The Fraud Telescope

Ross Anderson
Cambridge

CCCC Conference, July 14 2016

How do we know what's going on?

- Situational awareness is a big soft spot
- At Cambridge, we have lots of publications online about card fraud and online scams
- So fraud victims search, find us and contact us, especially after secondary victimisation (where the bank said it was all their fault)
- This gives us a valuable perspective on emerging fraud techniques

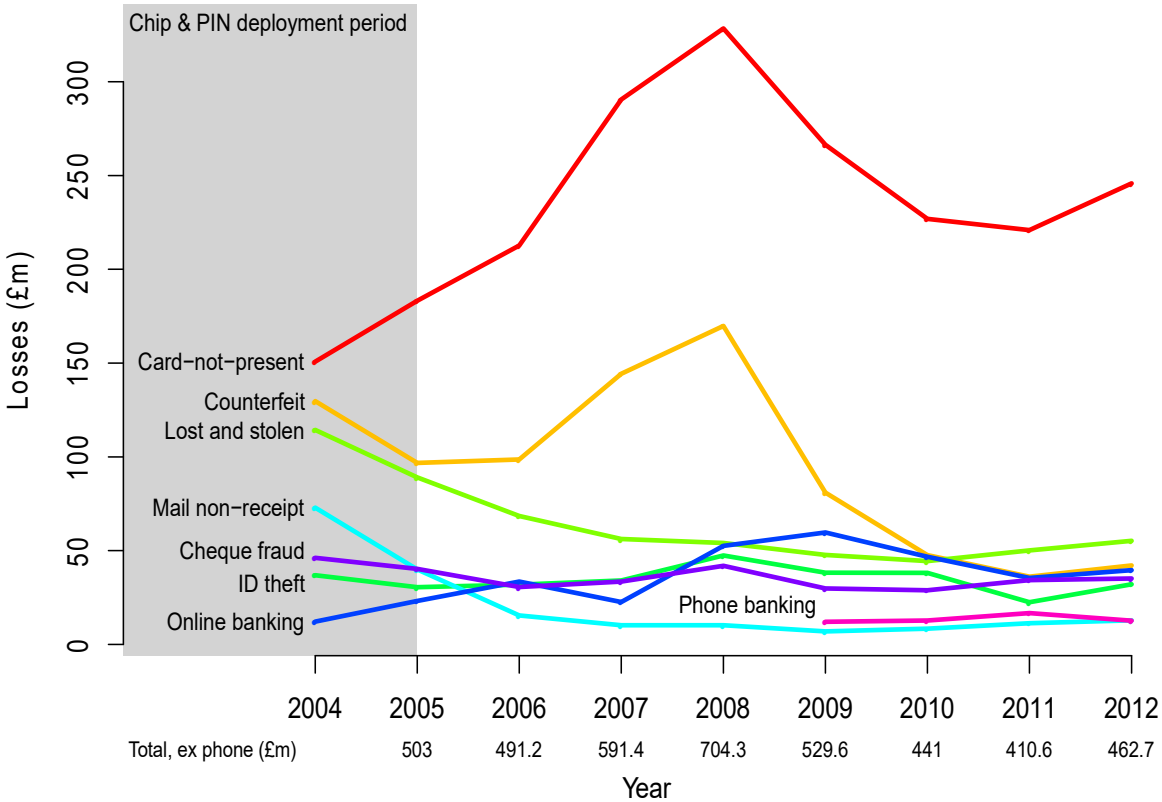
In the land of the blind …

- The British Crime Survey asks 40,000+ people whether they've been a victim of crime each year
- By 2009–10: acquisitive crime about 1 million traditional 'serious' crime (burglaries, car theft…)
- But about 2–3 million other (dodgy auctions, credit card disputes, online banking scams …)
- The second category was excluded from other official statistics from 2007
- This month: NCA finally admits that cyber-crime is most of it

EMV (‘Chip and PIN’)

- Now deployed in Europe and elsewhere
- ‘Liability shift’ – disputes charged to cardholder if pin used, else to merchant
- Changed many things, not always in the ways banks expected…

Fraud history, UK

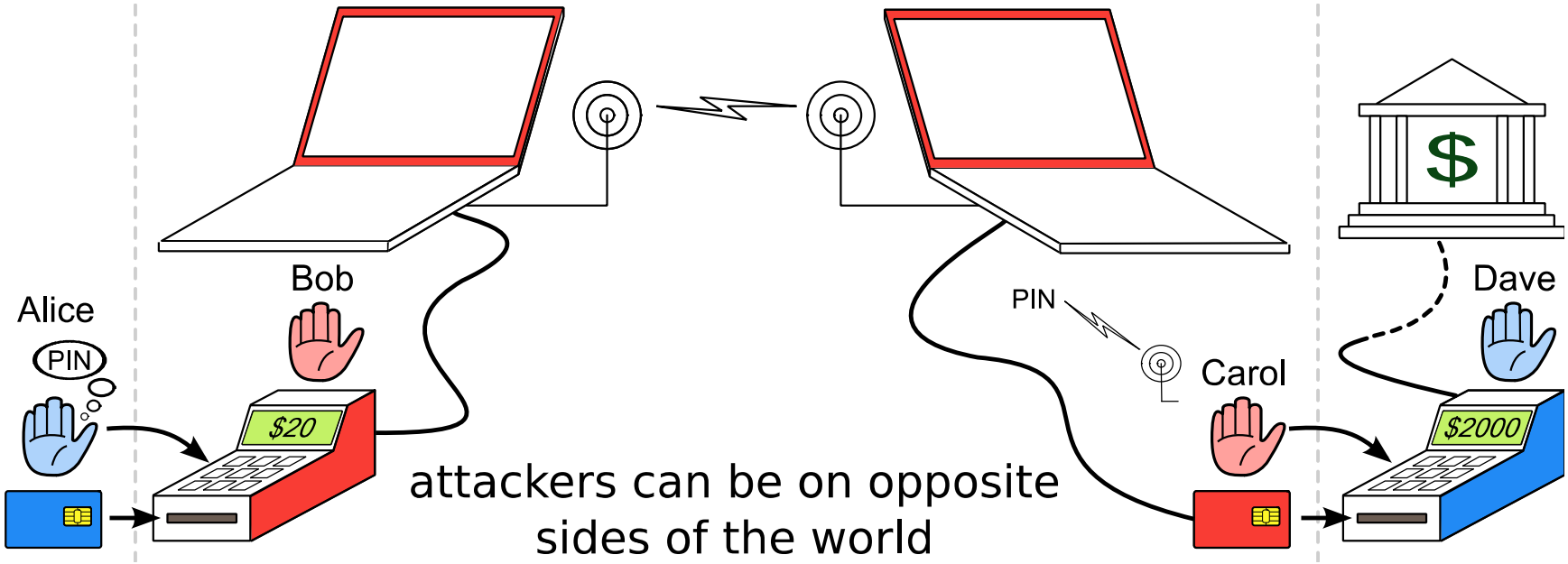


- Cardholder liable if PIN used
- Else merchant pays
- Banks hoped fraud would go down
- It went up …
- Then down, then up again

How might we attack EMV?

- 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 demo)



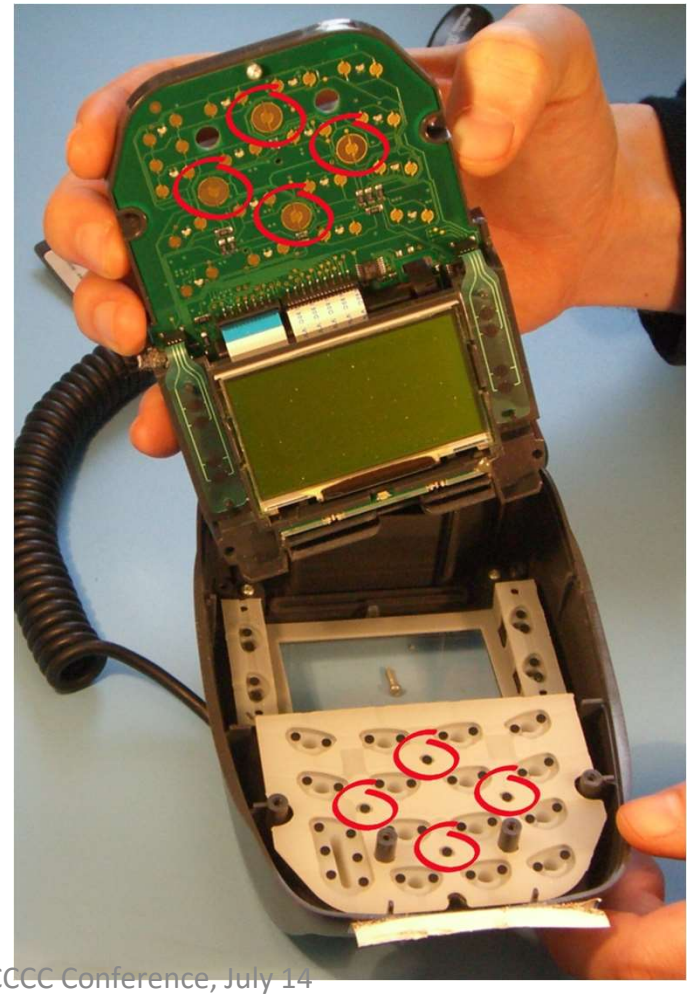
Attacks in the real world

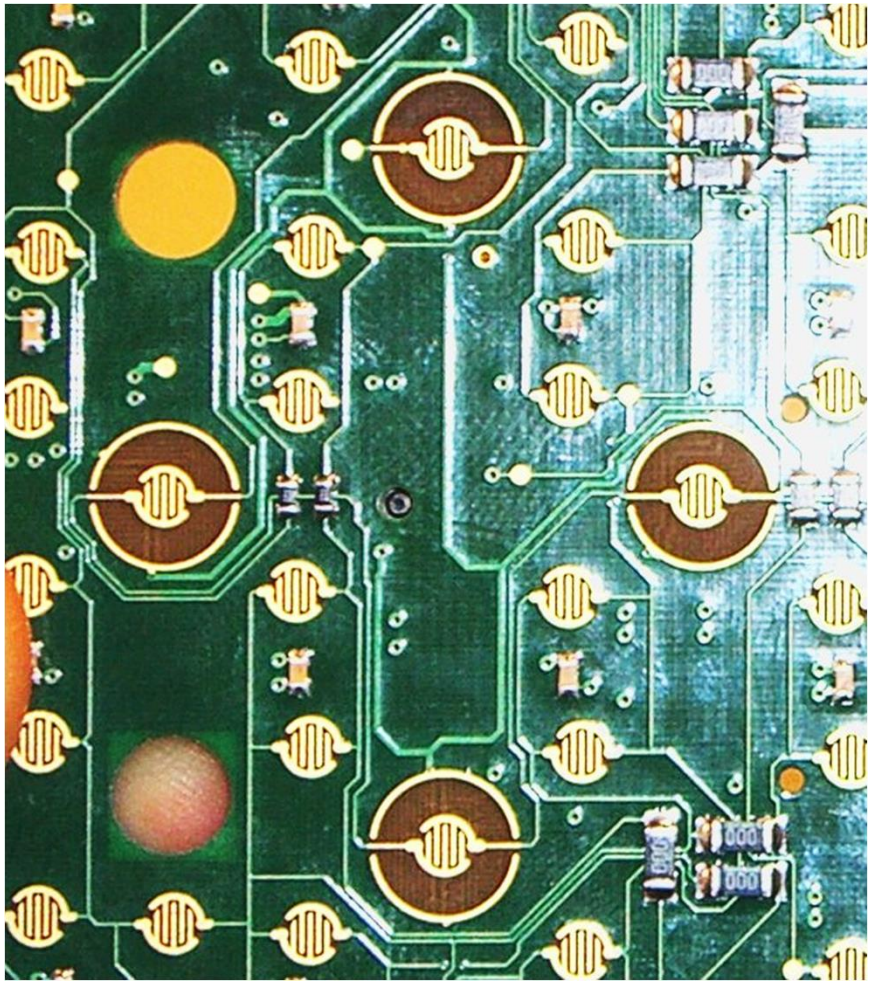
- The relay attack is almost unstoppable, and we showed it in TV in February 2007
- But it seems never to have happened!
- But mag-strip fallback fraud was easy for years
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier was blamed)
- Then ‘Tamil Tigers’
- After fraud at BP Girton: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

Tamper-proofing of the PED

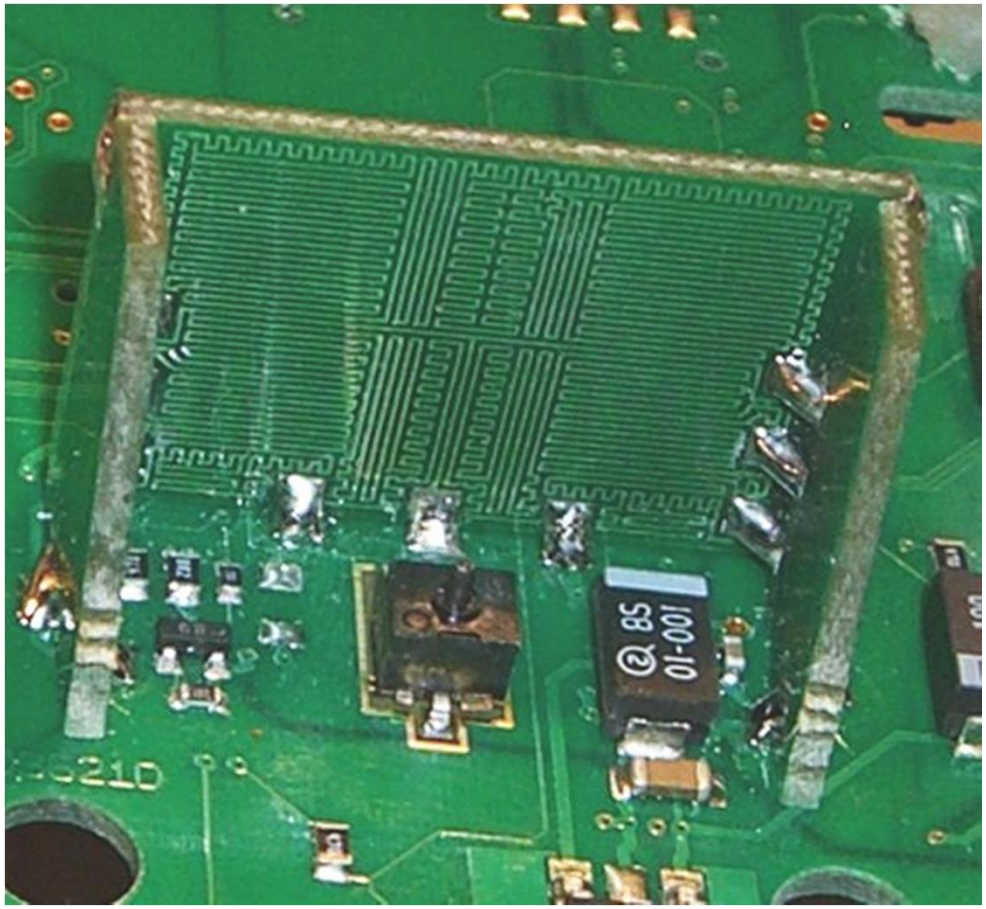
- In EMV, PIN sent from PIN Entry Device (PED) to card
- Card data flow the other way
- PED supposed to be tamper resistant according to VISA, APACS (UK banks), PCI
- 'Evaluated under Common Criteria'
- Should cost $25,000 per PED to defeat

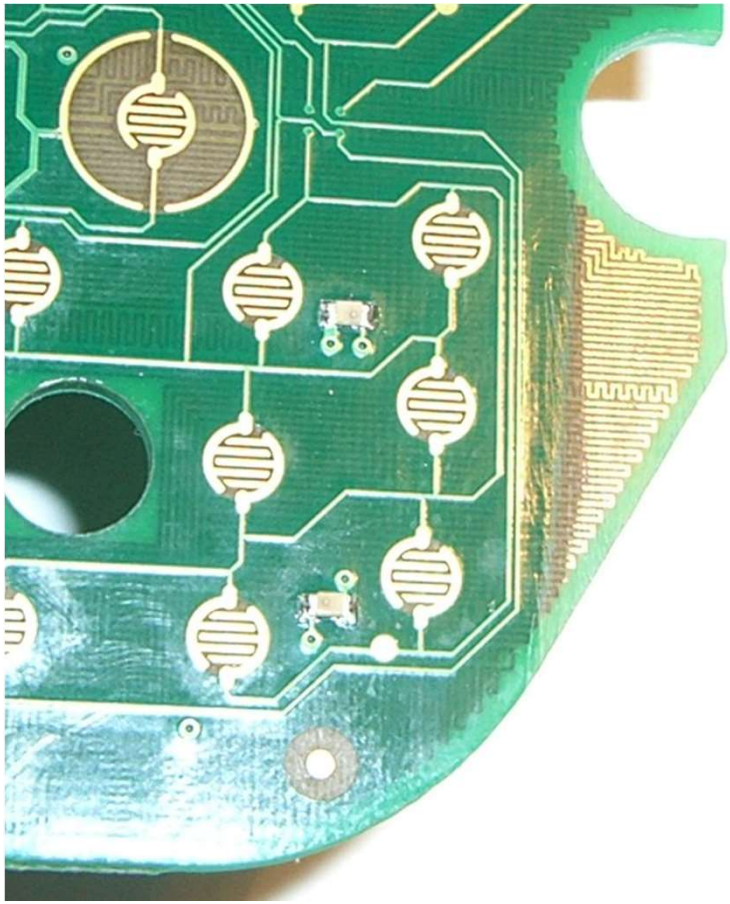
Tamper switches (Ingenico i3300)





… and tamper meshes too





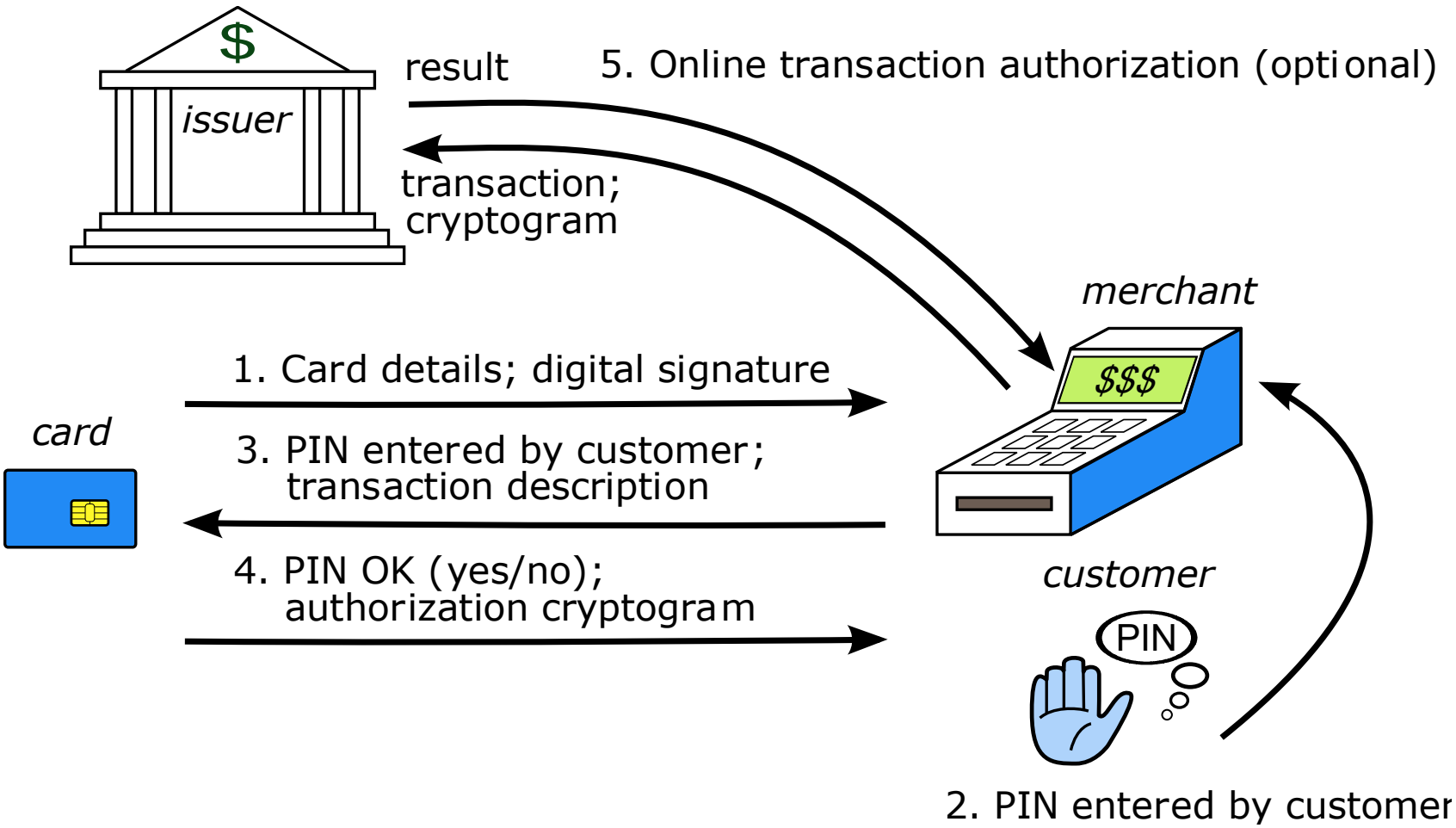
TV demo: Feb 26 2008

- 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)

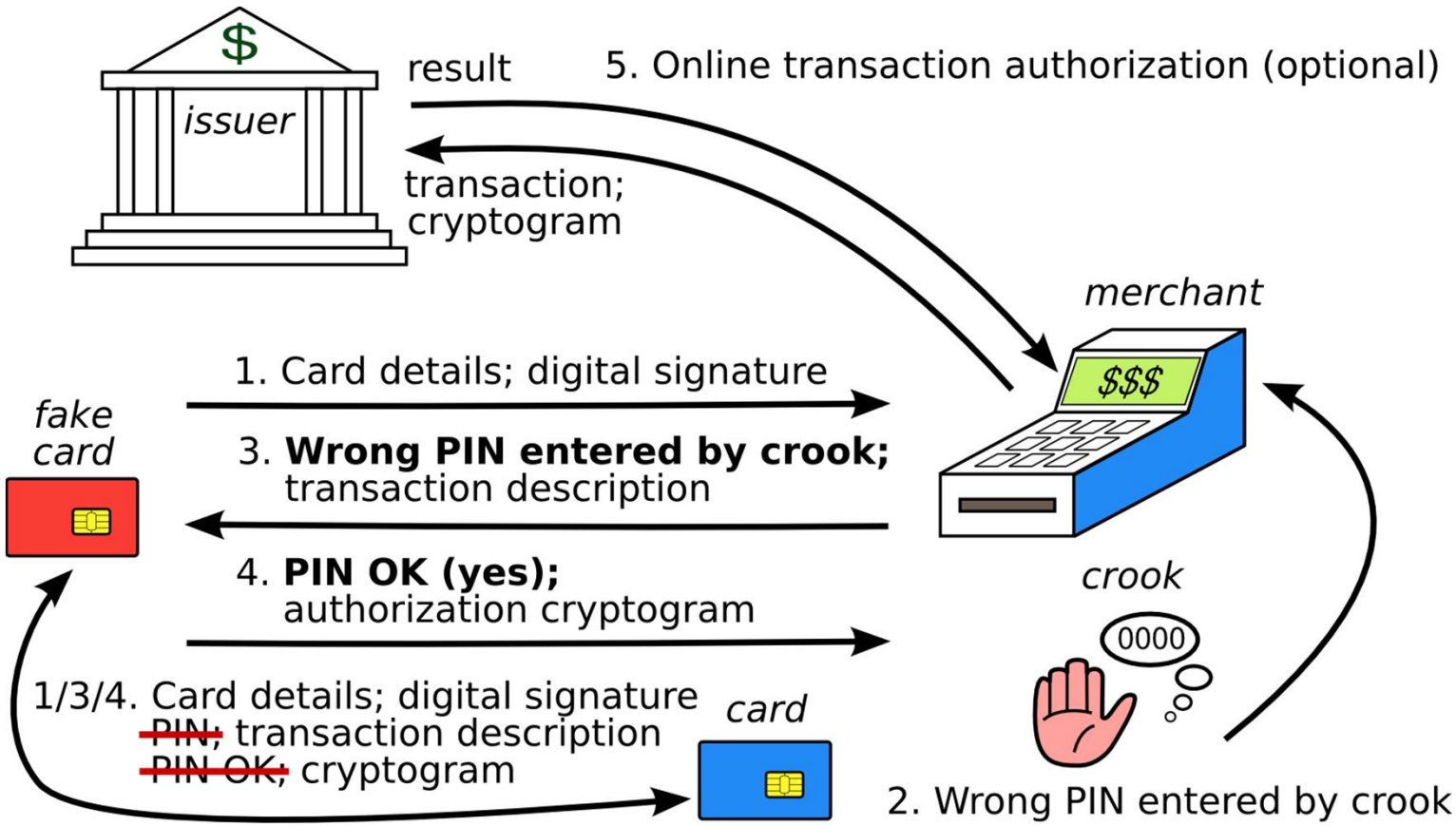
The ‘No-PIN’ attack

- Victims told us: crooks seem to be able to use a stolen card without knowing the PIN
- How? 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

- Might block at terminal, acquirer, issuer
- But – as with terminal tampering – acquirer incentives are poor
- Barclays blocked it July 2010 until Dec 2010
- Later, banks wrote to university PR department asking for Omar Chaudary’s thesis to be taken down from the website
- HSBC action 2015; other UK banks April 2016
- But victims still reporting likely cases in China!

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

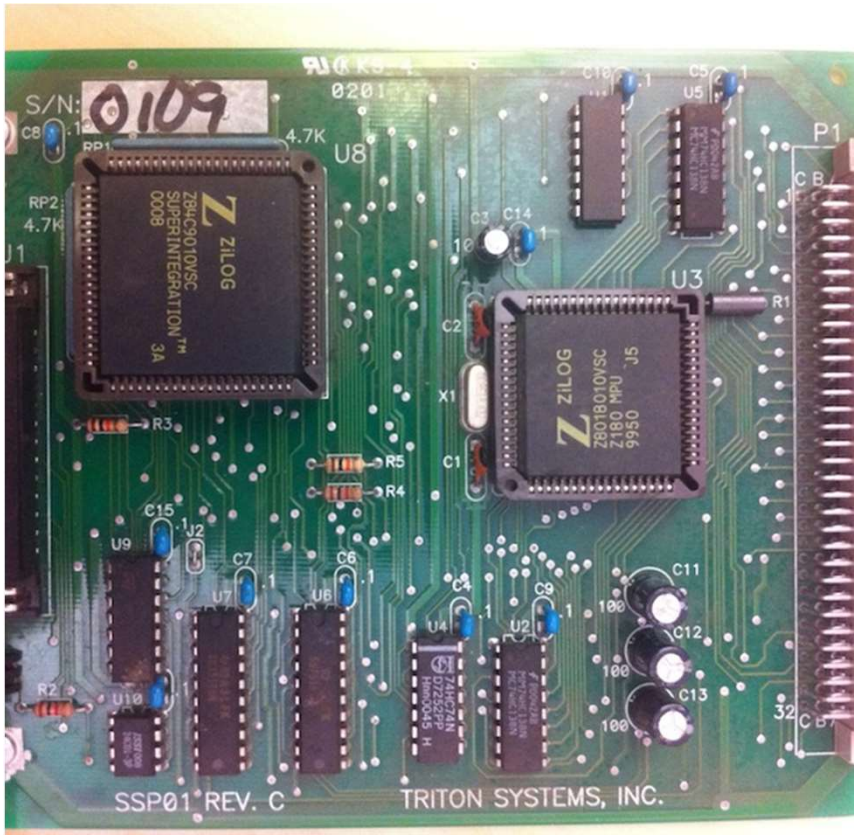
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

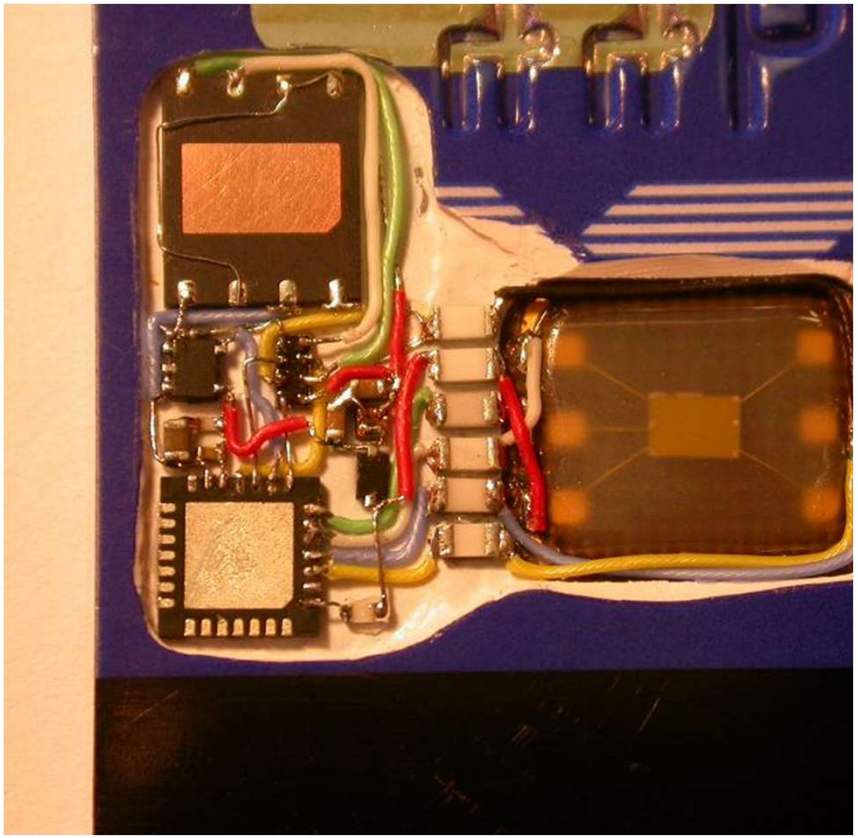
2011-06-28	10:37:24	F1246E04
2011-06-28	10:37:59	F1241354
2011-06-28	10:38:34	F1244328
2011-06-28	10:39:08	F1247348

- 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 Security & Privacy 2014
- Since then, we won a test 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

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 jumped bail; in jail now

We sometimes catch bad guys!

BBC Sign in News Sport Weather iPlayer TV Radio

NEWS LONDON

Home World UK England N. Ireland Scotland Wales Business Politics Health Edu

Entertainment & Arts

24 April 2014 Last updated at 15:04

Share

Cyber gang leader Tony Colston-Hayter jailed for bank scam

The leader of an internet gang which stole £1.25m from banks has been jailed for five-and-a-half years.

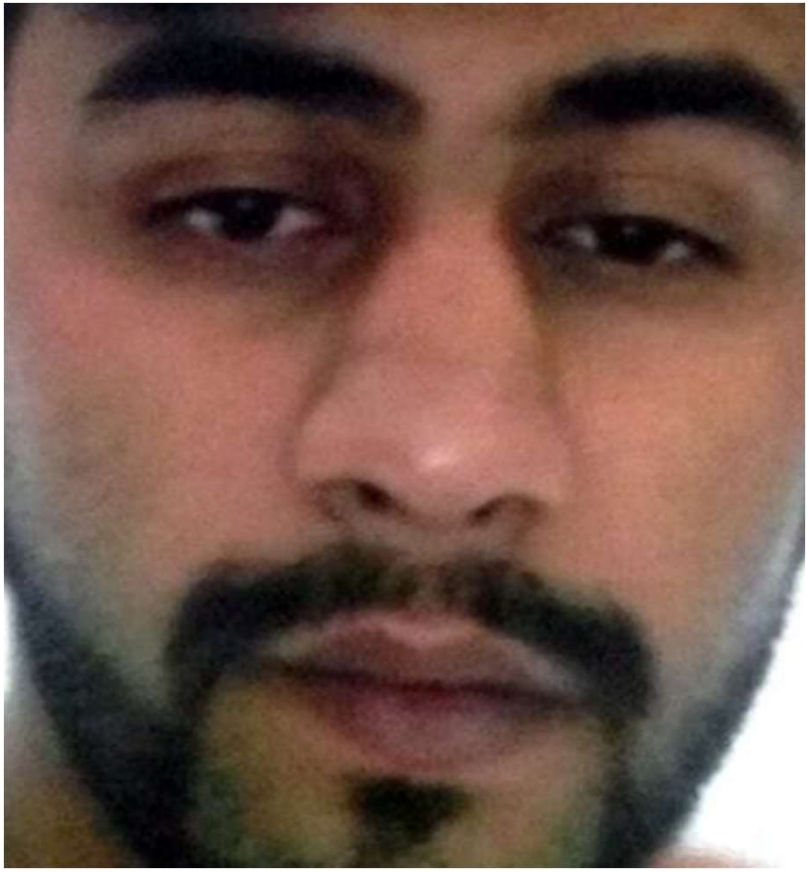
Tony Colston-Hayter, 48, led the gang which used a "Trojan horse" device to hijack computers at branches of Barclays and Santander.

They also stole credit and bank card details from about one million intercepted letters and used the money to buy Rolex watches and jewellery.

Nine others were also sentenced at Southwark Crown Court for the scam.

- Hayter got good at social-engineering call centres
- He got 5½ years; 8 others jailed too
- One of our two complainants got a refund (she sued)

The £60m Lloyds vishing scam



- Feezan Choudhary plus Lloyds insiders
- Social-engineer the one-time code
- Due to be sentenced in September
- Our client will have to sue for a refund!

Crooked rental ads

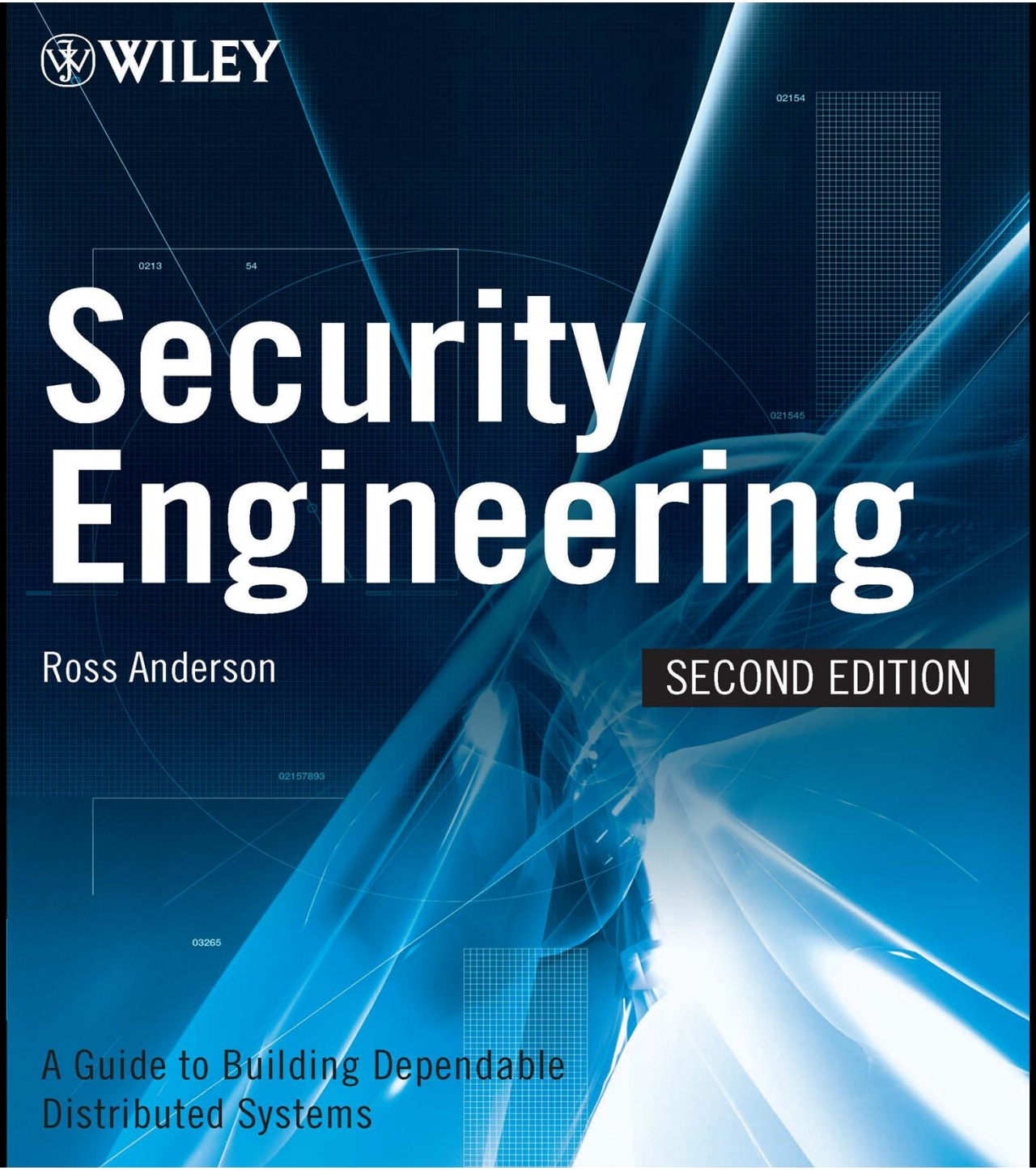
- About 80% of Cambridge ads in Craigslist
- + many in London
- Maybe one gang in Belgium or Ireland, one in West Africa
- Police not interested

What we're learning

- Most of the benefit is from single anecdotes that tell us to look hard at something
- Sparse evidence is better at falsifying hypotheses than confirming them
- Basically, there are many ways of doing fraud – but what gets done is what pays big time whether by big winnings or because it scales
- But we're interested in odd cases as well as the apparently significant stuff at scale

What we're learning (2)

- It's basically down to incentives – if Alice guards a system and Bob pays the cost of failure, you can expect trouble
- Ditto if Alice lobbies the regulator to dump the cost on Bob
- Banks' contract terms are often unreasonable (see our paper on bank fraud reimbursement)
- Post-brexit, what policy levers are there?


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems