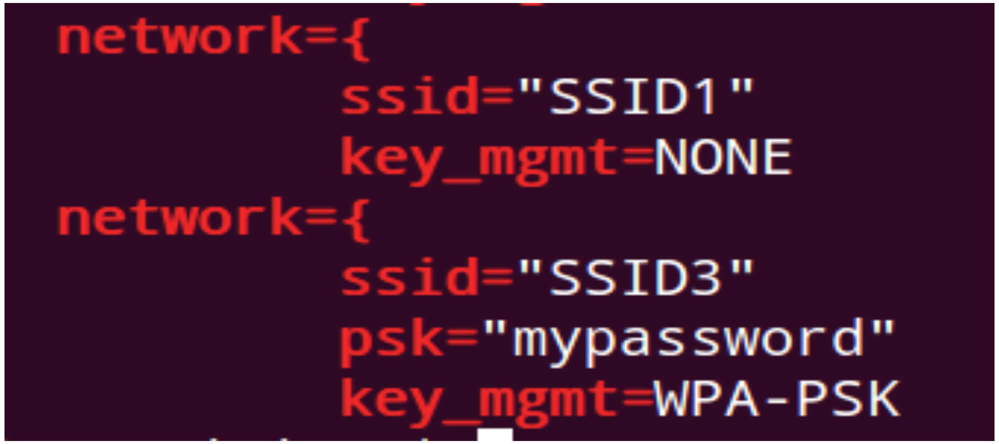
Attacks on factory reset (2)

- We bought 23 Android phones from eBay etc
- In most cases, got the Google master cookie



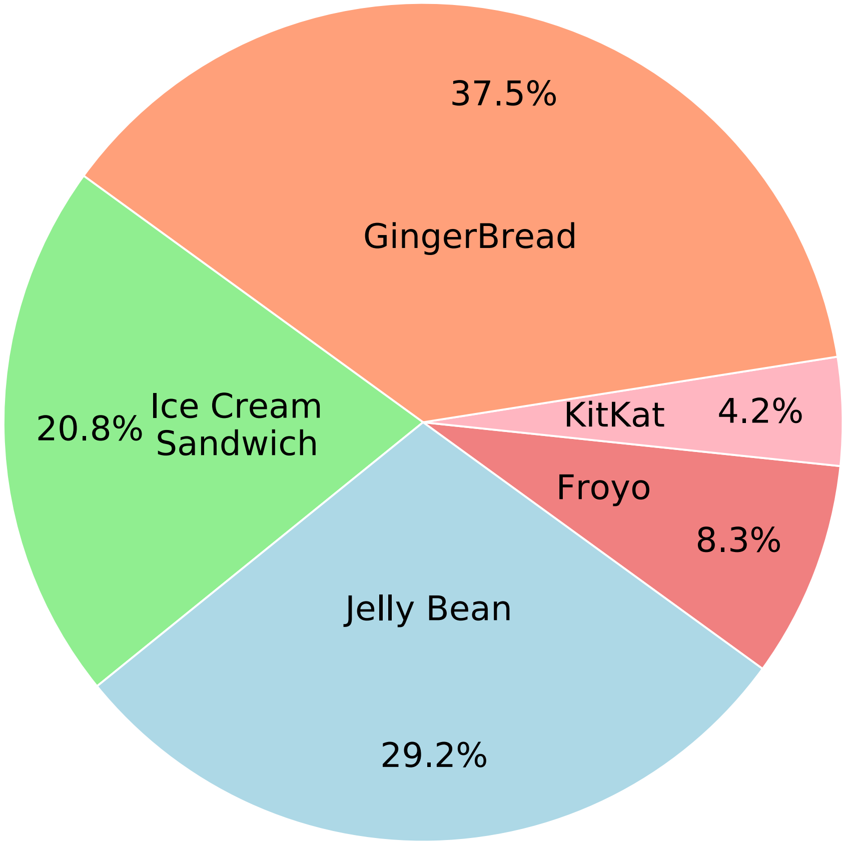
```
username@gmail.comcom.googleAFcb4KRs88NZlzN-r6qHrSHGF1TWyh...TKw==
clDQAAAJ4AAABQPfQhNXLTDYDLgHoIFDdDIEojBokYr_6ad0WeSr2kVpK4...B-0pd
androidmarketDQAAAJ8AAAD1NNQae0_yxfgNMtSvnQVangE3DAatlKtTo...INkZV
```

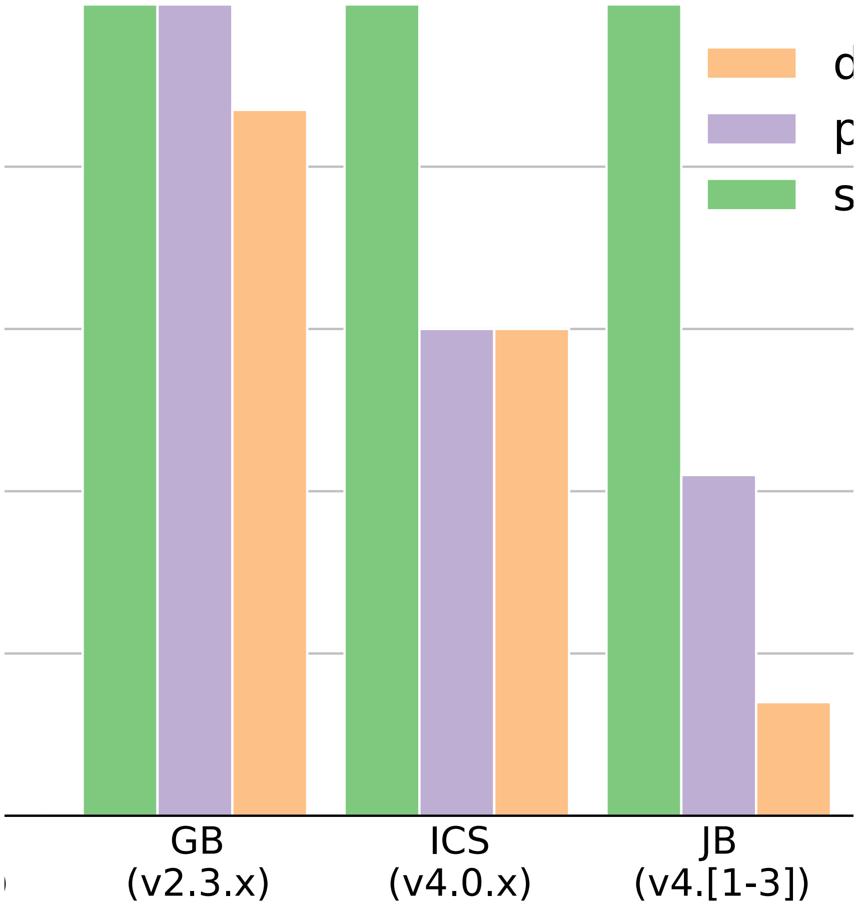
- It’s also easy to spot personal data, credentials



```
network={
        ssid="SSID1"
        key_mgmt=NONE
network={
        ssid="SSID3"
        psk="mypassword"
        key_mgmt=WPA-PSK
```

340 million vulnerable phones!

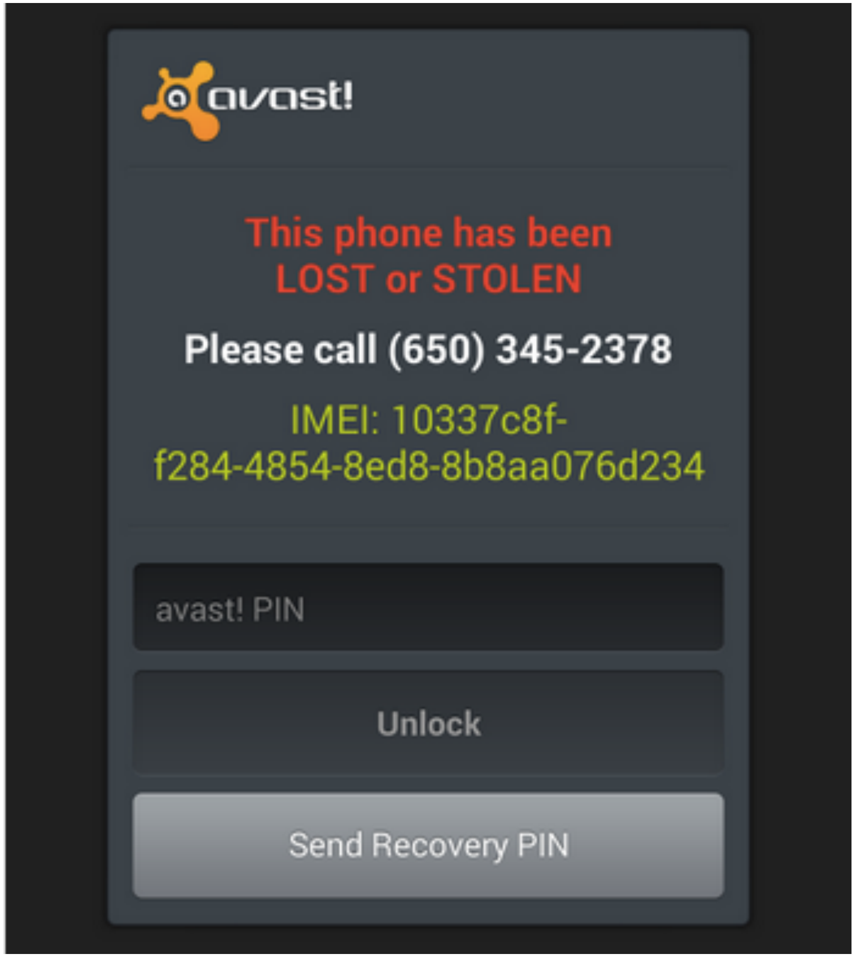




Attacks on factory reset (3)

- Technical details: mostly screw-ups by OEMs
- The memory hierarchy is complex!
- If a user, encrypt your phone (at least)
- If an implementer, read our papers
- If a reseller, watch for crooked staff!
- That is where this attack might most easily scale, now there are markets for credentials

Attacks on Remote Wipe



This phone has been LOST or STOLEN

Please call (650) 345-2378

IMEI: 10337c8f-f284-4854-8ed8-8b8aa076d234

- Remote wipe was even worse!
- We tested the top 10 mobile AV products
- They inherited the factory reset attacks, plus more too
- Again, many details: see the paper

Attack scale

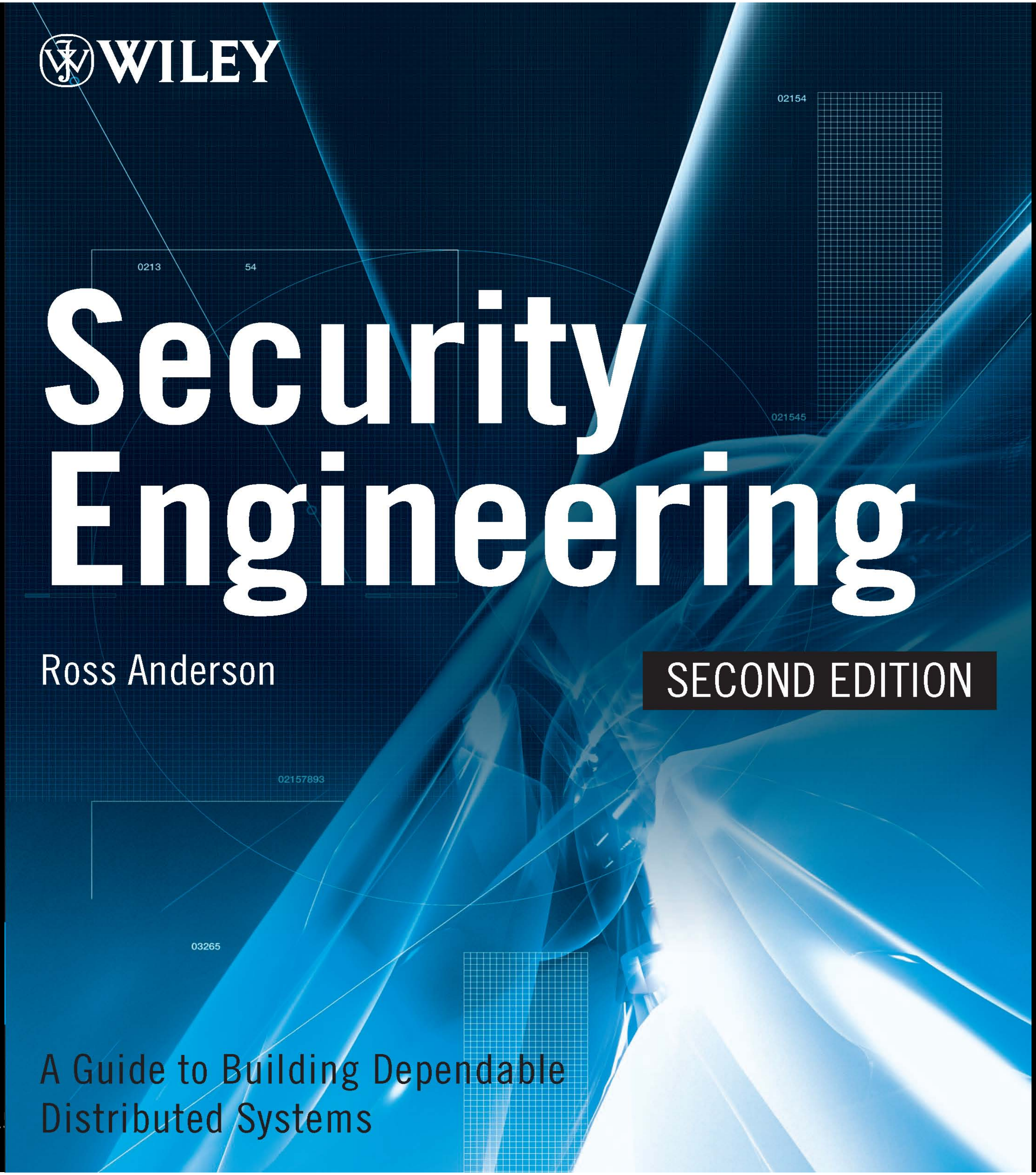
- Small: a specialist team can demonstrate it to a TV journalist
- Medium: a gang of crooks can take a few million before they get caught
- Large: scales to nine / ten figures and forces industry action
- Most of the discussed attacks are 'medium'
- Paul Kocher's effect was 'large'!

Conclusion

- In 1993 “Why cryptosystems fail”: many ATM frauds down to poor implementation, ops
- Two technology cycles since: EMV in 2003, and mobile payments now
- Systems are more complicated, which means more ways to screw up
- They are also more global, so more firms can screw up, and more governance issues
- Issues spreading to many related applications

More …

- MOST next month (at S&P) for factory reset, AV
- Our 2014 IEEE S & P paper on the preplay attack
- Our 2012 IEEE S & P paper on the no-PIN attack
- See www.lightbluetouchpaper.org for our blog
- And http://www.cl.cam.ac.uk/~rja14/banksec.html
- Workshop on Economics and Information Security (WEIS): next edition in the Netherlands, June 2015
- My book 'Security Engineering – A Guide to Building Dependable Distributed Systems'



WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems