How Smartcard Payment Systems Fail

Ross Anderson

Cambridge

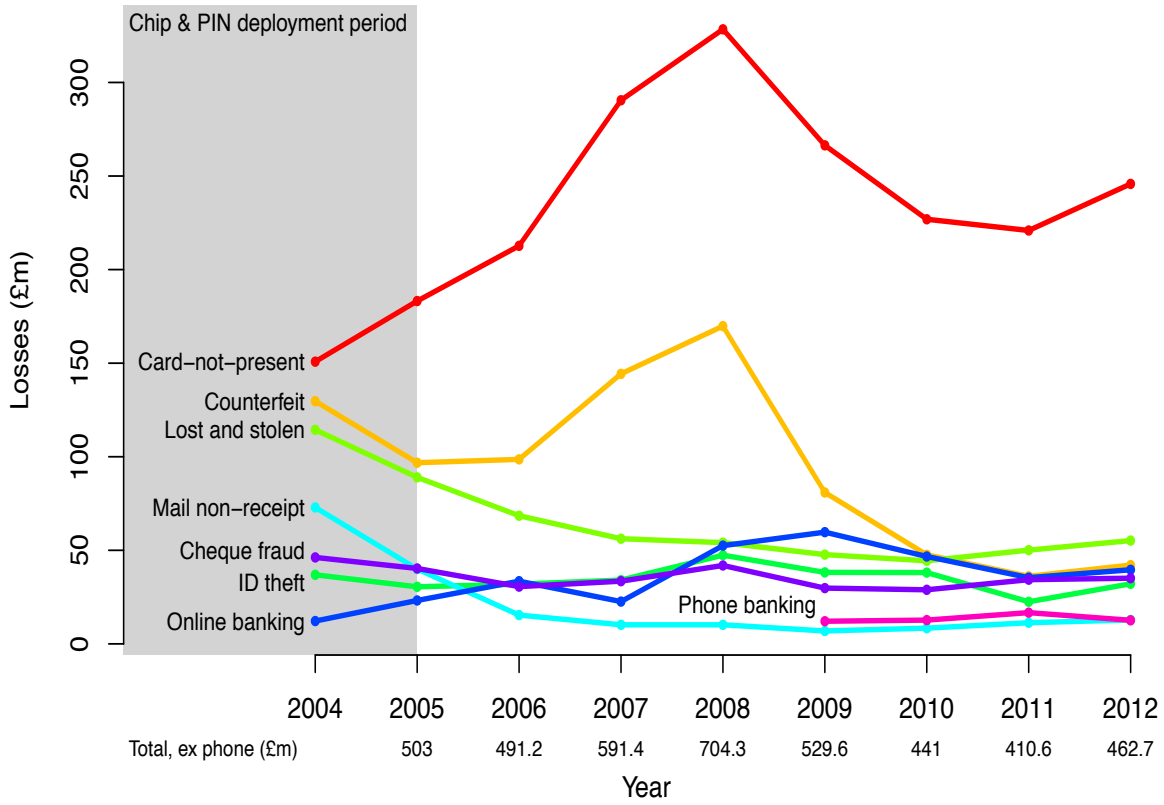
The EMV protocol suite

- 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

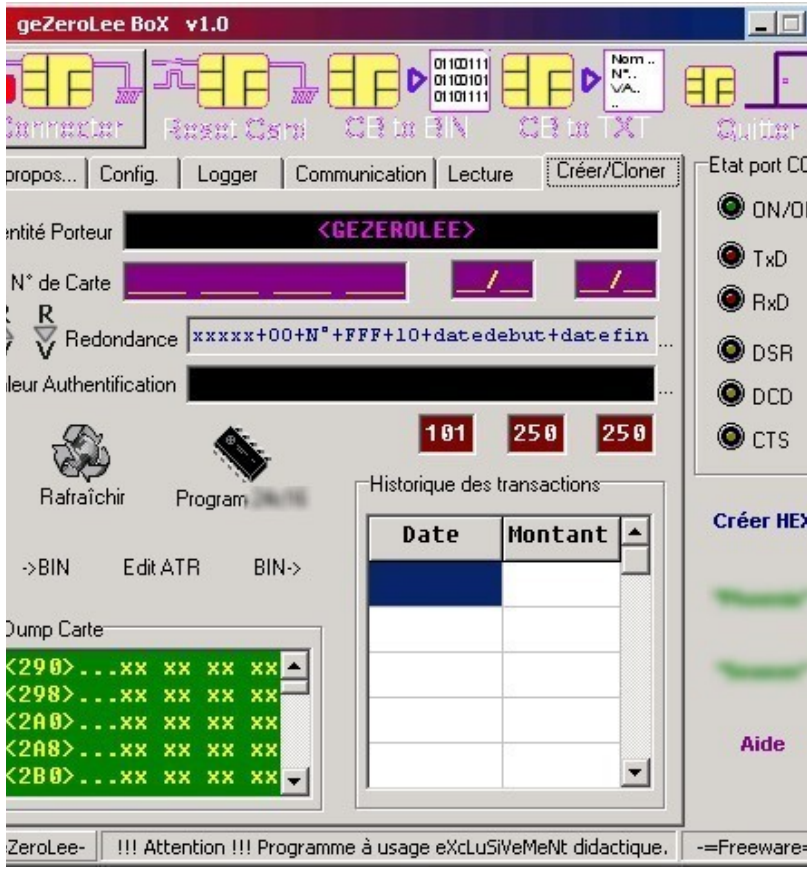
EMV shifted the landscape…

- 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

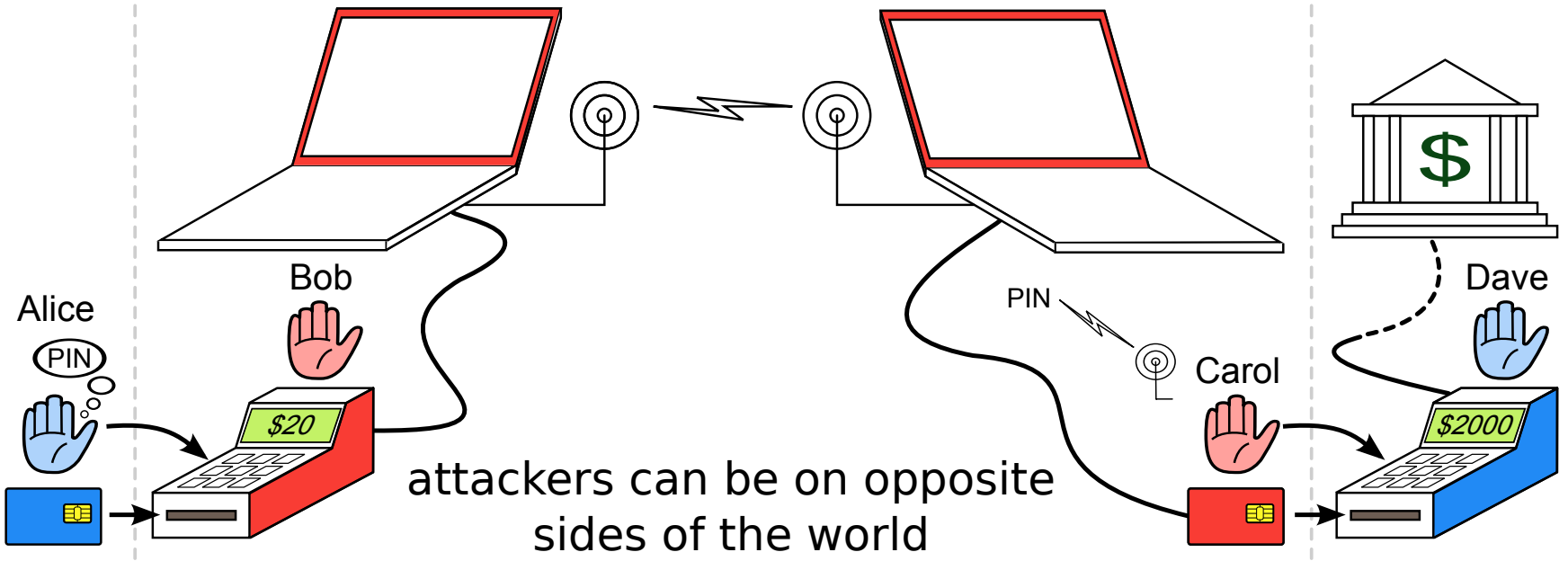


- Cheap cards are SDA (no public key capability, so static certificate)
- A ‘yes card’ can impersonate in an offline terminal
- Fairly easy to do, but not seen much

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)



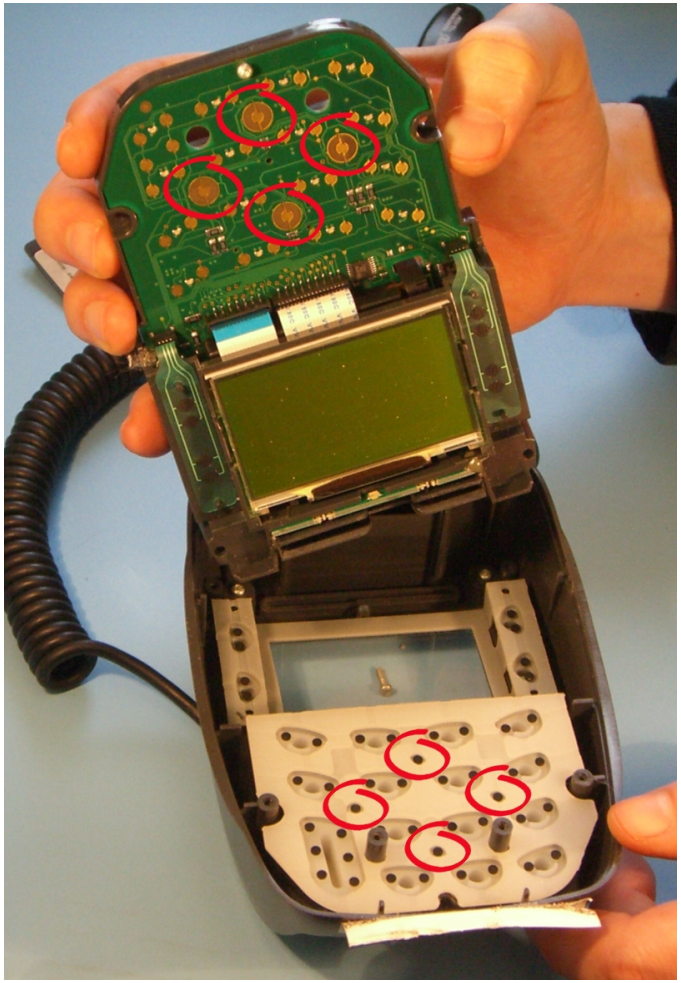
Attacks in the real world

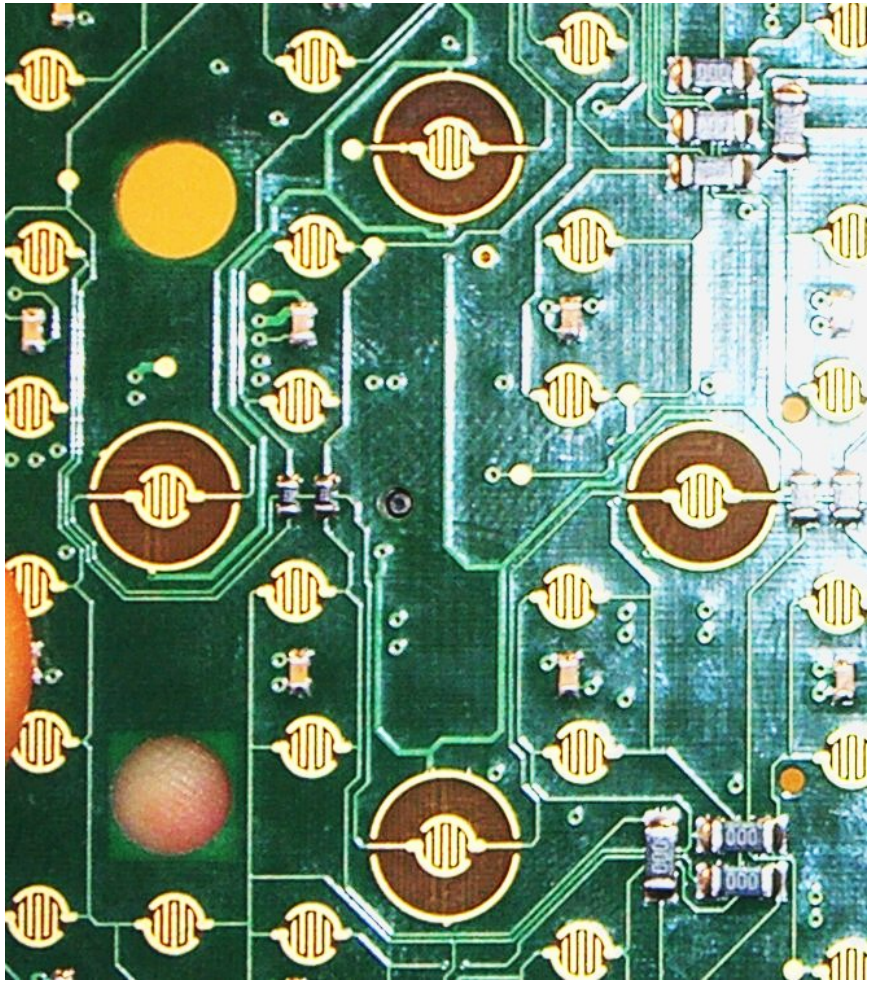
- The relay attack is almost unstoppable, and we showed it in TV in February 2007
- But it seems never to have happened!
- So far, mag-strip fallback fraud has been easy
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier was blamed)
- Then ‘Tamil Tigers’
- After fraud at BP Girton: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

Tamper-proofing of the PED

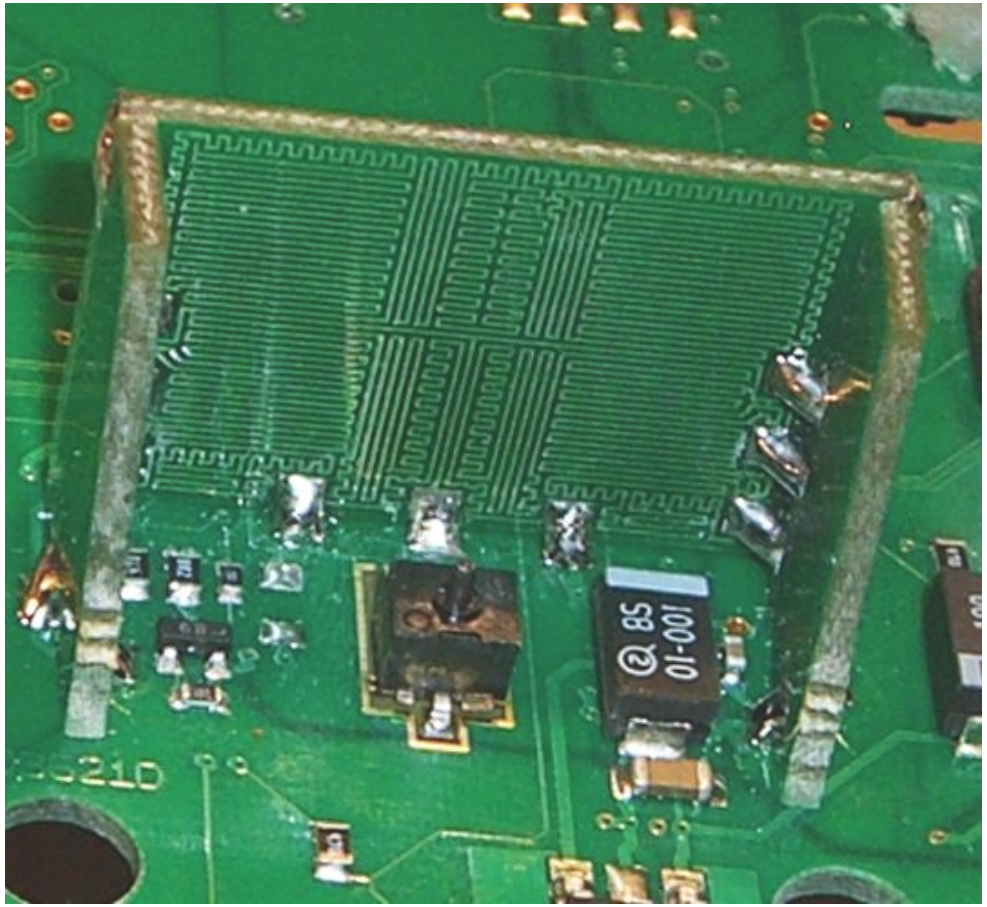
- In EMV, PIN sent from PIN Entry Device (PED) to card
- Card data flow the other way
- PED supposed to be tamper resistant according to VISA, APACS (UK banks), PCI
- 'Evaluated under Common Criteria'
- Should cost $25,000 per PED to defeat

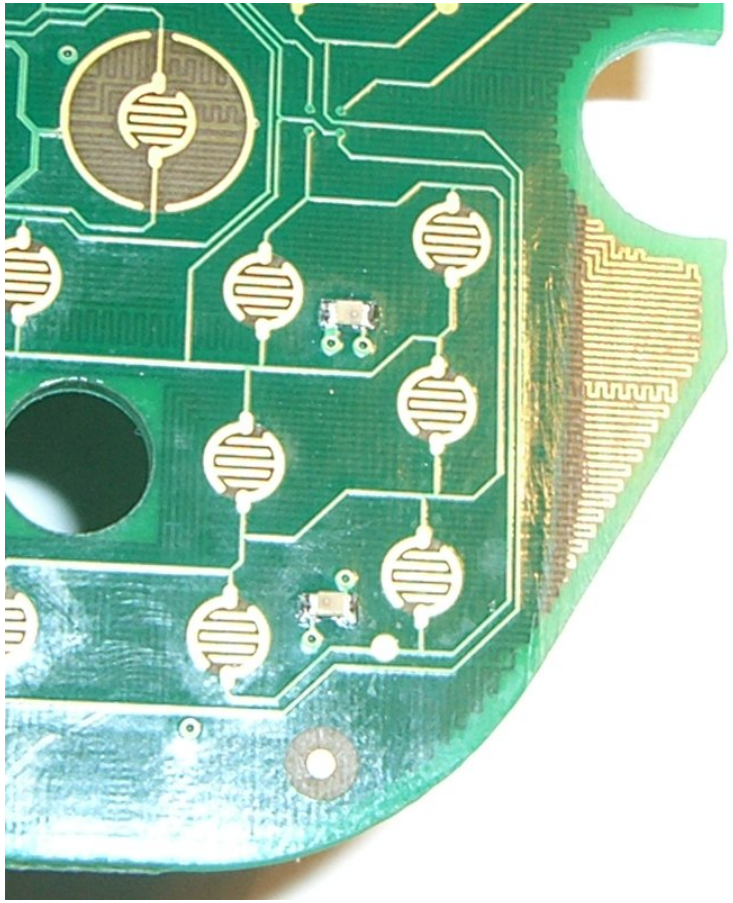
Tamper switches (Ingenico i3300)





… and tamper meshes too





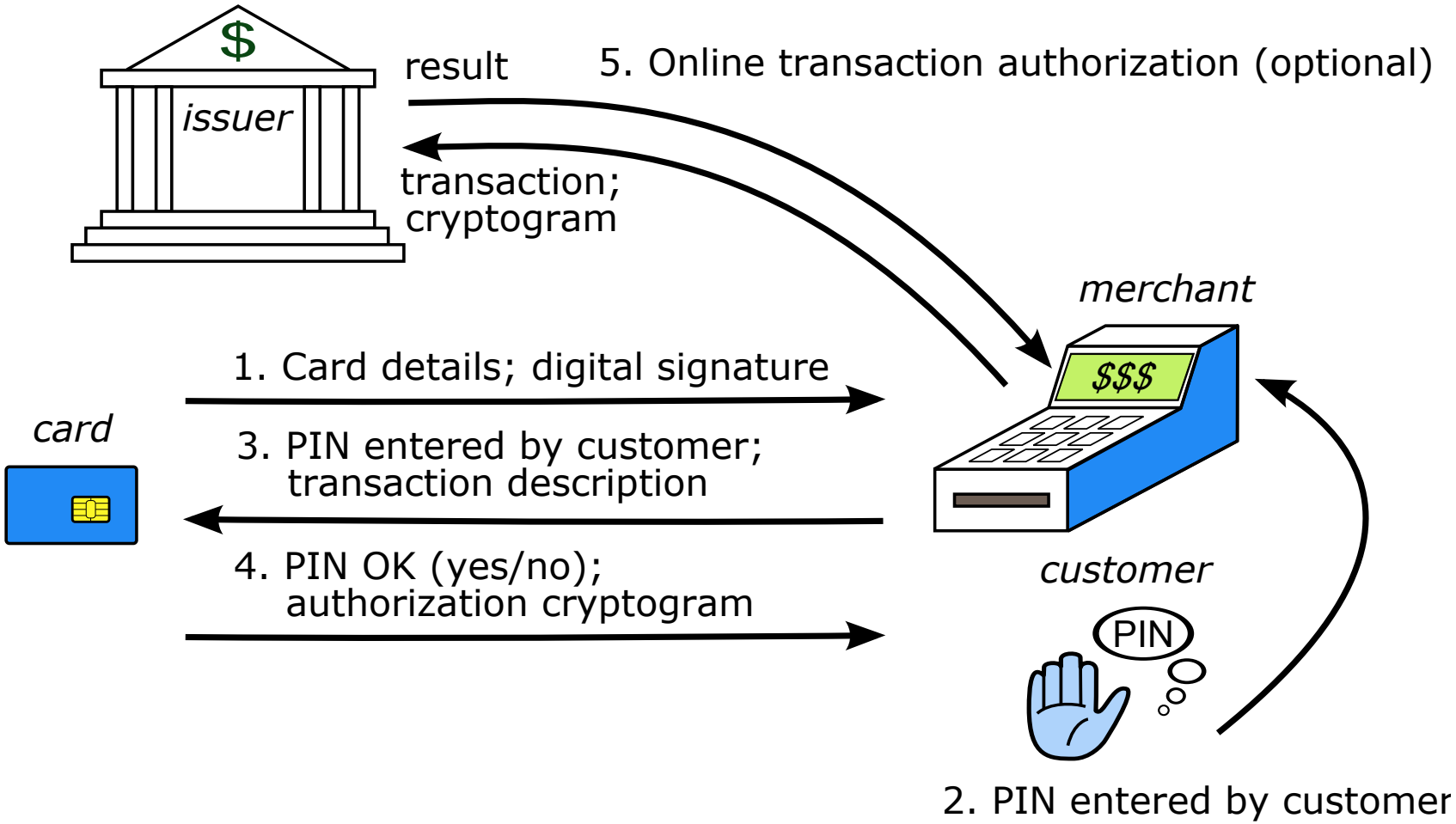
TV demo: Feb 26 2008

- 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)

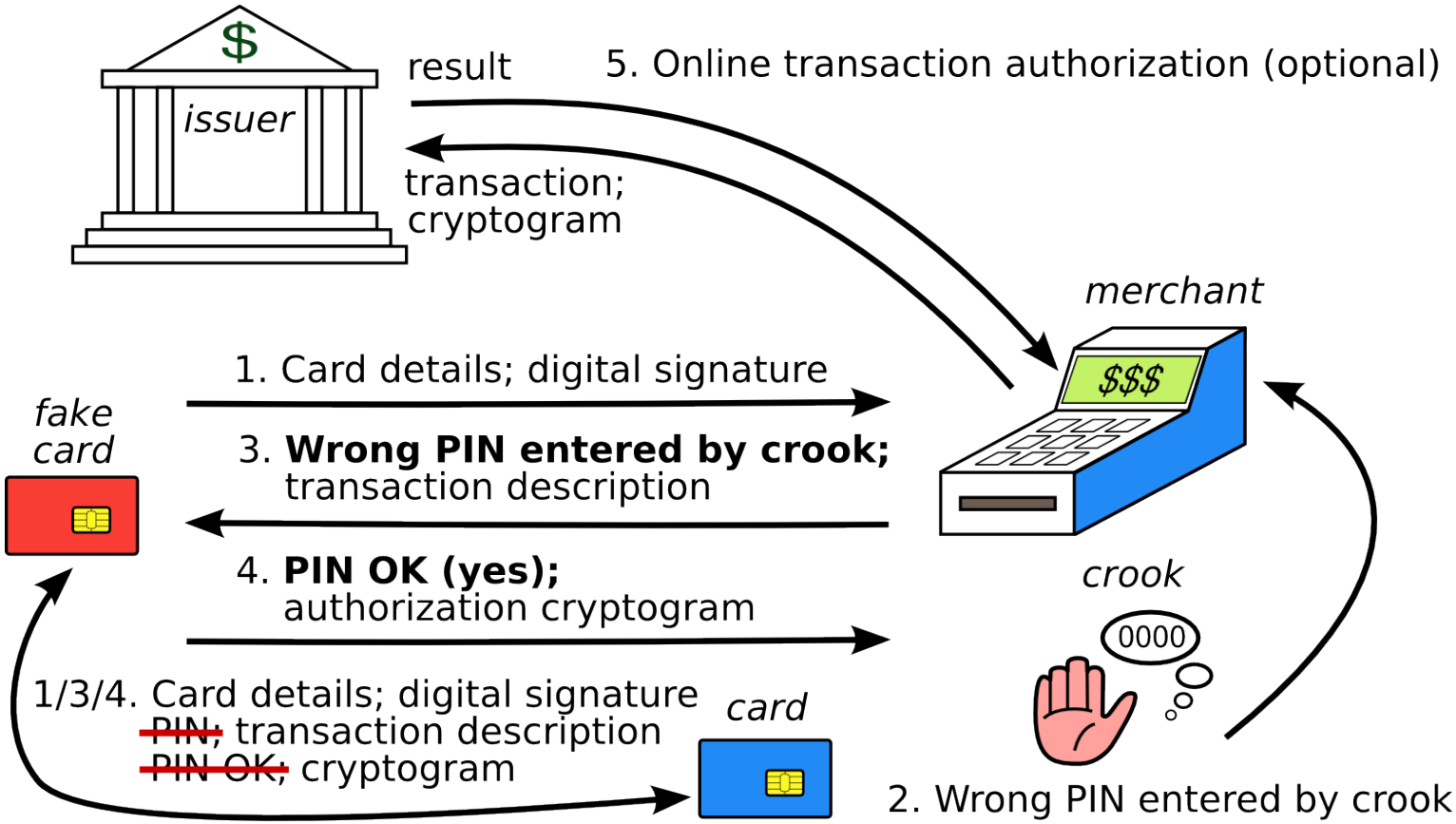
The ‘No-PIN’ attack

- 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



A ‘No-PIN’ transaction



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!

Card Authentication Protocol

- Lets banks use EMV in online banking
- Users compute codes for access, authorisation
- A good design would take PIN and challenge / data, encrypt to get response
- But the UK one first tells you if the PIN is correct
- This puts your personal safety at risk …

Crime victims tortured for PINs

guardian.co.uk

Police think French pair tortured for pin details

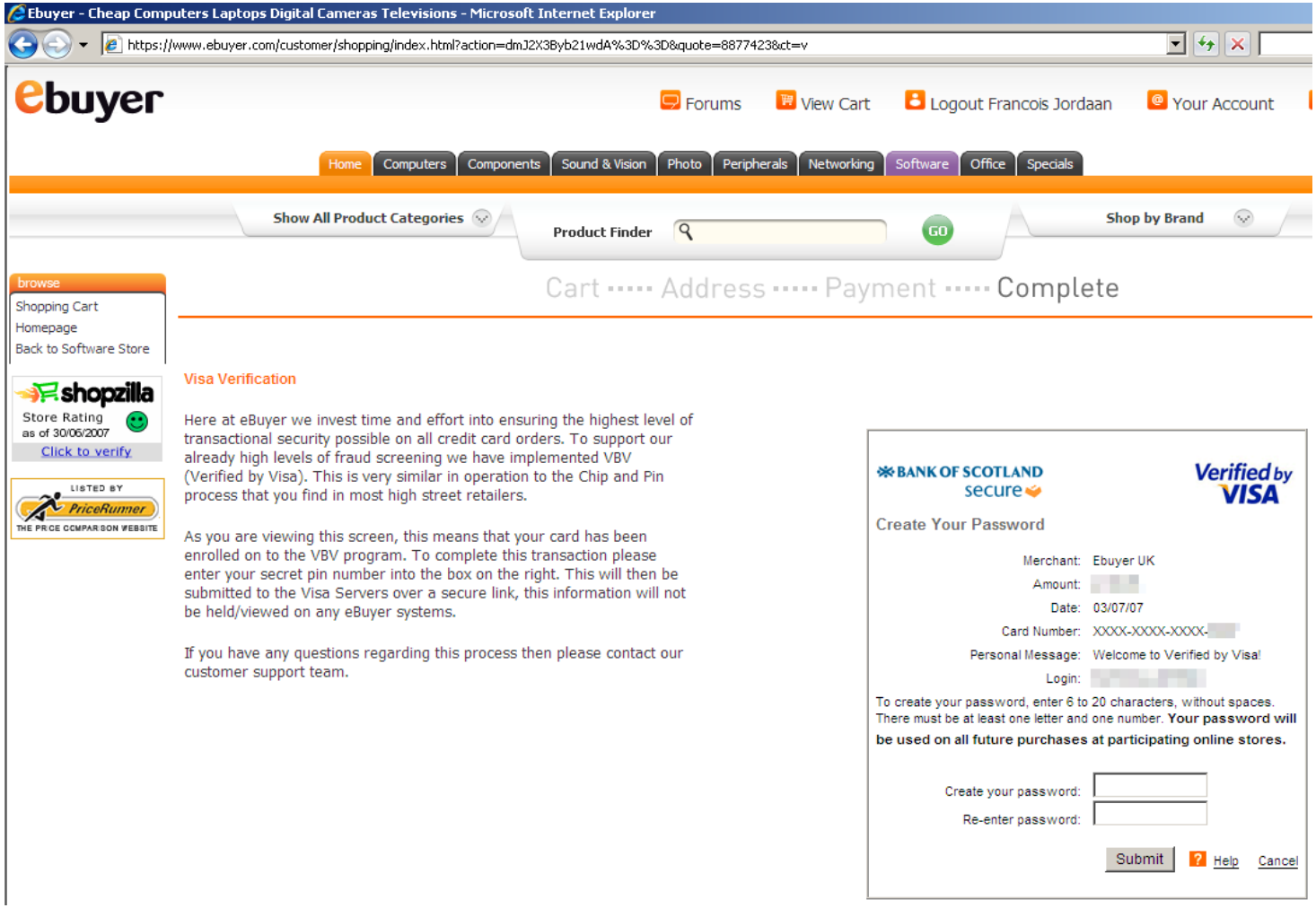
Matthew Taylor
The Guardian, Saturday July 5 2008


Laurent Bonomo and Gabriel Ferez, two French exchange students who were killed in London. Photographs: Met police/Getty

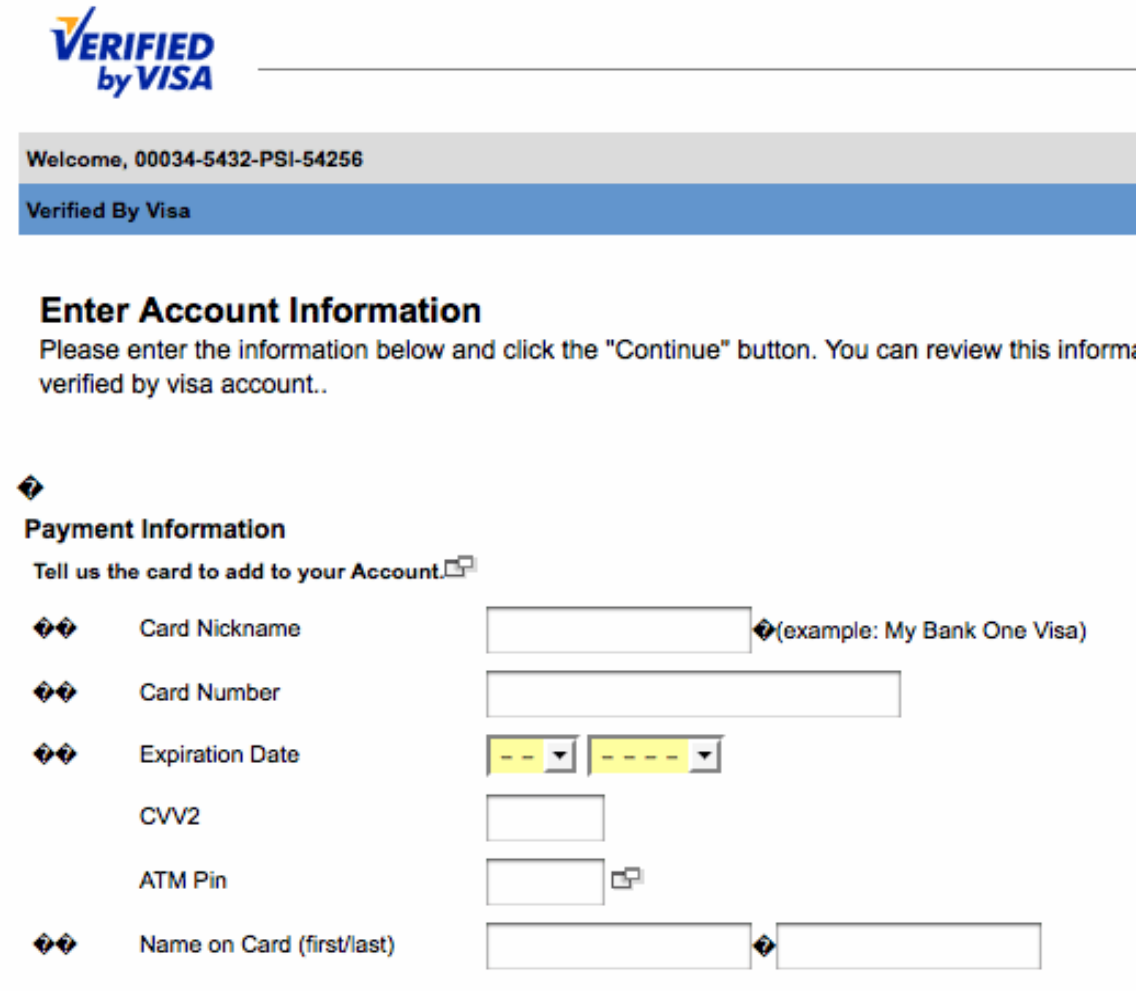
The two French students who were bound up and brutally murdered at a bedsit in south London may have been tortured for their bank and credit card pin numbers, police said yesterday.

Laurent Bonomo and Gabriel Ferez, both 23, were found at Bonomo's flat in New Cross, south London, on Sunday night. They had been stabbed more than 200 times, bound, gagged, and tortured over several hours.

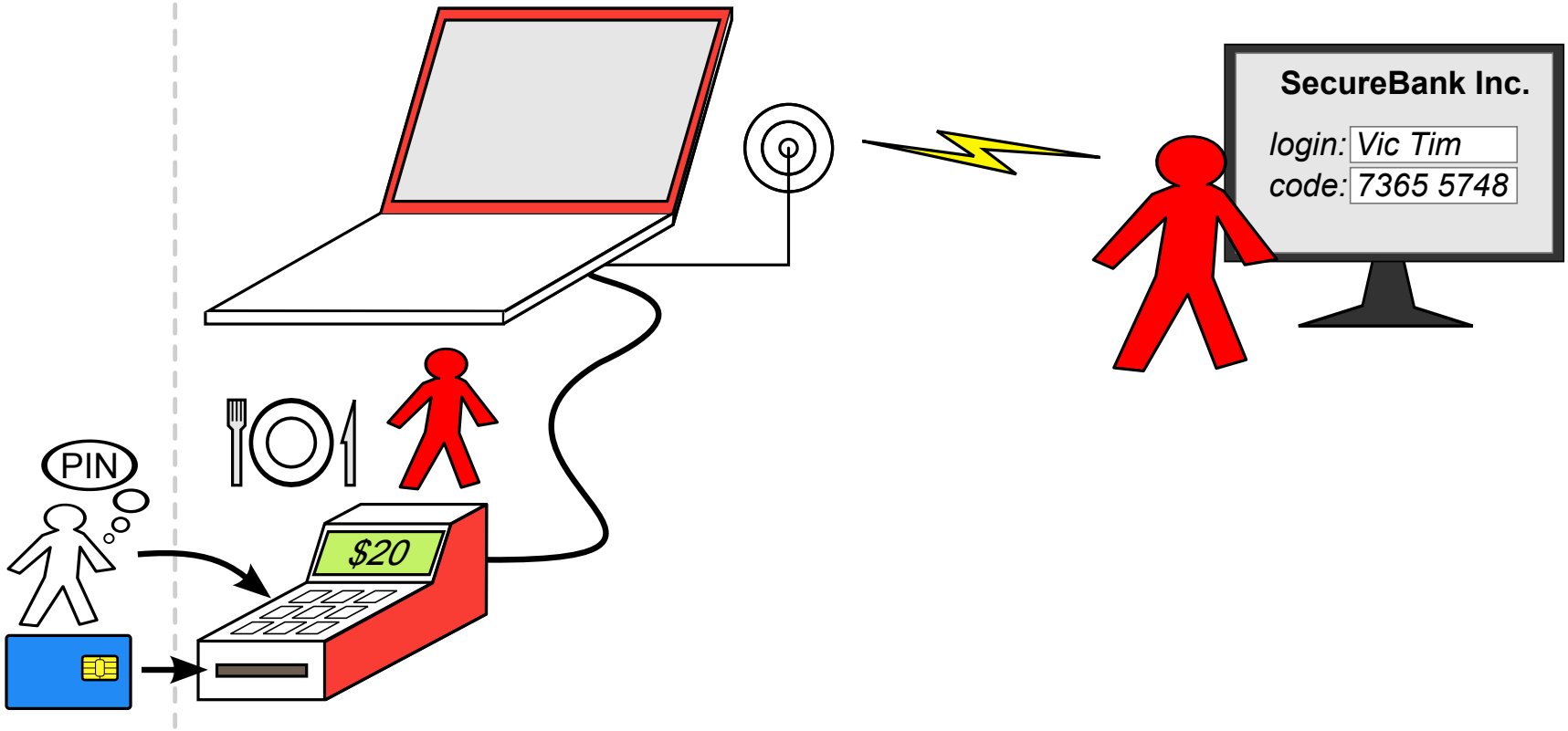
Phishing attacks?



Less suspicious than this …



CAP attacks through wicked shops



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

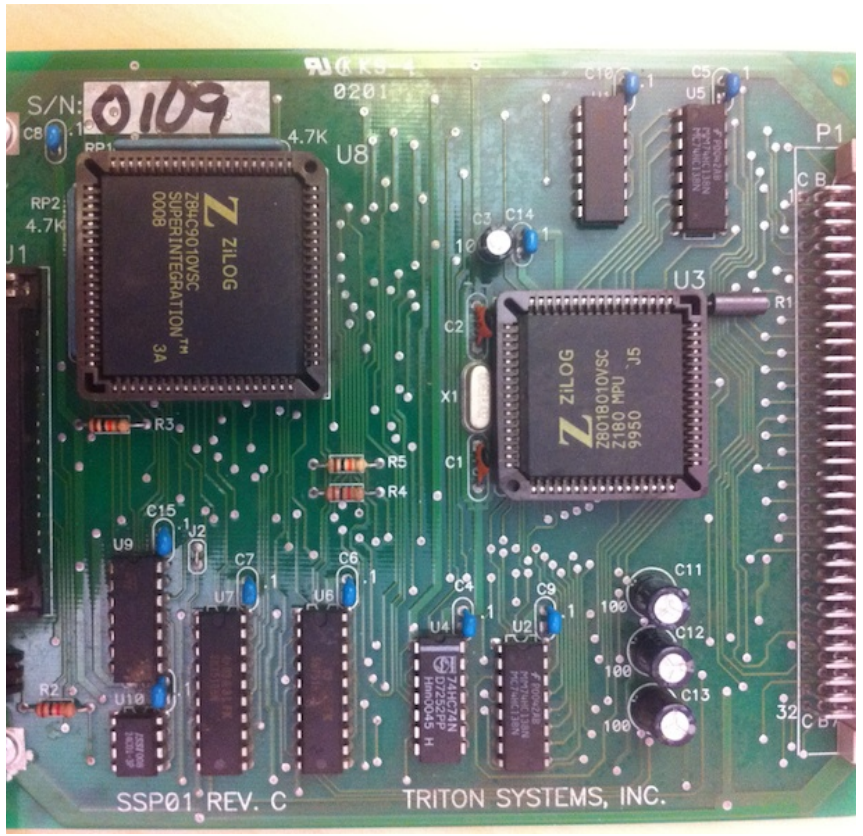
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

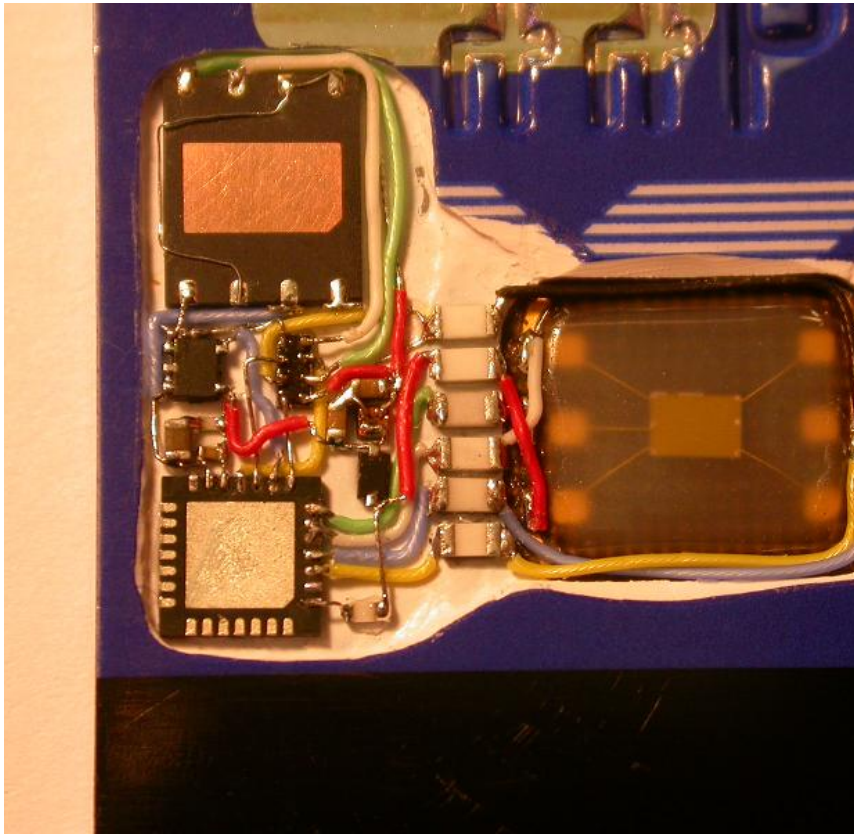
2011-06-28	10:37:24	F1246E04
2011-06-28	10:37:59	F1241354
2011-06-28	10:38:34	F1244328
2011-06-28	10:39:08	F1247348

- 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 accepted at Oakland this year
- Since then, we have a live case…
- Sailor spent €33 on a drink in a Spanish bar. He got hit with six transactions for €3300, an hour apart, from one terminal, through three different acquirers, with ATC collisions

Back end failures too …

- Interesting case in R v Parsons, Manchester crown court, 2013
- Authorisation and settlement are different systems with different transaction flows
- Authorisation reversals not authenticated
- How to take the banks for maybe £7.5m (and the banks only noticed £2.5m of it …)
- Parsons now a fugitive from justice

In the UK we have no Reg E, and no breach reporting laws…

Skimming device found at Tesco

POLICE arrested two people in connection with a bank card skimming scheme.

They have been released on police bail.

The pair were arrested on Tuesday morning following the discovery of a skimming device attached to an ATM situated at Tesco's in Coniston Road, Flitwick.

Officers arrived at 11.30am and confiscated the device and other equipment associated with the copying of bankcard information.

The two were held custody and detectives requested an extension to question the pair.

Detective Sergeant Dennis Simpson of the Economic Crime Unit is urging members of the public who used this machine between 10.30am and 11.30am on Tuesday morning to check their accounts and report any unauthorised transactions to him as soon as possible.

DS Simpson is also appealing for anyone who witnessed people tampering with this machine, or anyone who noticed anyone acting suspiciously in the car park of the store on Tuesday morning to come forward and assist with the investigation.

Anyone with information can contact DS Simpson, in confidence, on 01582 394014, or Crimestoppers, anonymously, on 0800 555 111.

Open :- Mon-Fri 9am to 5pm, Sat 10am to 2pm.

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’
- ‘Large’ might be contained using analytics

What does EMV hold for the USA?

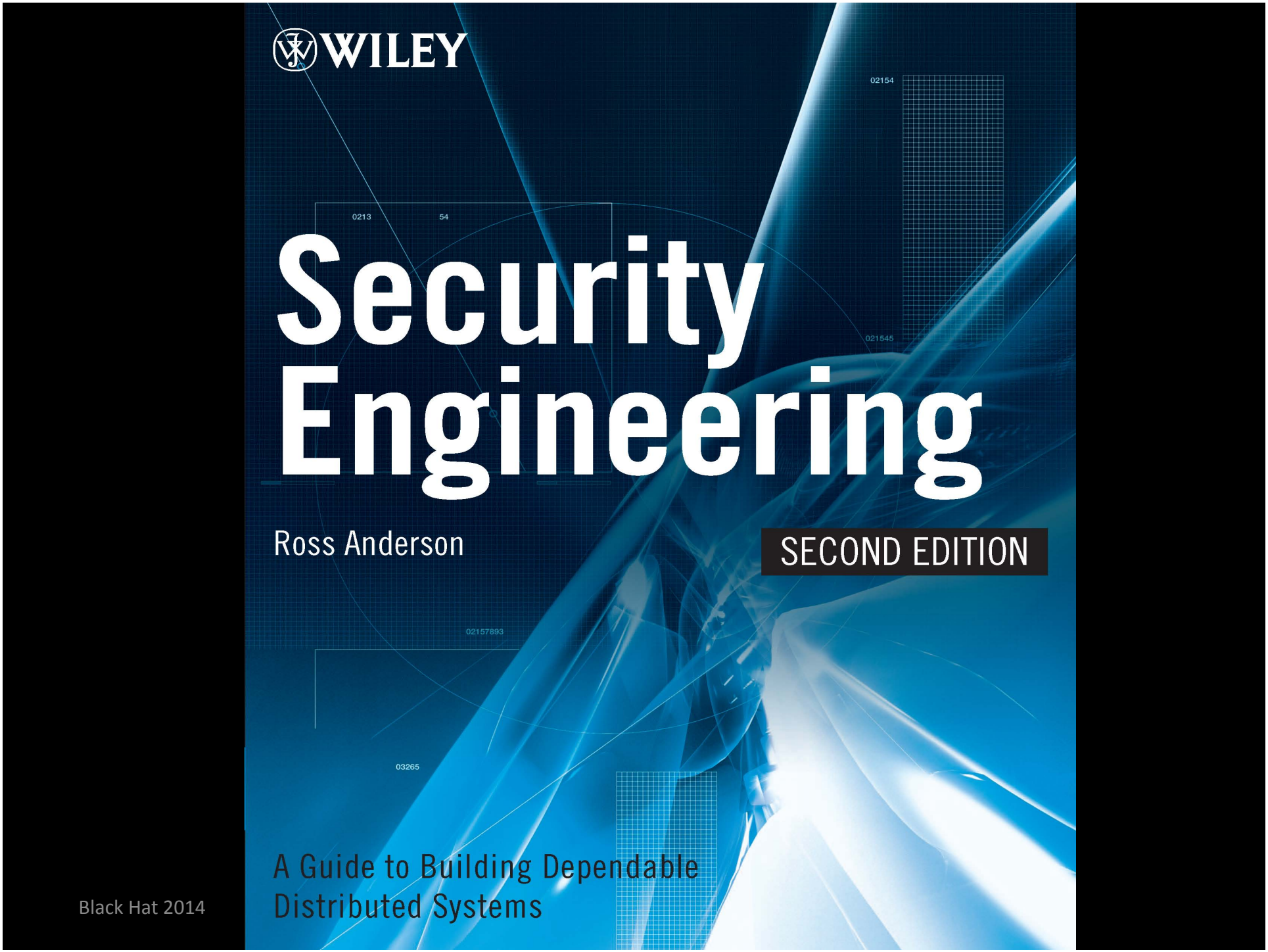
- It looks like the effects of the liability shift will be mitigated by Reg E, Reg Z, & the Fed
- Many banks may use chip-and-signature, as in Singapore
- Consumer protection might still be undermined by payment innovation, e.g. move from credit cards to PIN debit, or phone payments
- EMV with less liability shift will be an interesting natural experiment!

Broader lessons

- Governance at global scale is hard
- EMVCo largely superseded by vendor lobby …
- Featuritis can break anything!
- Issuers, acquirers have different interests (even if departments of the same bank)
- No-one represents the poor consumer
- Key: proper documentation, including breach notification and responsible vulnerability disclosure (NOT the EU NIS Directive!)

More …

- Our 2014 IEEE Security & Privacy paper on the preplay attack
- Our 2012 IEEE Security & Privacy 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'



Black Hat 2014