The Internet of Bad Things, Observed

Ross Anderson

Cambridge

Bad software

- Since the 1980s, we think of malware as something that happens in Windows PCs
- But now CPUs and communications end up in everything that costs more than a few bucks
- Every industry is becoming a bit like the software industry
- How is the world going to change?
- Who will be the bad actors, what will be their motives and methods, and what can we do?

Bad software (2)

Bad software (3)

- Vehicle fuel economy (continuing)
- Smart meters and domestic energy efficiency
- Safety of medical devices (see papers by Harold Thimbleby)
- Surveillance of drug efficacy and safety (see papers by Ben Goldacre)
- Redlining (how do you regulate AI?)
- …

Government malware

- We've seen malware used to bug phones and laptops (Snooping Dragon, Bundestrojaner, WARRIORPRIDE…)
- Now the gang boss's kid's Barbie doll has an exploitable microphone
- So does the emergency call assist button in his car, even if his phone's off
- And the drugs squad wants to read meters to know who's running a lot of lamps …
- One warrant to hack them all?

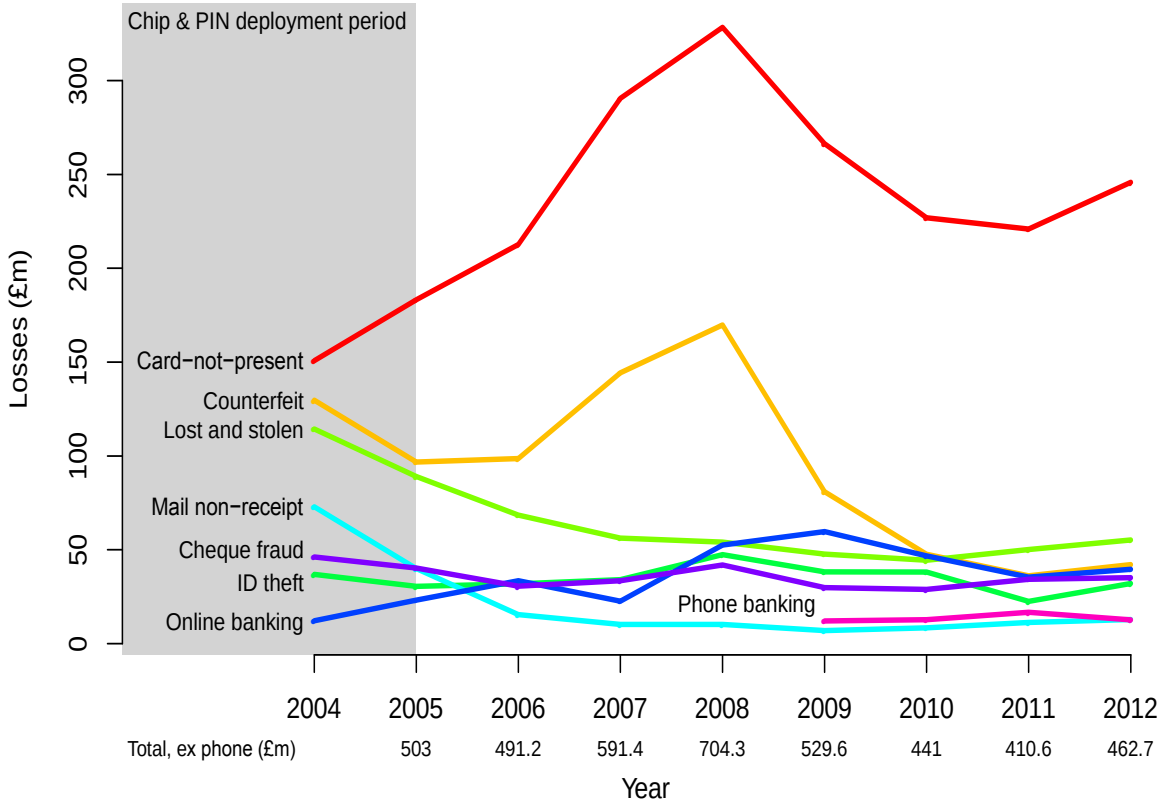
The EMV protocol suite

- 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
- Supposedly deployed in the USA by 2015
- Fascinating story of failures and frauds
- Many lessons for security engineers!

EMV 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

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…

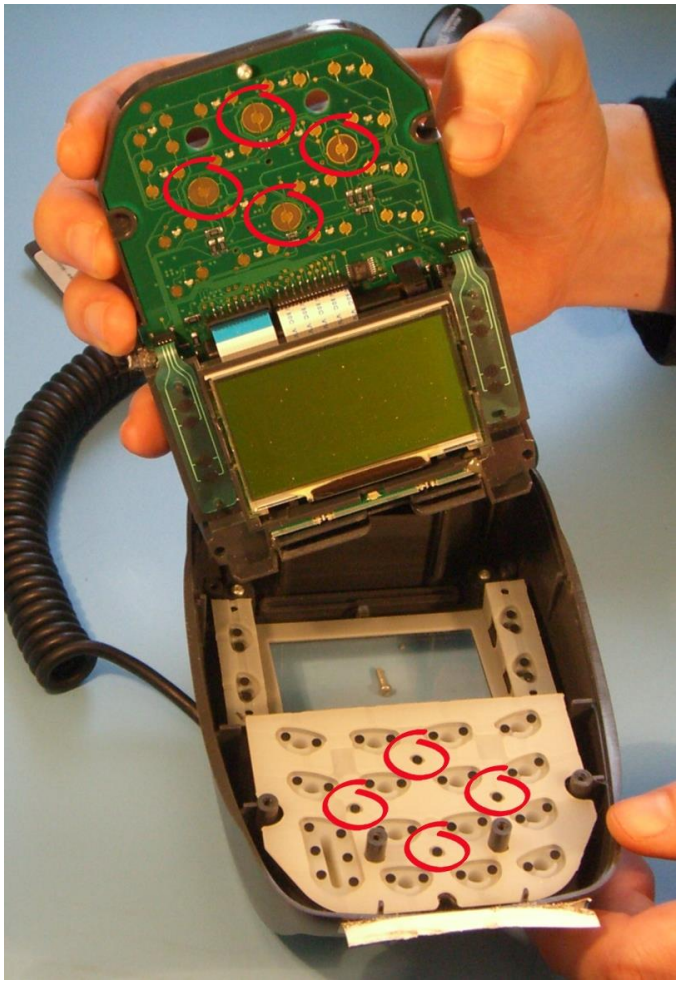
What about a false terminal?

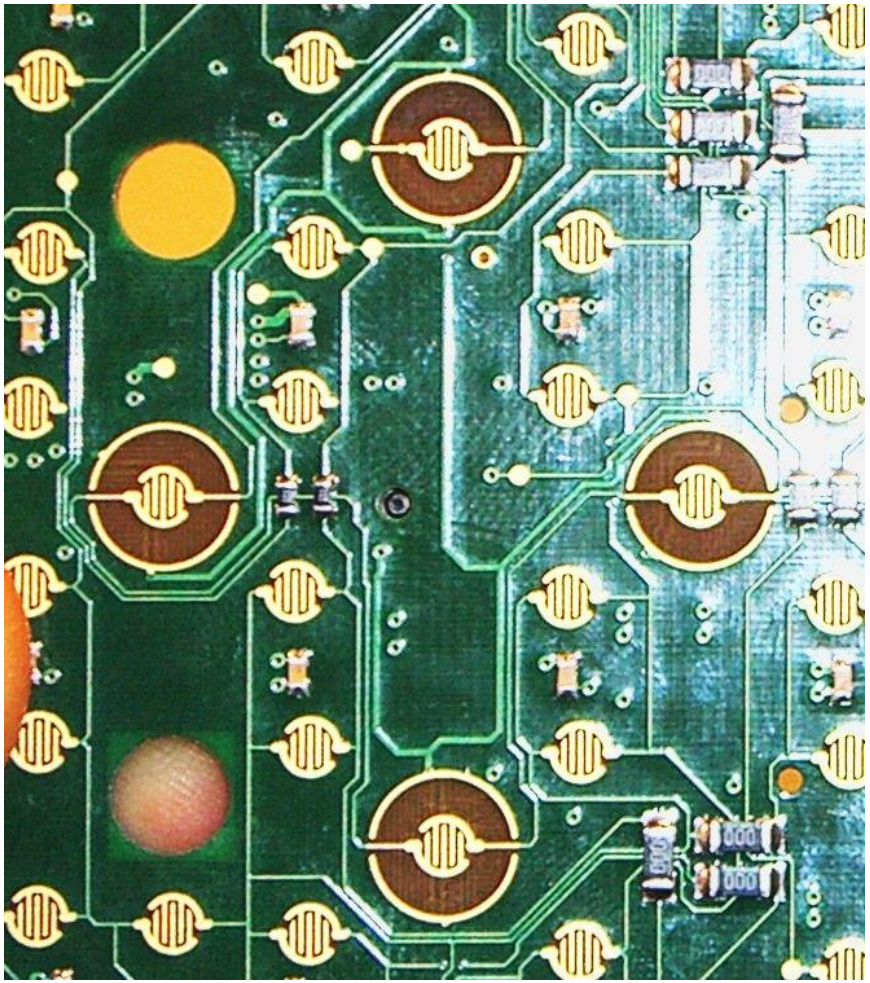
- Replace a terminal's insides with your own electronics
- Capture cards and PINs from victims
- Use them to do a man-in-the-middle attack in real time on a remote terminal in a merchant selling expensive goods

Tamper-proofing of the PED

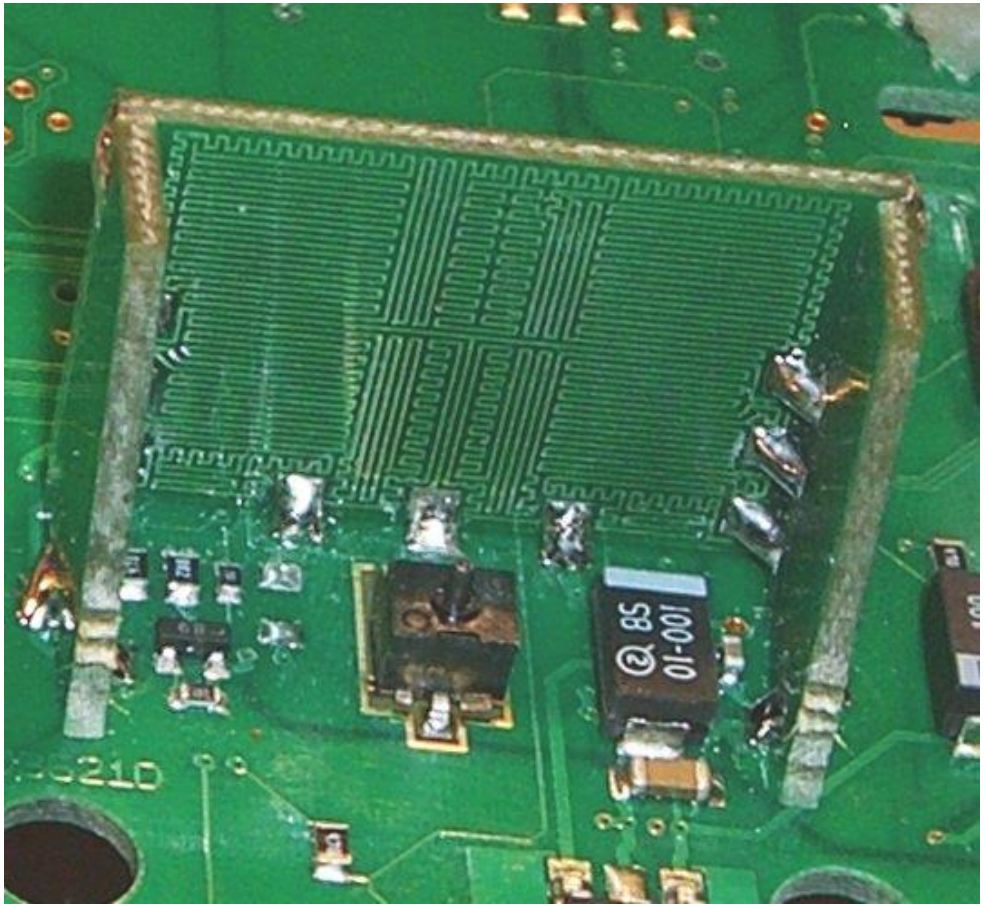
- In EMV, PIN sent from PIN Entry Device (PED) to card
- Card data flow the other way
- PED supposed to be tamper resistant according to VISA, APACS (UK banks), PCI
- ‘Evaluated under Common Criteria’
- Should cost $25,000 per PED to defeat

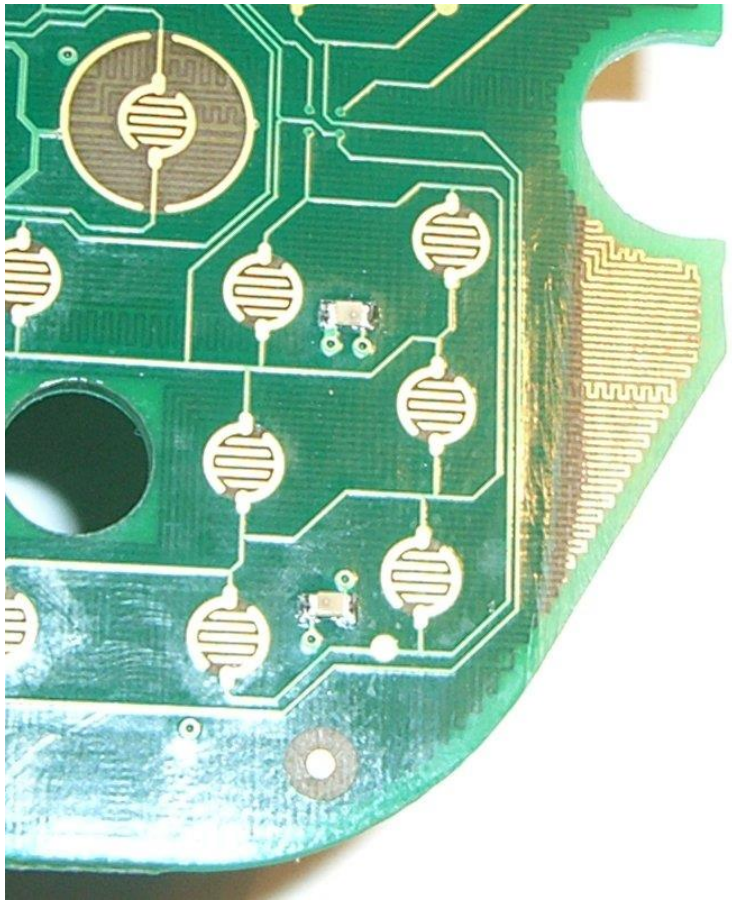
Tamper switches (Ingenico i3300)





… and tamper meshes too

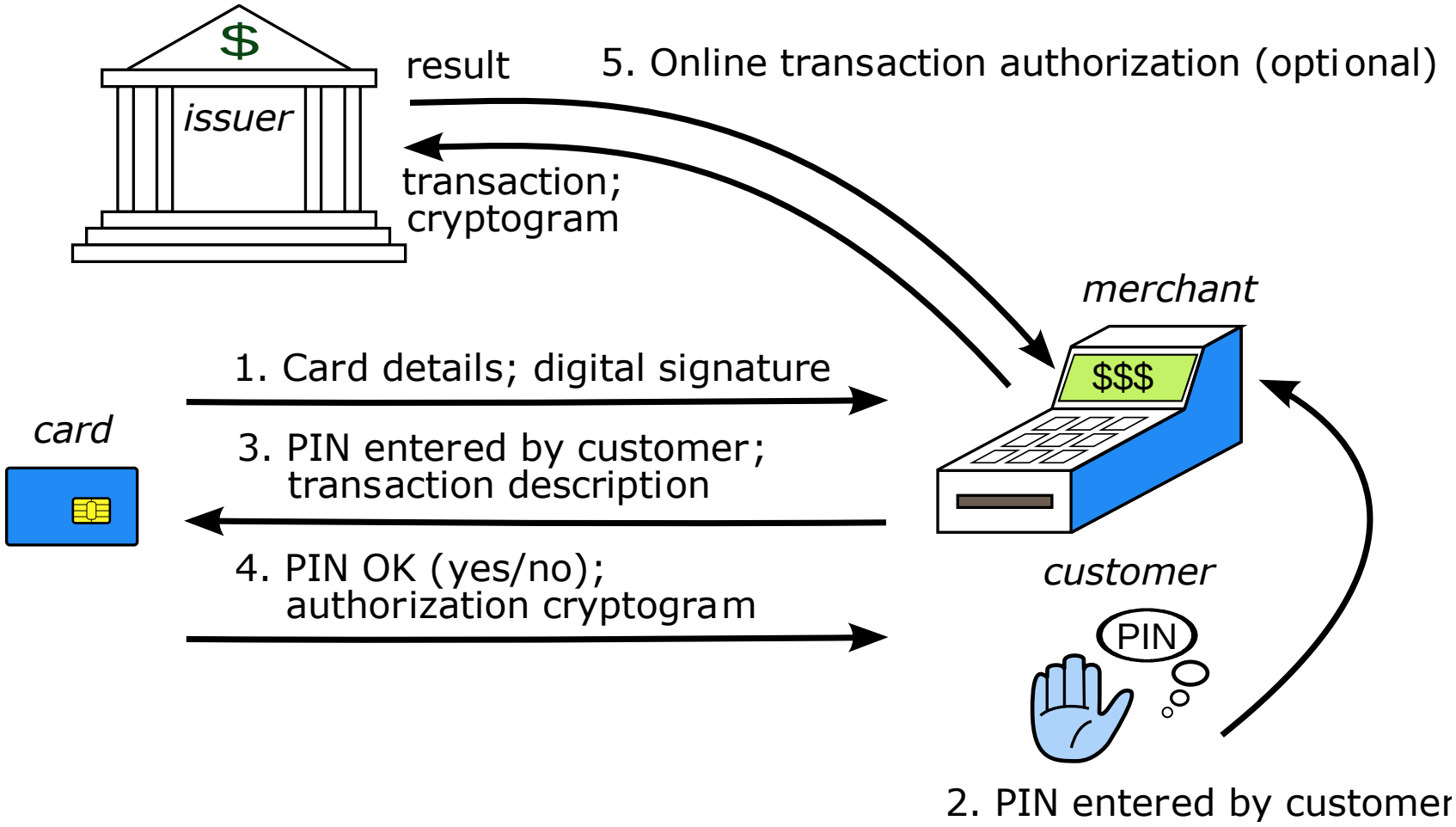




TV demo: Feb 26 2008

- 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)

A normal EMV transaction



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

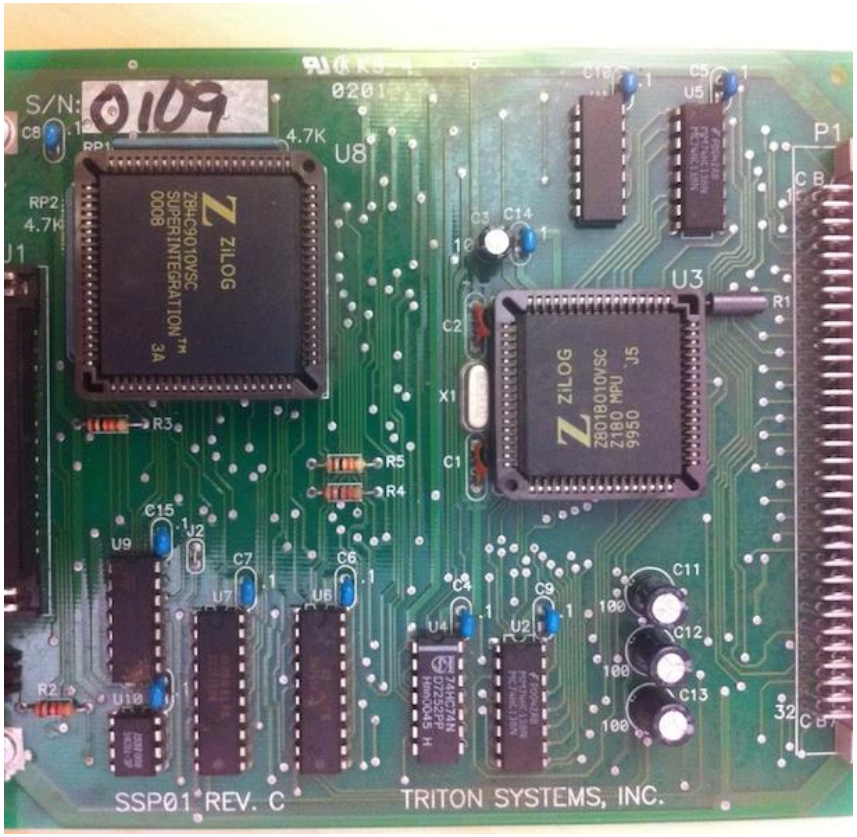
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

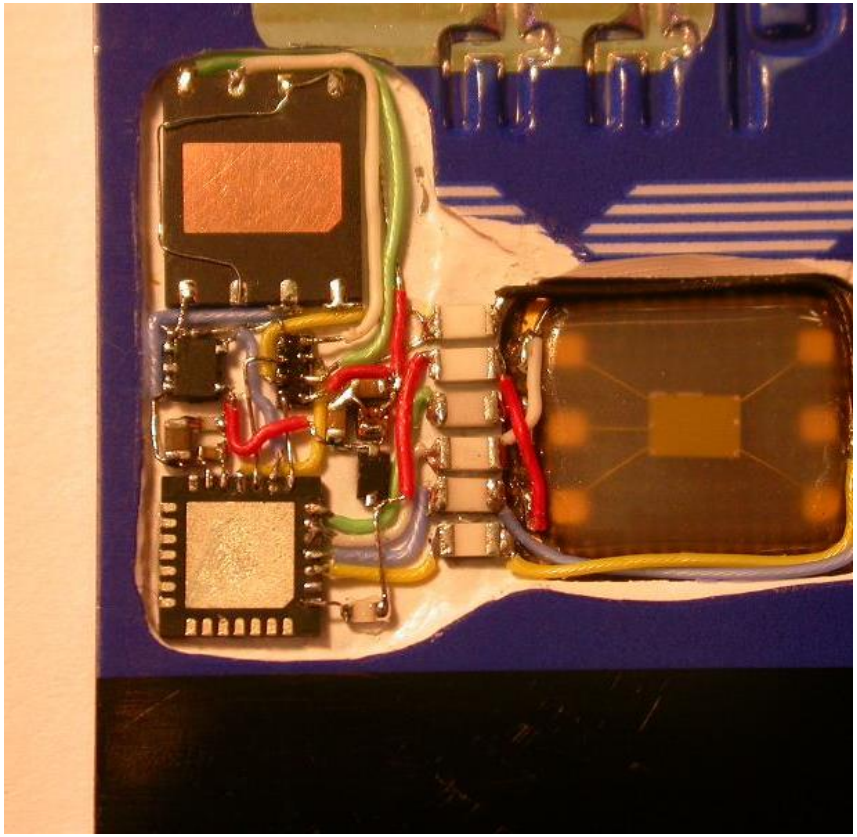
2011-06-28	10:37:24	F1246E04
2011-06-28	10:37:59	F1241354
2011-06-28	10:38:34	F1244328
2011-06-28	10:39:08	F1247348

- 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)



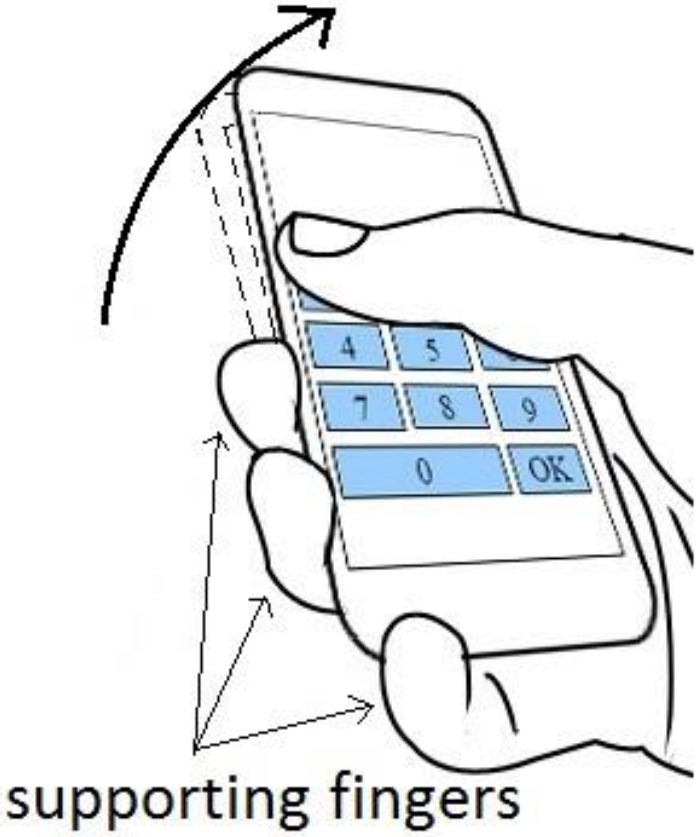
The preplay attack

- 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

Other terminal malware tricks

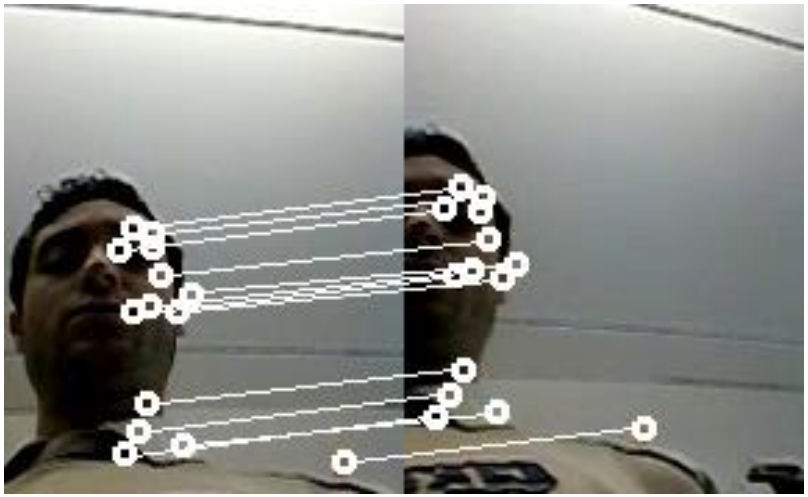
- In 2010–1 we discovered the “No-PIN” attack
- Bad people can use a man-in-the-middle device to use a stolen EMV card for which they don’t know the PIN
- First done in France by adding electronics to stolen cards
- Can now be done in PIN entry device (PED) software (Turkey?), or a SIM shim hidden in the PED (possible case in China)

Phone malware: 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
- Laurent and I asked: does it really?

Attacks on factory reset (2)

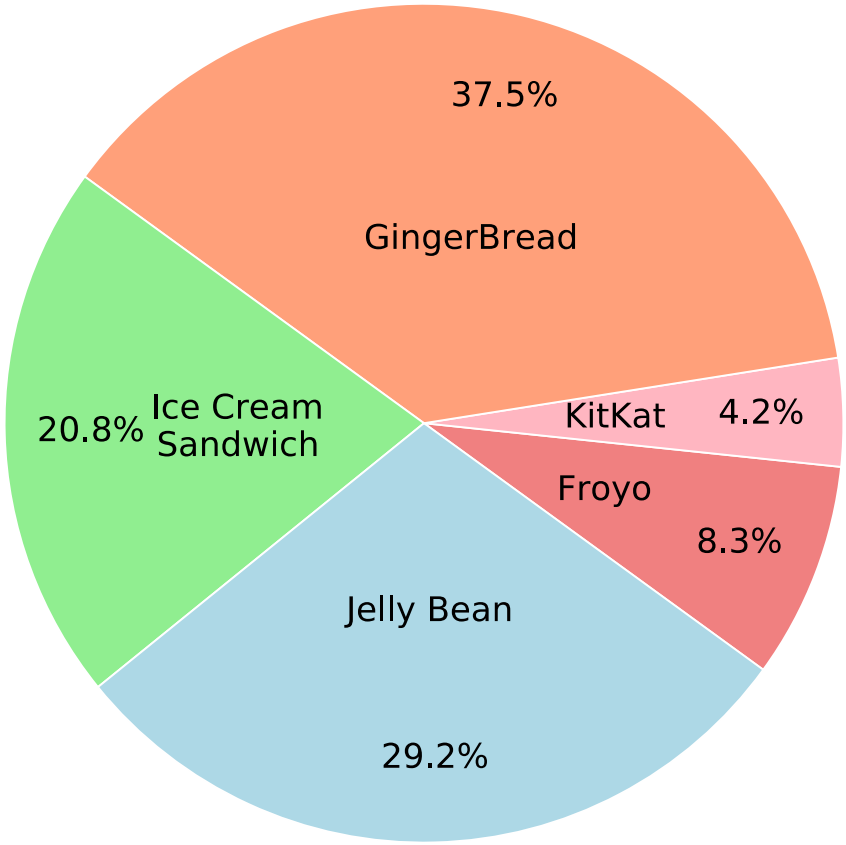
- We bought 23 Android phones from eBay etc
- In most cases, got the Google master cookie

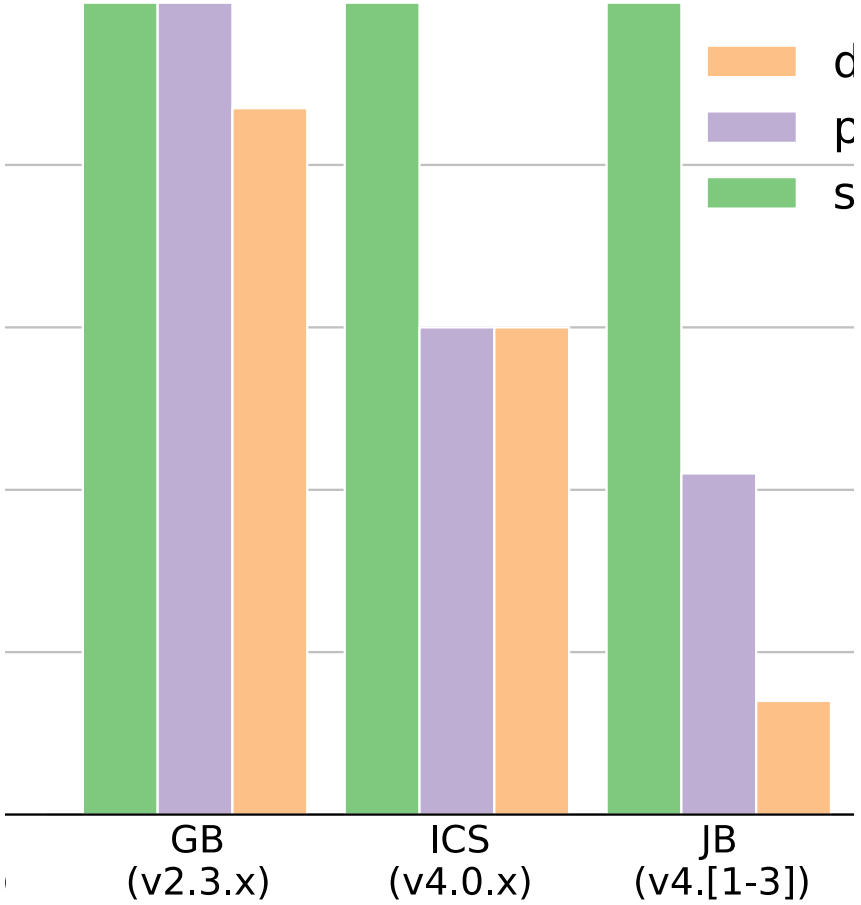
```
username@gmail.comcom.googleAFcb4KRs88NZlzN-r6qHrSHGF1TWyh...TKw==
clDQAAAJ4AAABQPfQhNXLTDYDLgHoIFDdDIEojBokYr_6ad0WeSr2kVpK4...B-0pd
androidmarketDQAAAJ8AAAD1NNQaeO_yxfgNMtSvnQVangE3DAatlKtTo...INkZV
```

- 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!

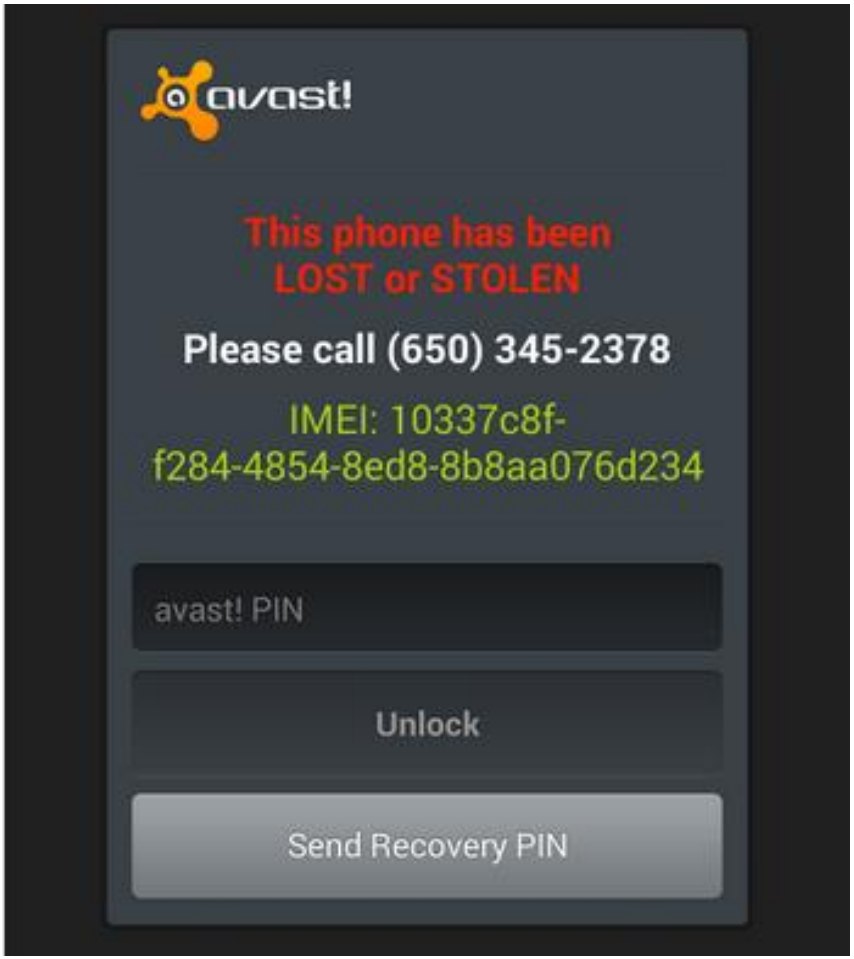




Attacks on factory reset (3)

- 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



- 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

How can we monitor all this?

- ‘Device Analyzer’ is an app that’s been run on 23,000 mobile devices
- With ethical approval, and full user consent (users reminded every month)
- Who’s running what app; who’s using what radio service; traffic patterns (non-linkable)…
- 251 researchers have used samples, 61 signed access licenses, 2 joint projects

Cambridge Cloud Cybercrime Centre

- Thousand of people do academic security research but few work with real data
- Those who try, spend years getting access to data, then get swamped, then write up and leave
- Can’t do open data as most datasets dirty
- Other people can’t repeat out work, so is it science?

Perhaps we have an answer…

- We have 5 years funding from the EPSRC to create the **Cambridge Cloud Cybercrime Centre**
- Our academic status will help us collect one of the largest and most diverse datasets on cybercrime
- We will mine and correlate these data to extract information about criminal activity. We will detect it better & faster and invent the forensics of the future
- We aim to create a sustainable centre for academic research into cybercrime.
- BUT we want others to be able to play too!

Fighting crime isn't competitive

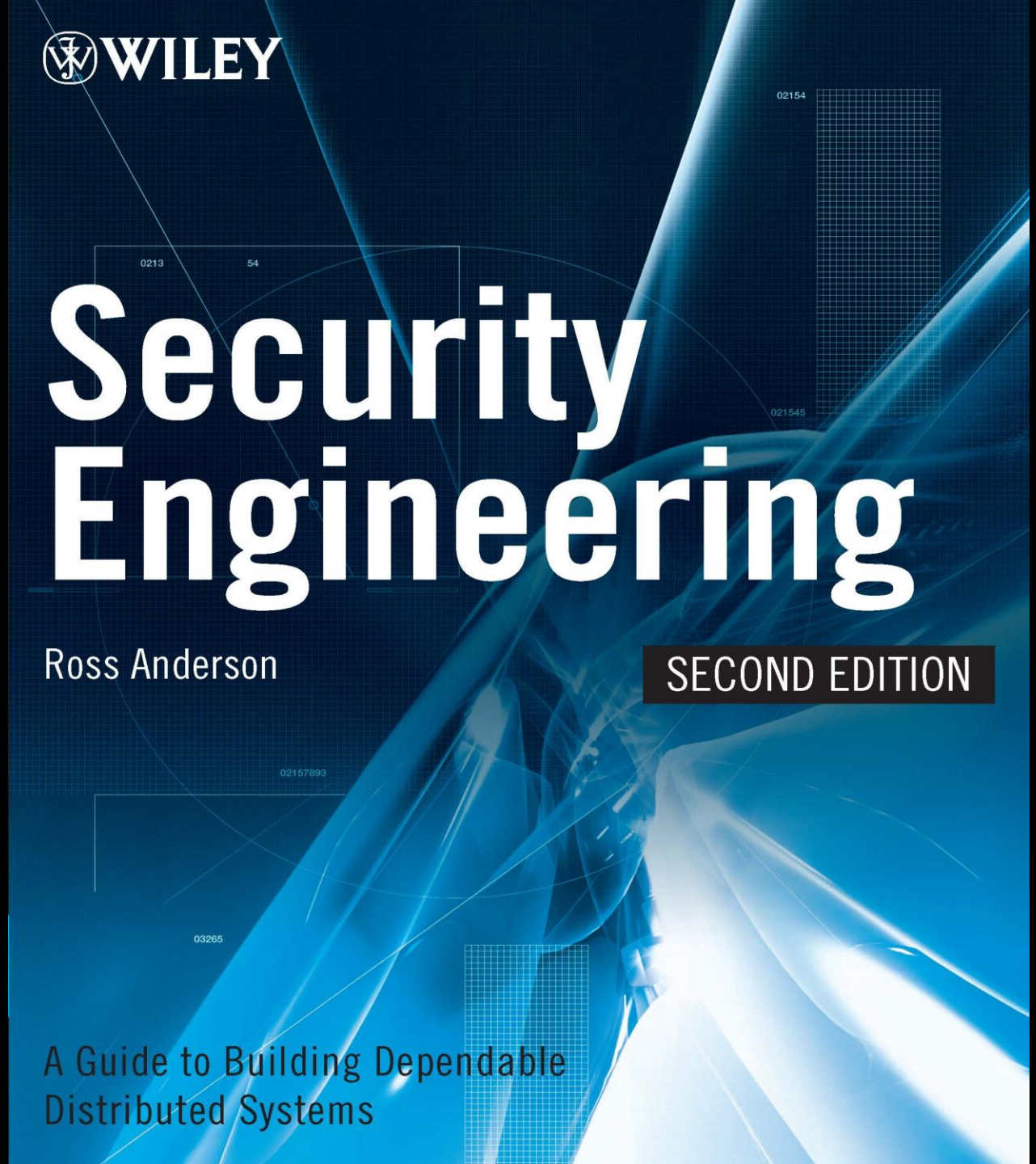
- We're going to have a LOT of data, available to other researchers under a standard NDA
- At the end of the first five years we want to be judged not on how many papers we wrote in Cambridge but how many papers others wrote because we helped to make that possible
- We also want to see MSc and undergraduate students tackling cybercrime projects and confirming or refuting classic results.
- We want to see new ways to prevent crime, to detect and deter criminals

Conclusion

- Malware scaled up in the 1980s as a PC thing
- That's now changing. We're already seeing it on Android and in payment terminals
- The Internet of Bad Things will be next
- Many questions of technology, and policy!
- Our new Cambridge Cloud Cybercrime Centre will provide a shared platform to study this
- Share your data with us!

More …

- Cambridge cloud cybercrime centre: https://www.cambridgecybercrime.uk/
- Device Analyzer: https://www.deviceanalyzer.cl.cam.ac.uk
- 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 at Berkeley, June 2016
- My book 'Security Engineering – A Guide to Building Dependable Distributed Systems'



VB, Prague, 2015