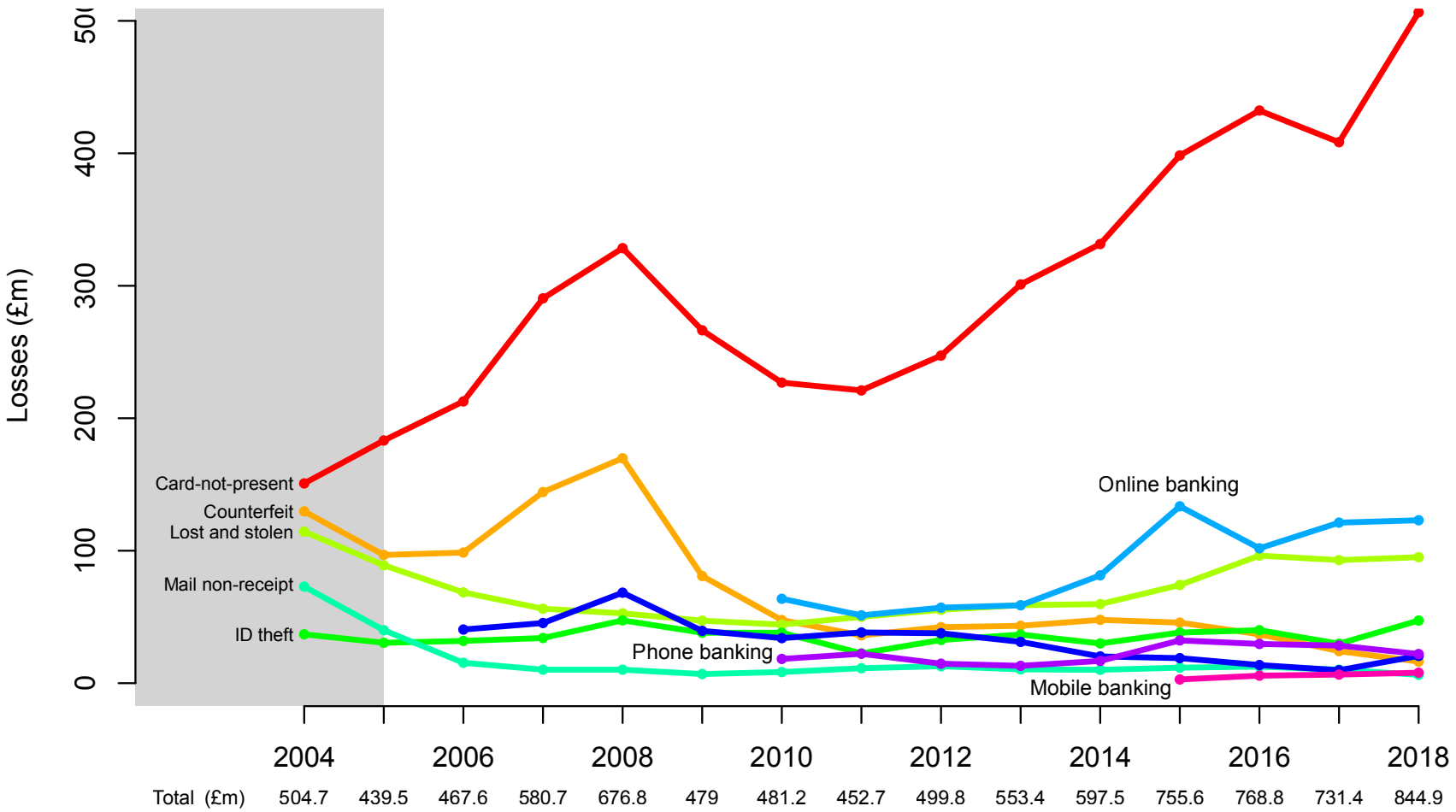
The EMV protocol suite

- Named for Europay-MasterCard-Visa with UK branding ‘chip and PIN’
- Developed late 1990s; deployed in UK 2003–6
- Europe, Canada followed; USA from 2015
- Banks’ big idea dea: if PIN used, blame the customer, else blame the merchant.
- What could possibly go wrong?

Card fraud history



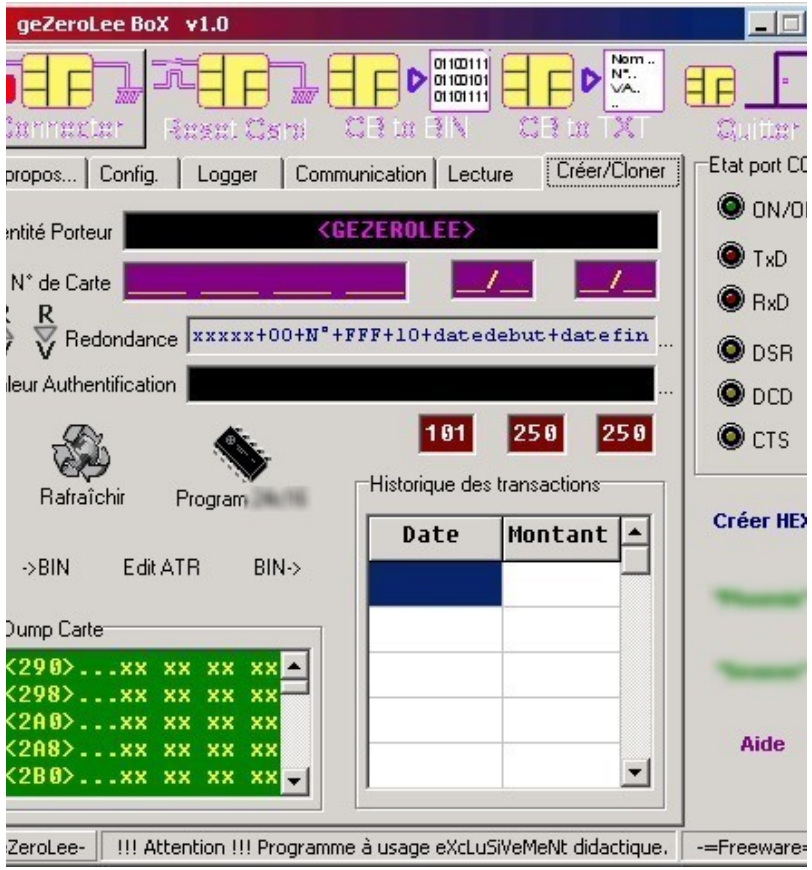
EMV shifted the landscape…

- 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

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
- Jol is now Barclays’ CISO…

Attack the optimisations

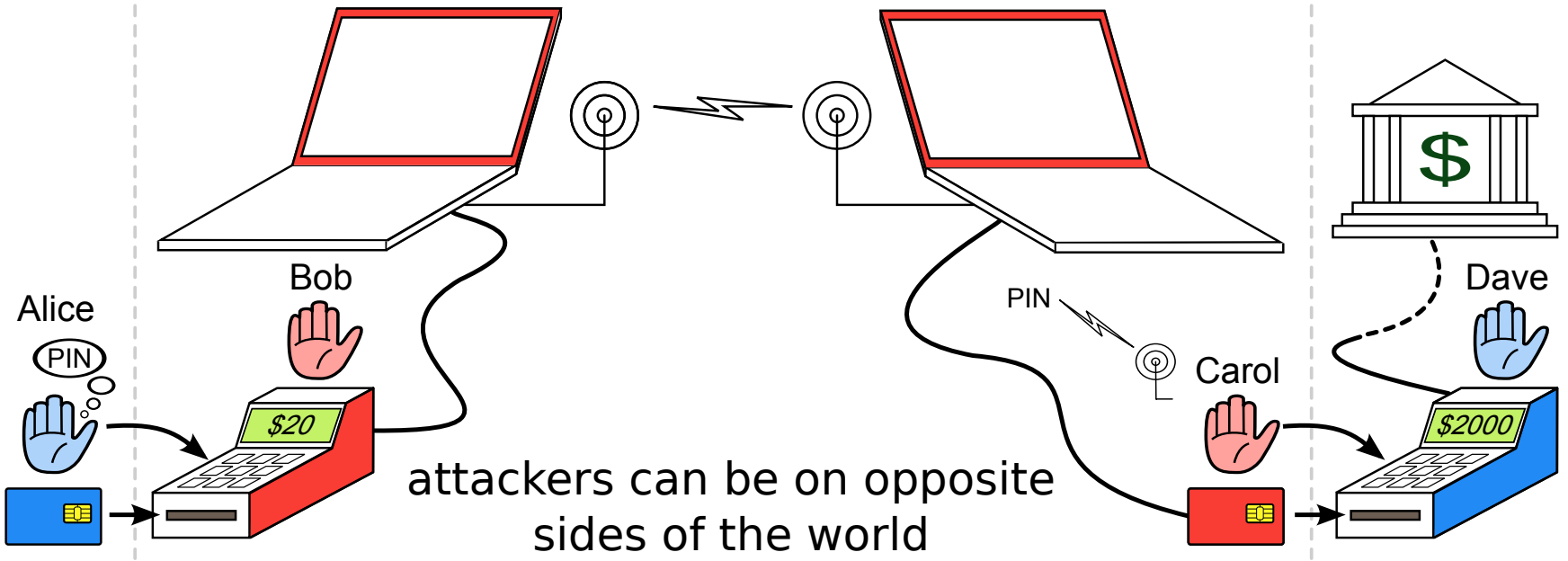


- Cheap cards are SDA (no public key crypto, static cert)
- A ‘yes card’ can do fraud offline
- Done in France, phased out from 2011

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!
- For years, mag-strip fallback fraud was easy
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier Trintech went bust)
- Then ‘Tamil Tigers’
- After fraud at BP Girton: we investigate

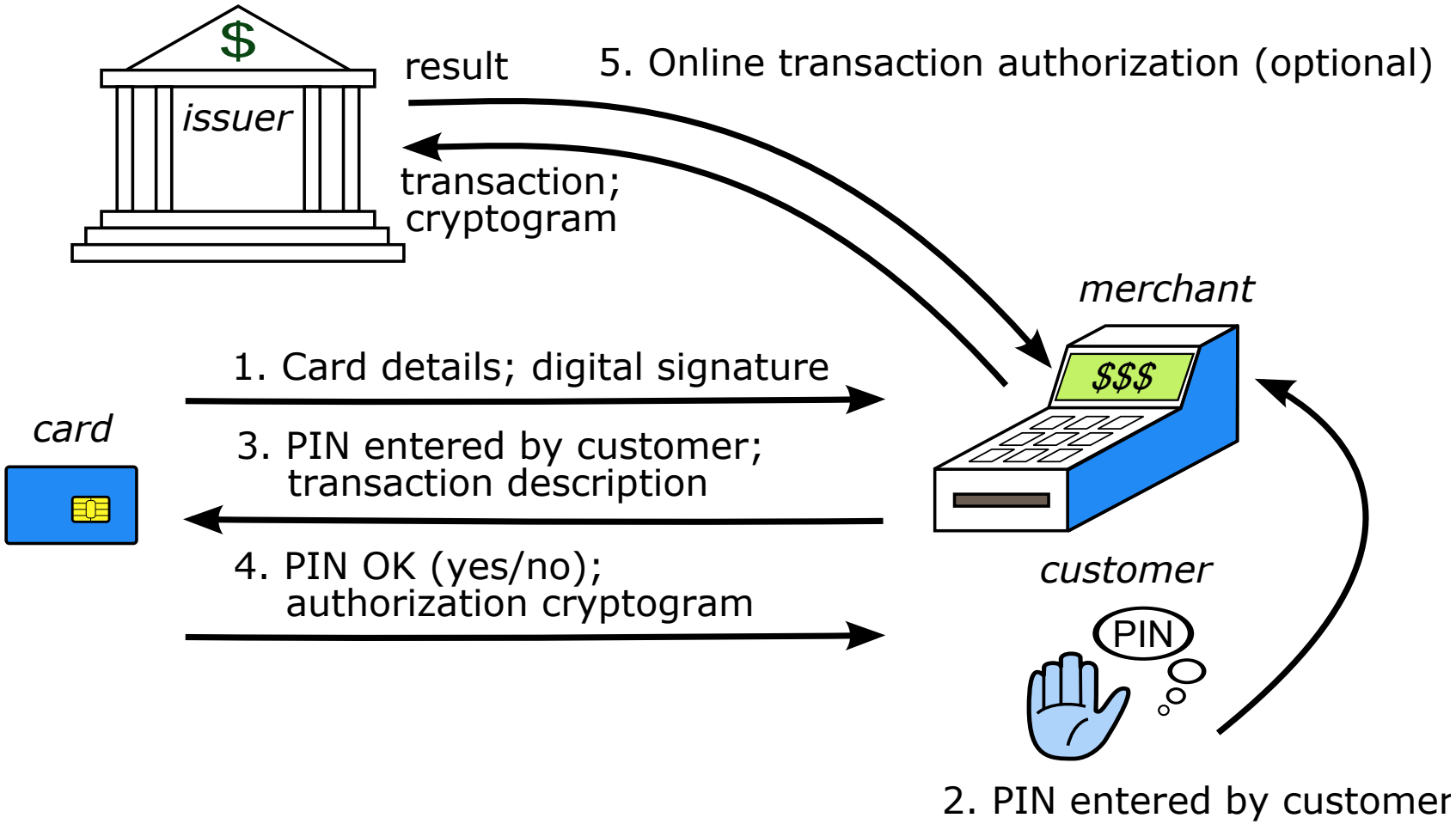
TV demo: Feb 26 2008

- 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)

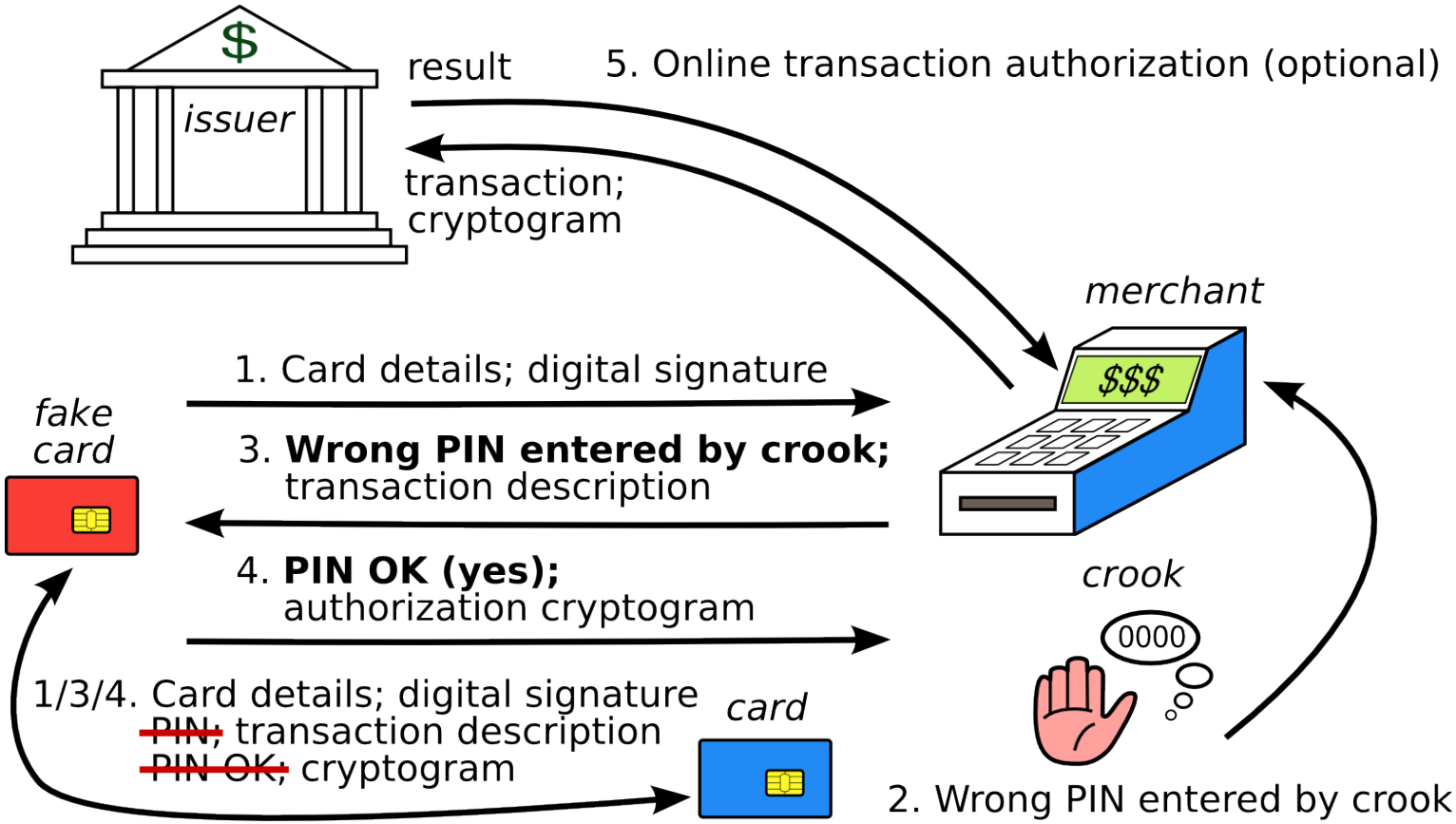
The ‘No-PIN’ attack

- 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
- By 2015 HSBC blocked it; 2017, other UK banks too

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

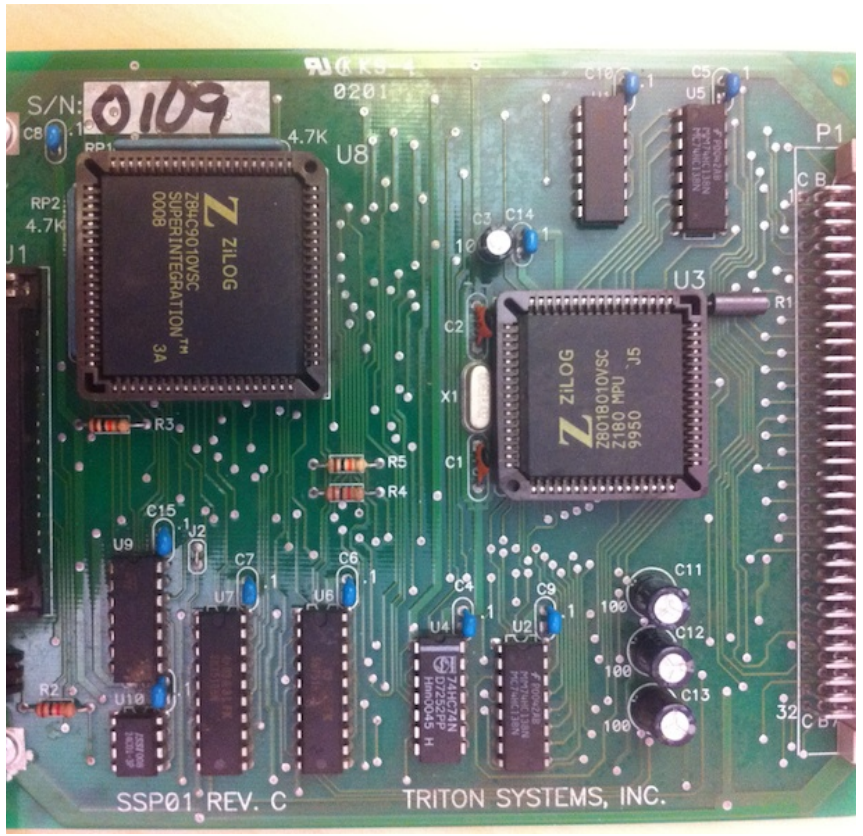
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

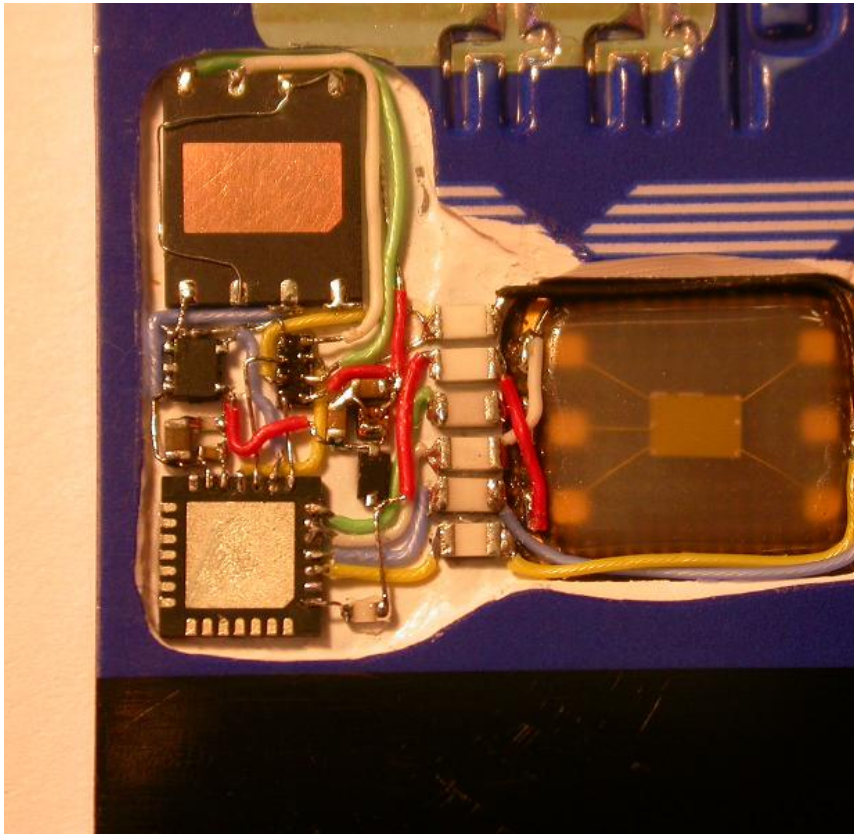
2011-06-28	10:37:24	F1246E04
2011-06-28	10:37:59	F1241354
2011-06-28	10:38:34	F1244328
2011-06-28	10:39:08	F1247348

- 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 2014, then a live 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

Authorised Push Payment

- Not on my graph as not calculated the same way in previous years
- However it's shot up to £354.3 million – second only to remote purchase fraud and more than the rest put together
- Has been surfaced thanks to FCA / PSR action
- The regulators' attention is overdue and welcome…

The death of 2FA

- PSD2 got banks to make 2fa universal
- Attacks ramping up rapidly!
- SIM swap started in South Africa, then Nigeria, then the USA since about 2016 (it got going there as a way of stealing instagram accounts)
- SS7 hacking used to be the agencies' baby
- Used in Germany for bank fraud in 2016, in the UK last year
- German banks consider SMS 2FA obsolete…

More …

- See www.lightbluetouchpaper.org for our blog
- And http://www.cl.cam.ac.uk/~rja14/banksec.html for our papers on payments
- Workshop on Economics and Information Security (WEIS): next edition in Brussels, June 2020
- See Arvind Narayanan's latest paper on SIM swap
- And my book 'Security Engineering – A Guide to Building Dependable Distributed Systems' (the chapter on Banking and Bookkeeping is underway)