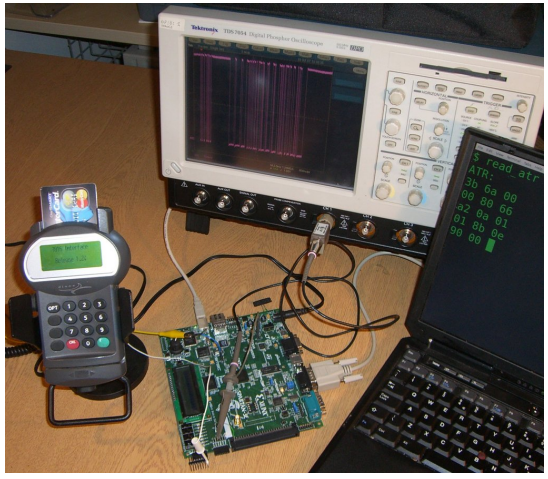
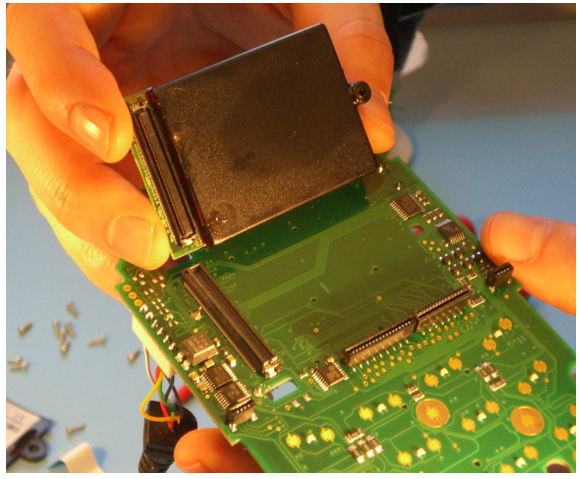
Secure Payment Architecture





Steven J. Murdoch

http://www.cl.cam.ac.uk/users/sjm217/

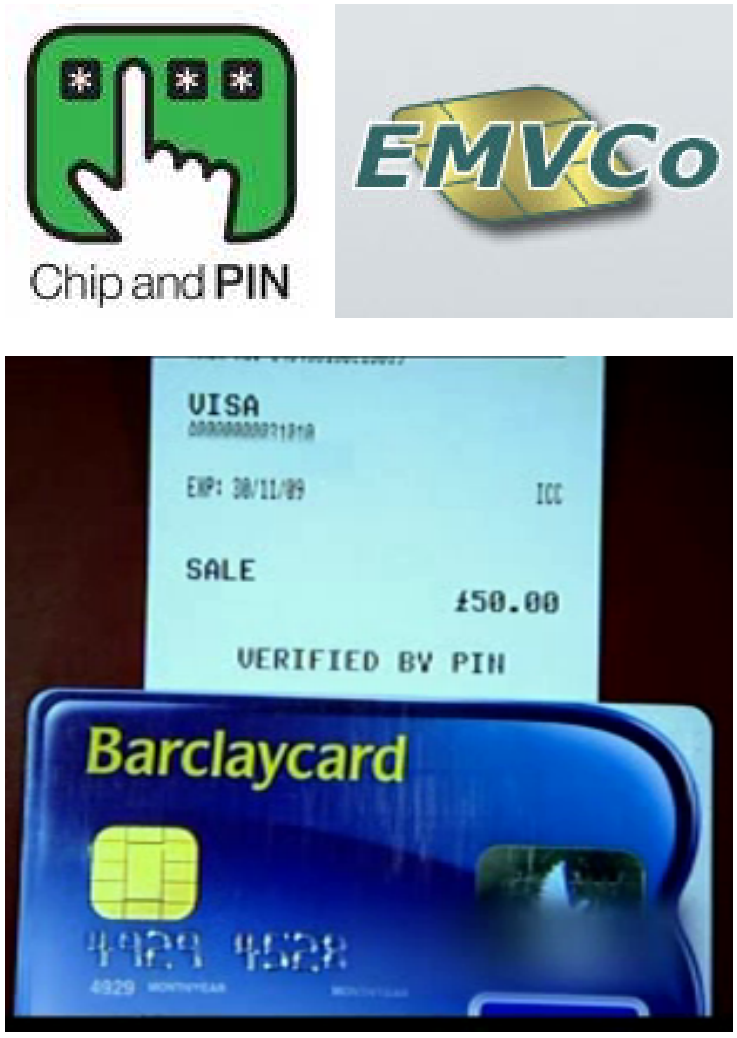
work with Saar Drimer, Ross Anderson, Mike Bond

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

SecAppDev, February 2014, Leuven, BE

Chip & PIN has now been running in the UK for about 5 years

- Chip & PIN, based on the EMV (EuroPay, MasterCard, Visa) standard, is deployed throughout most of Europe
- In process of roll-out elsewhere
- Customer inserts contact-smartcard at point of sale, and enters their PIN
- UK was an early adopter: rollout in 2003–2005; mandatory in 2006
- Chip & PIN changed many things, although not quite what people expected

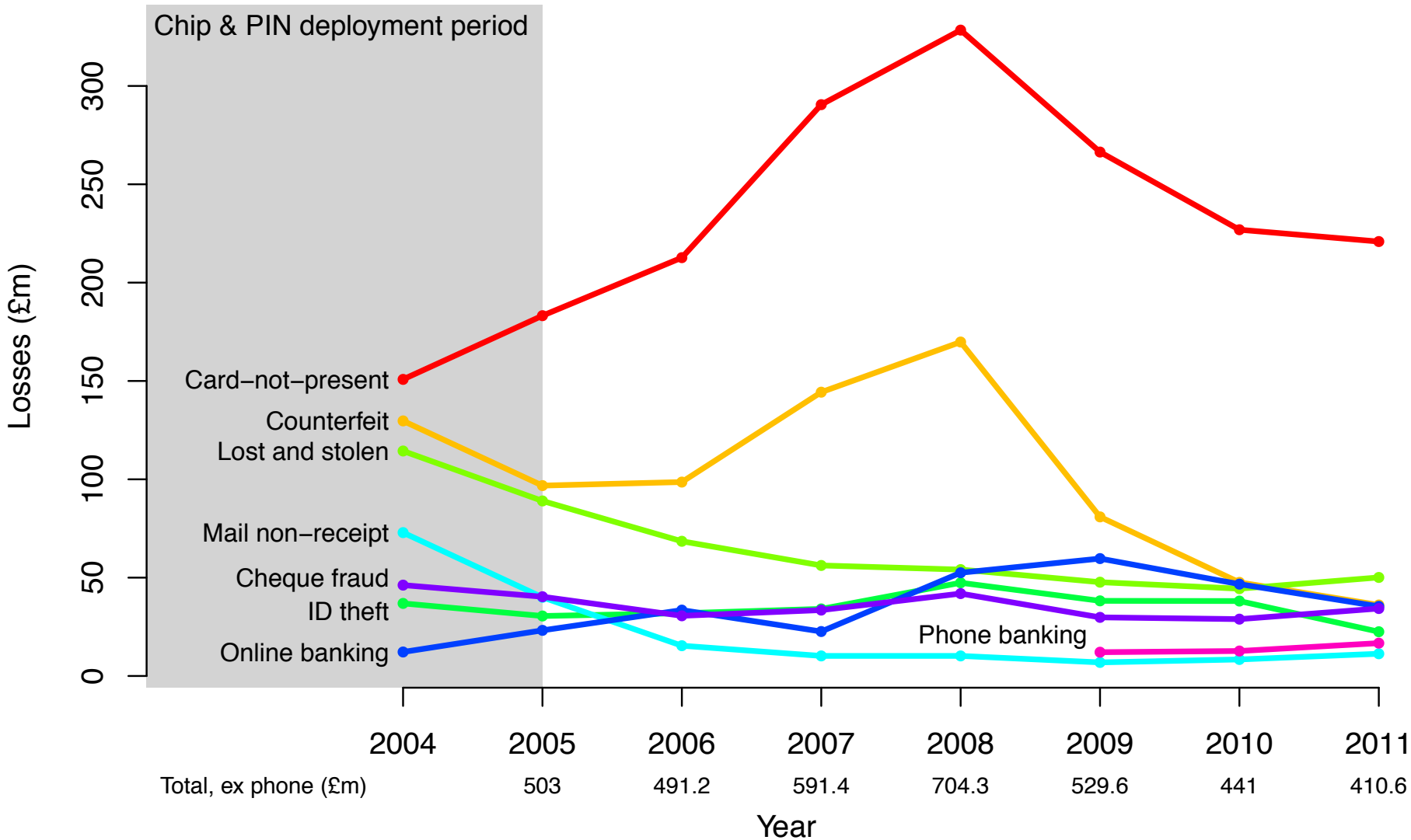


Card payments in the UK are different from the US (and elsewhere)

	Before Chip & PIN	**After Chip & PIN**
Cards	magstrip	magstrip and chip
Card verification	magstrip	chip if possible
ATM	PIN used	PIN used
Point-of-sale	signature used	PIN used

- No difference between credit and debit cards
- No ID check at point-of-sale (signature rarely checked either)
- Introducing Chip & PIN really made two changes:
  - Chip used for authenticating card (ATM and PoS)
  - PIN used for authenticating customer (only new for PoS)
- The effects of the two changes are often conflated

UK fraud figures 2004–2011



Source: Financial Fraud Action UK

Counterfeit fraud mainly exploited backwards compatibility features

- Upgrading to Chip & PIN was too complex and expensive to complete in one step
- Instead, chip cards continued to have a magstrip
  - Used in terminals without functioning chip readers (e.g. abroad)
  - Act as a backup if the chip failed
- Chip also contained a full copy of the magstrip
  - Simplifies issuer upgrade
  - Chip transactions can be processed by systems designed to process magstrip
- Criminals changed their tactics to exploit these features, and so counterfeit fraud did not fall as hoped
- Fraud against UK cardholders moved outside of the UK

Criminals could now get cash

Criminals collected:

- card details by a “double-swipe”, or tapping the terminal/phone line
- PIN by setting up a camera, tapping the terminal, or just watching

Cloned magstrip card then used in an ATM (typically abroad)

In some ways, Chip & PIN made the situation worse

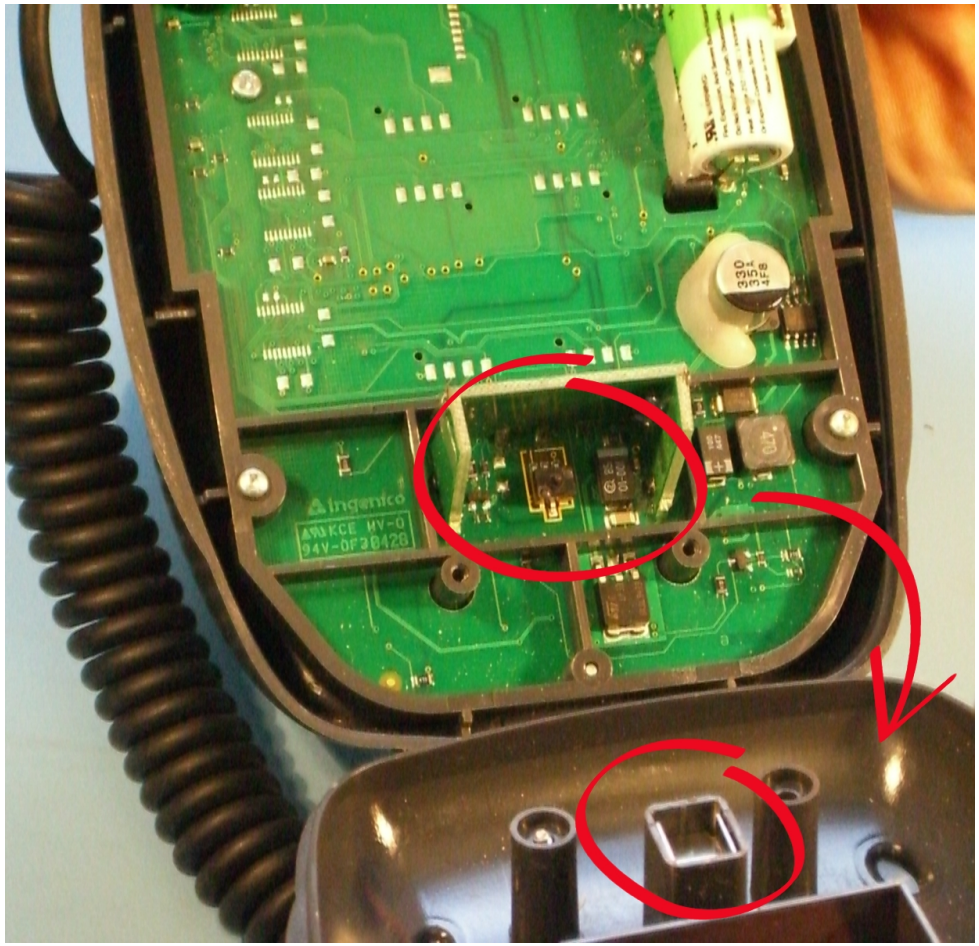
- PINs are used much more often (not just ATM)
- PoS terminals are harder to secure than an ATM

Tonight (ITV, 2007-05-04)

Terminal tamper proofing is supposed to protect the PIN in transit

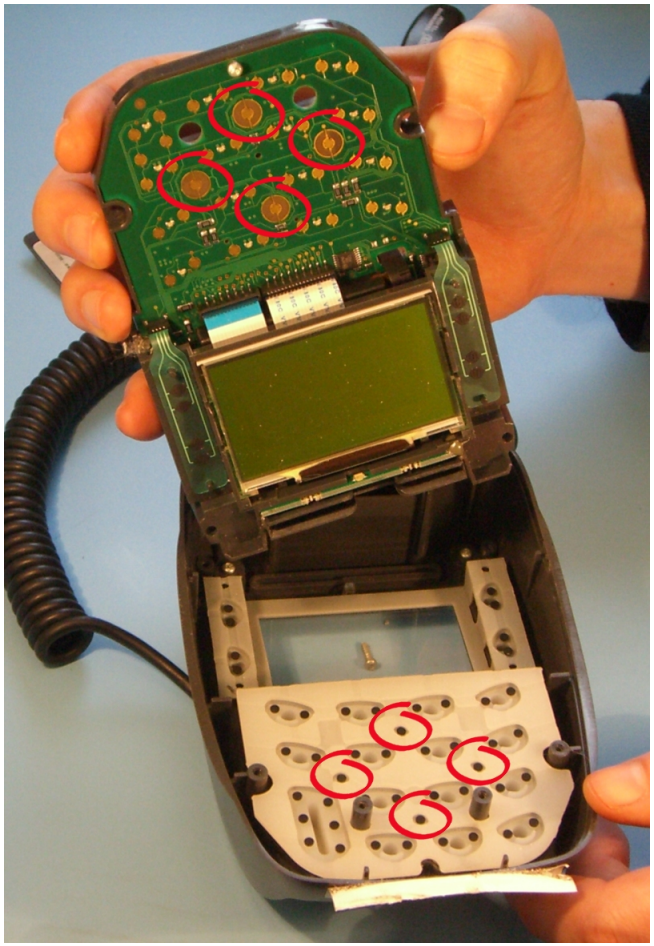
- In PoS transaction, PIN is sent from PIN entry device (PED) to card for verification
- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD $25,000 per PED**

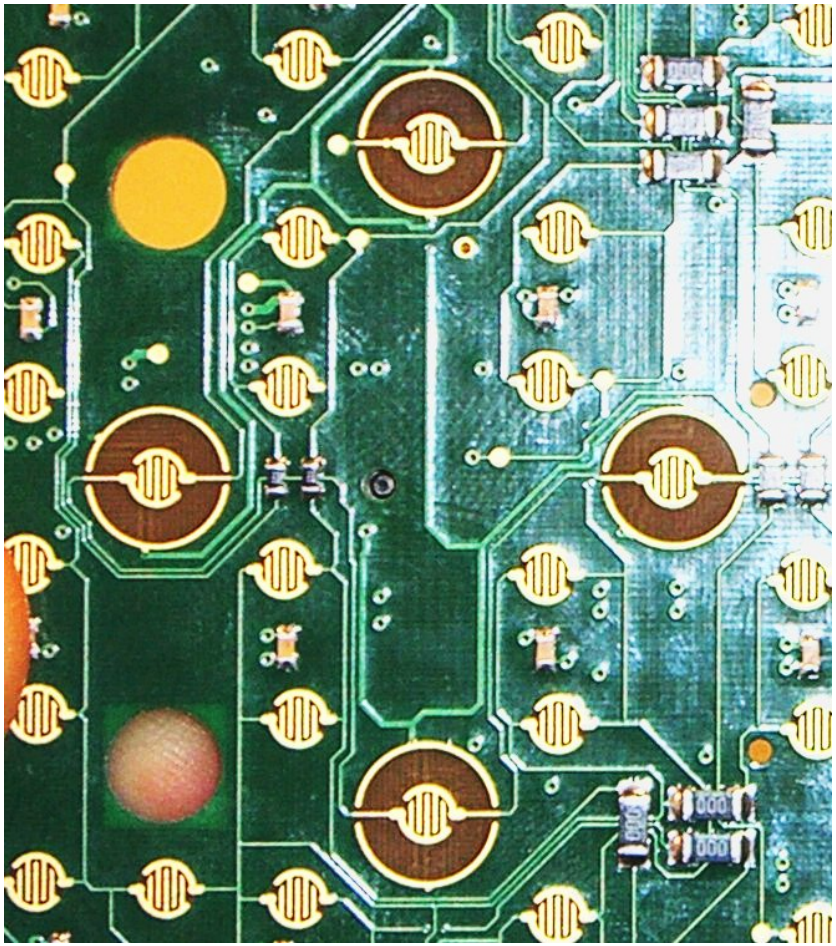
Protection measures: tamper switches



Ingenico i3300

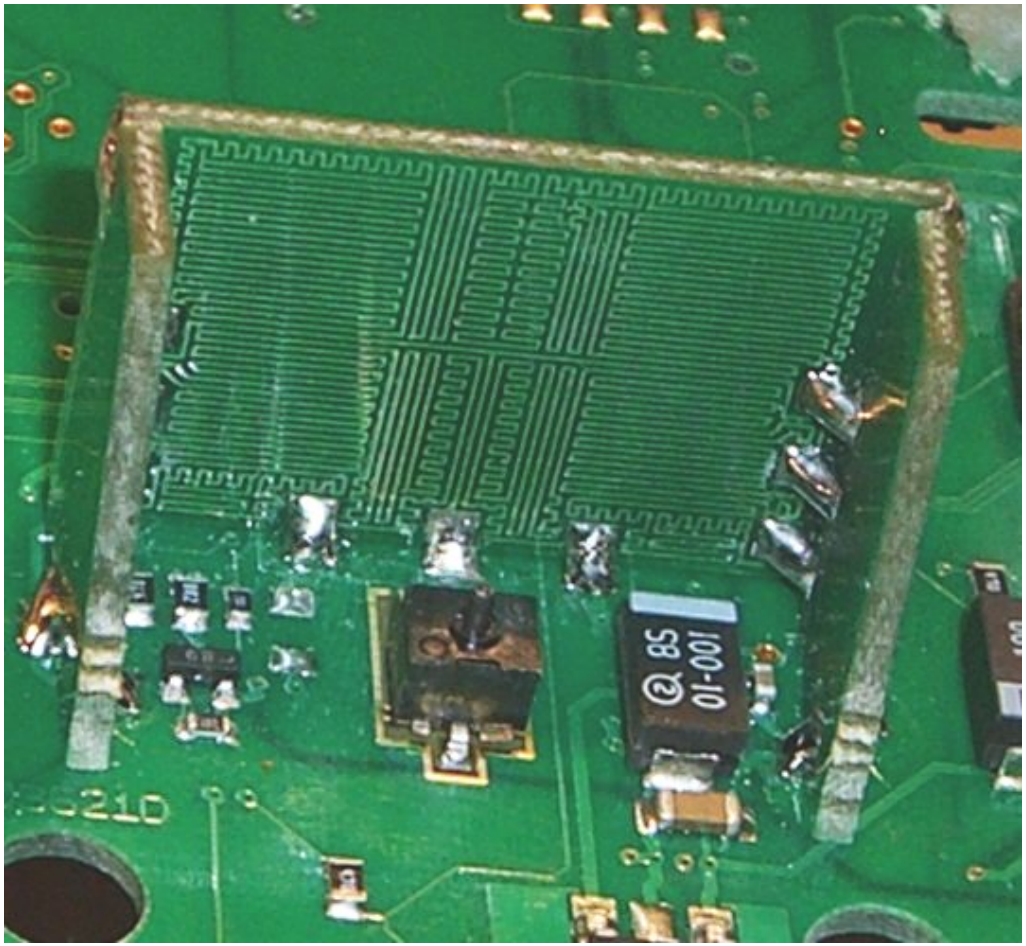
Protection measures: tamper switches

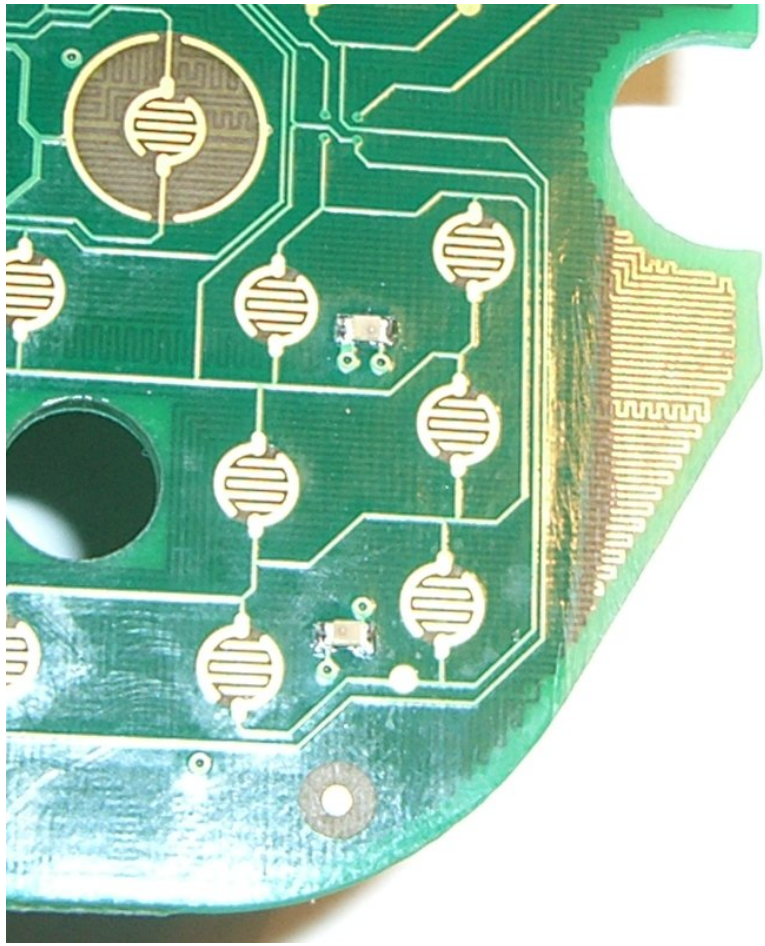




Ingenico i3300

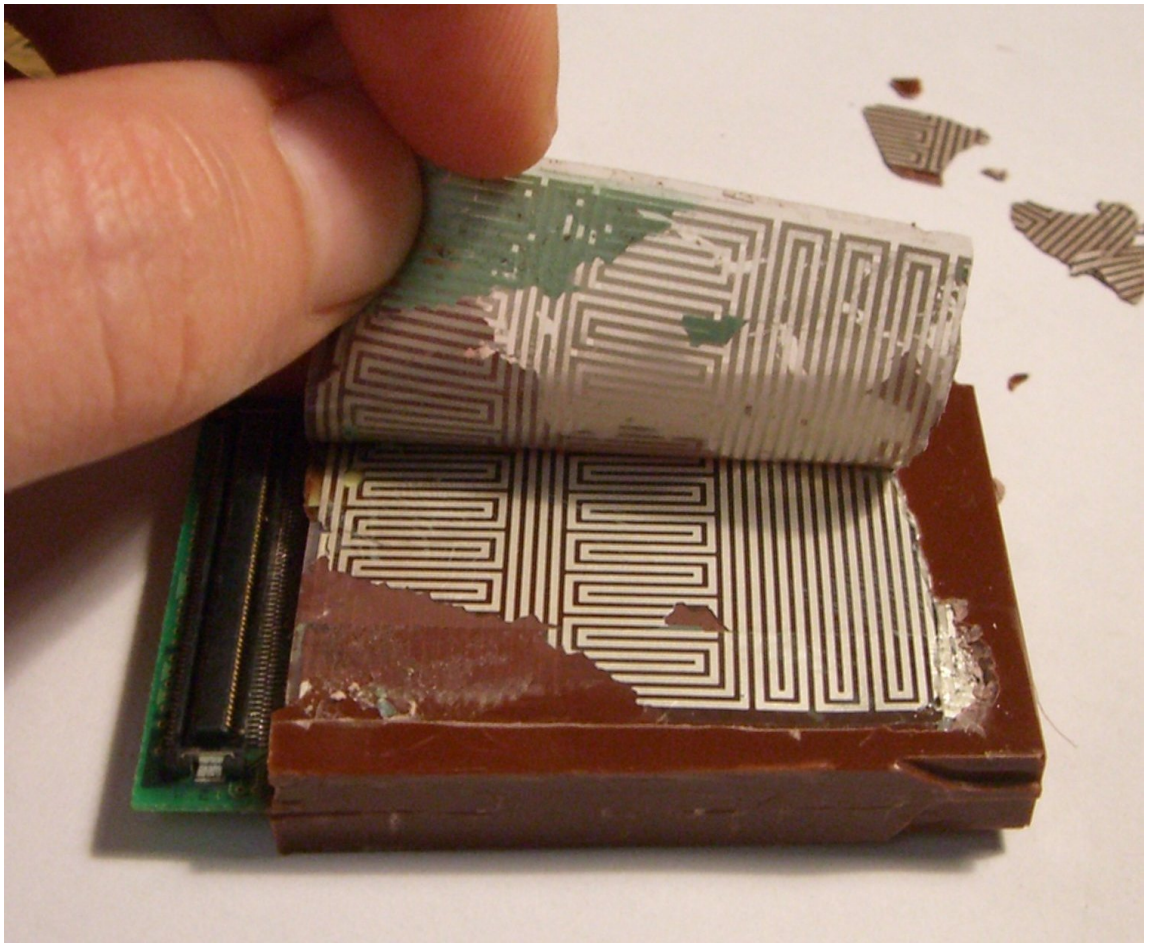
Protection measures: tamper meshes





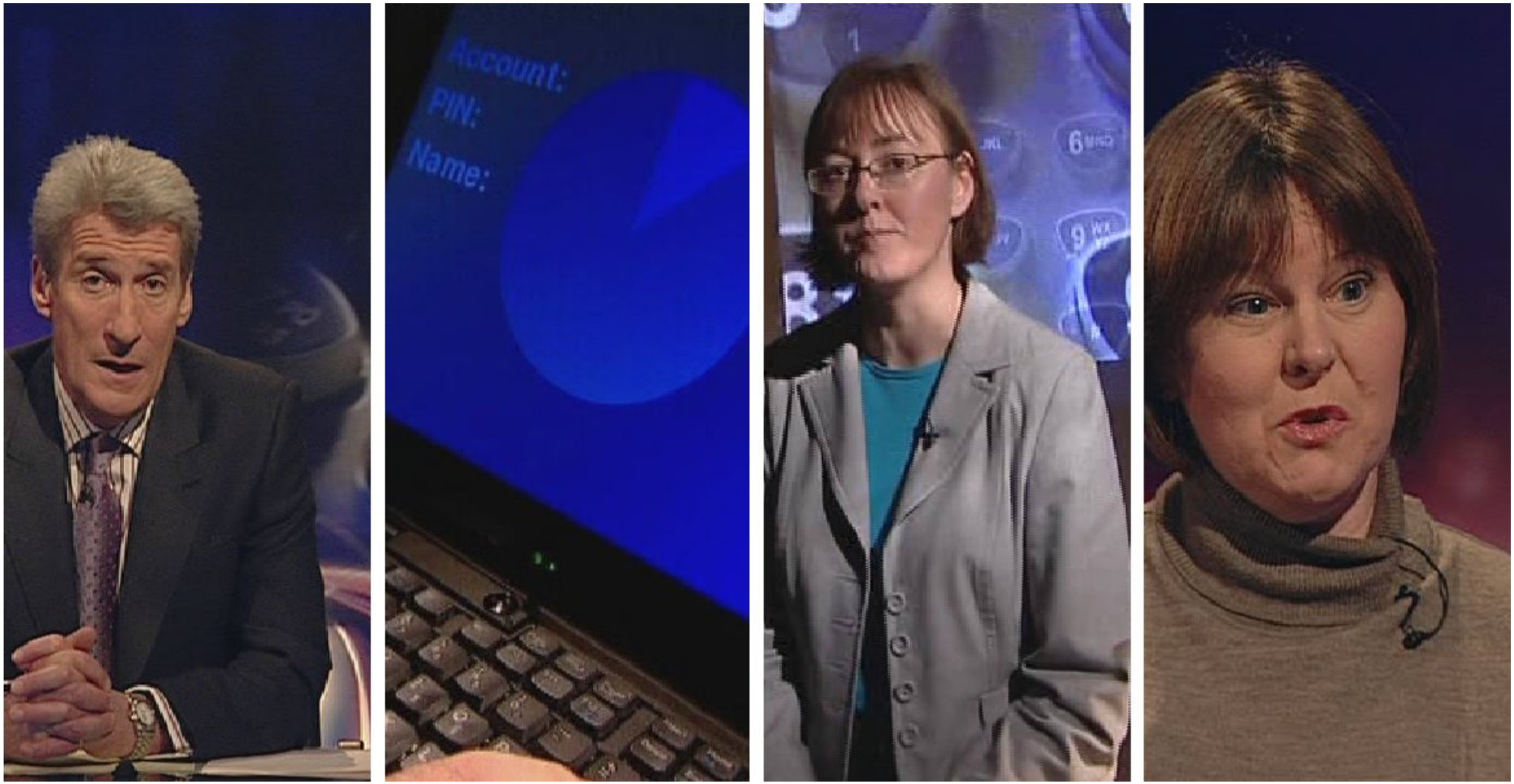
Ingenico i3300

Protection measures: tamper meshes



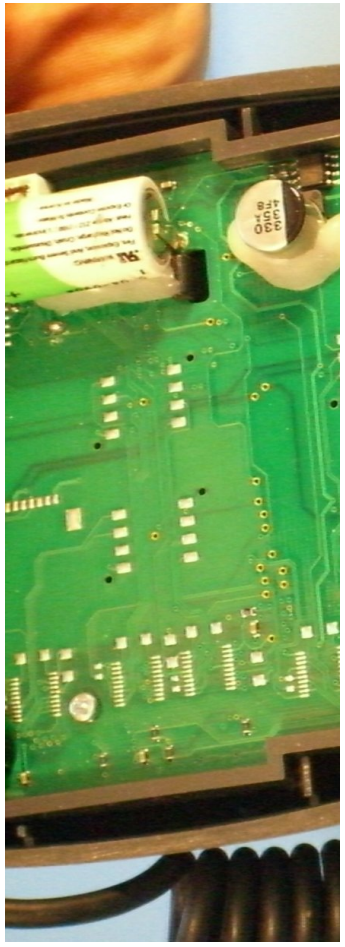
Ingenico i3300

BBC Newsnight filmed our demonstration for national TV



BBC Newsnight, BBC2, 26 February 2008

Holes in the tamper mesh allow the communication line to be tapped



An easily accessible compartment can hide a recording device

This type of fraud is still a serious problem in the UK

Initially (2005), PEDs were tampered on a small scale and installed by someone impersonating a service engineer

PED was collected later, and card details extracted

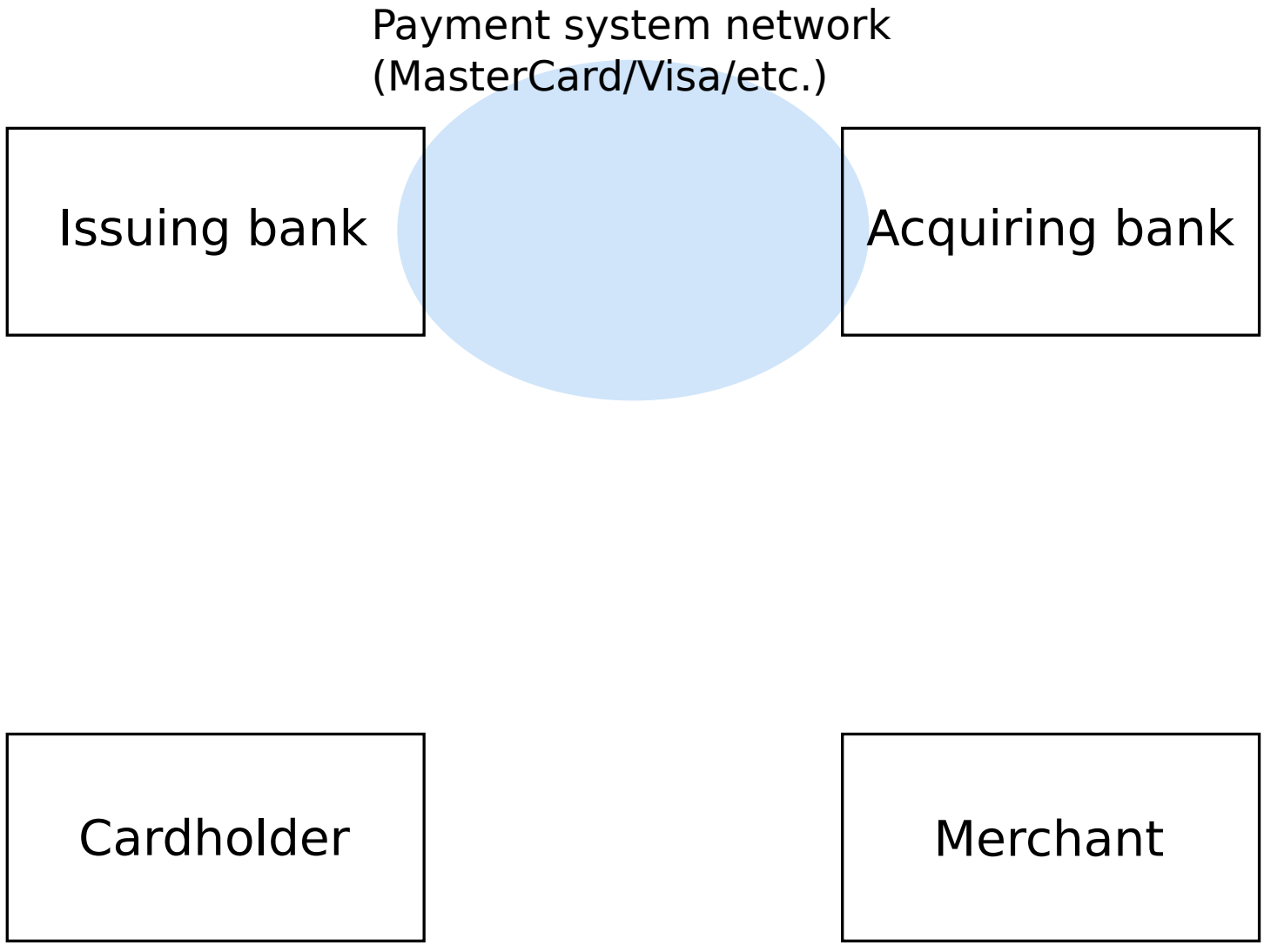
Now PEDs are being tampered with at or near their point of manufacture

A cellphone module is inserted so it can send back lists of card numbers and PINs automatically

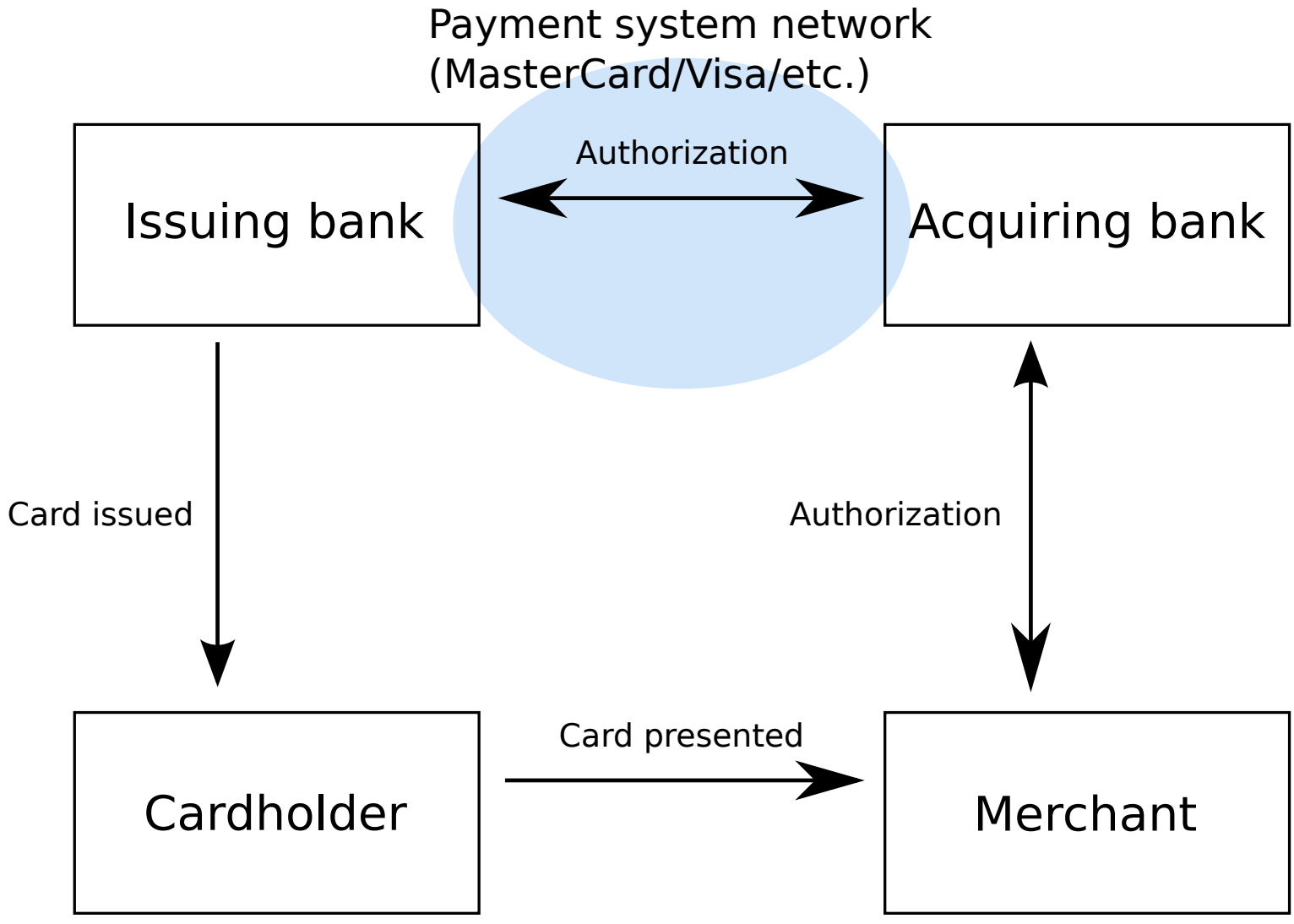
Chip & PIN vulnerabilities

- Fallback vulnerabilities are not strictly-speaking a Chip & PIN vulnerability
- However, vulnerabilities do exist with Chip & PIN
- To understand these, we need some more background information
- To pay, the customer inserts their smart card into a payment terminal
- The chip and terminal exchange information, fulfiling three goals:
  - Card authentication: that the card presented is genuine
  - Cardholder verification: that the customer presenting the card is the authorized cardholder
  - Transaction authorization: that the issuing bank accepts the transaction

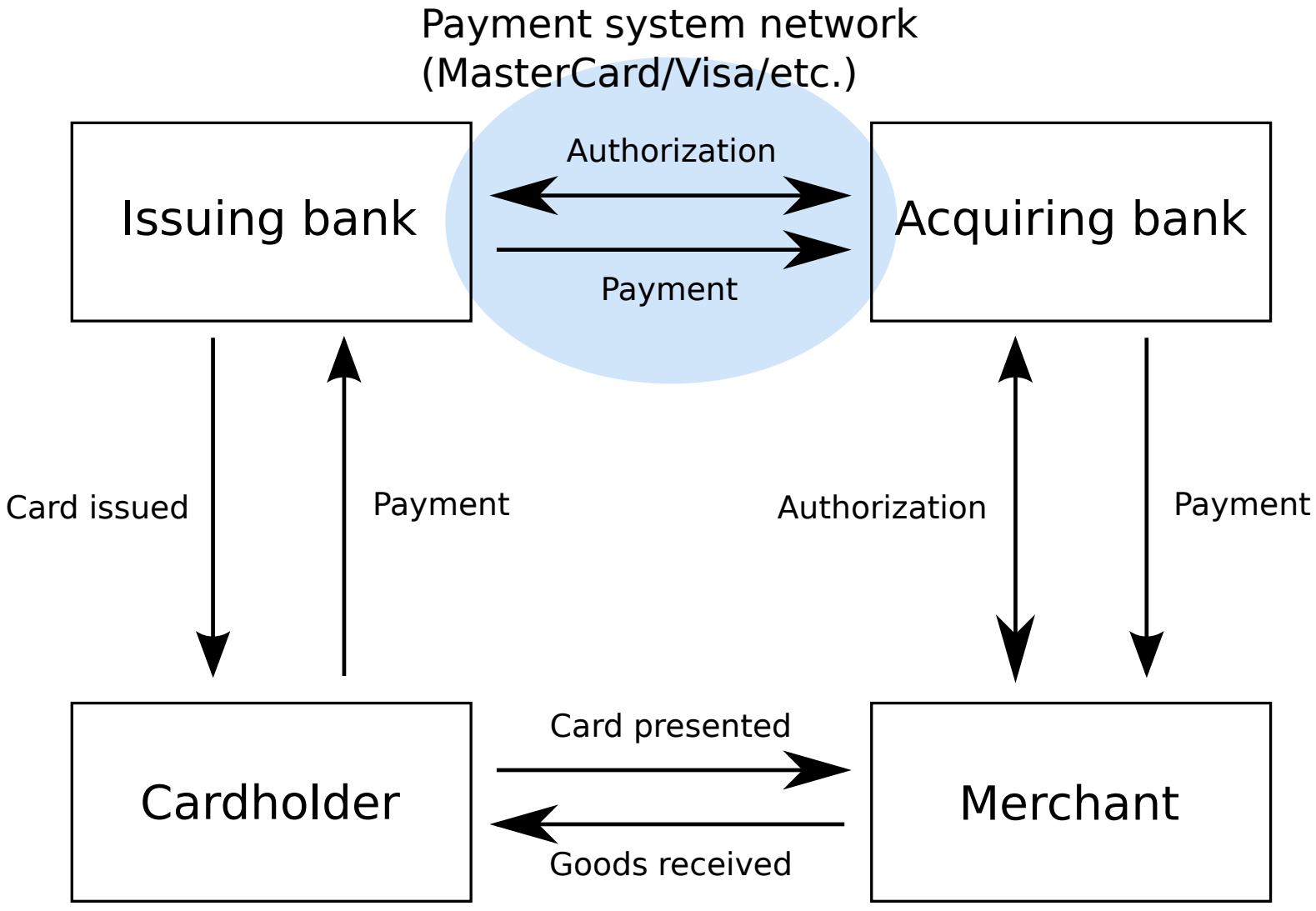
Terminology



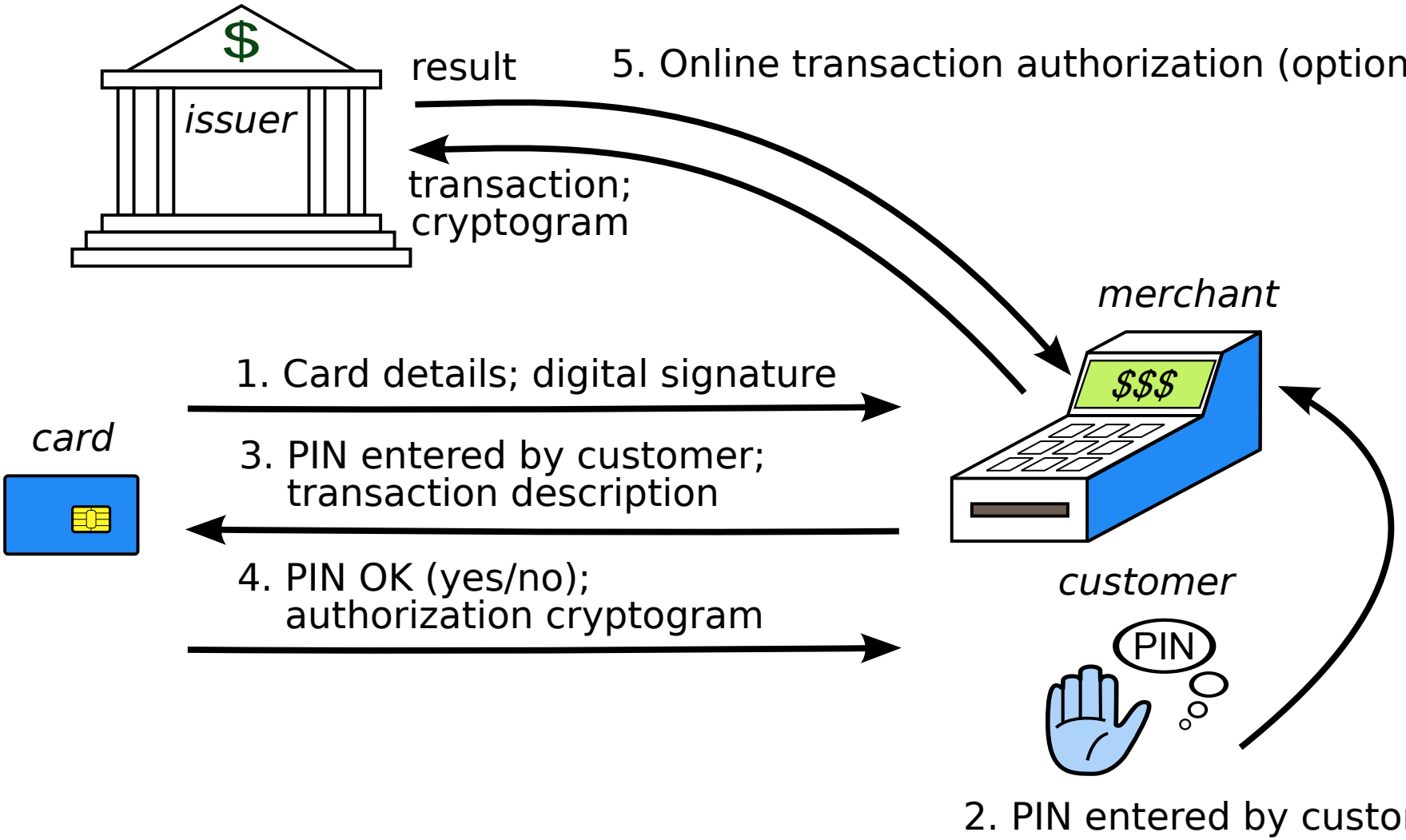
Terminology



Terminology

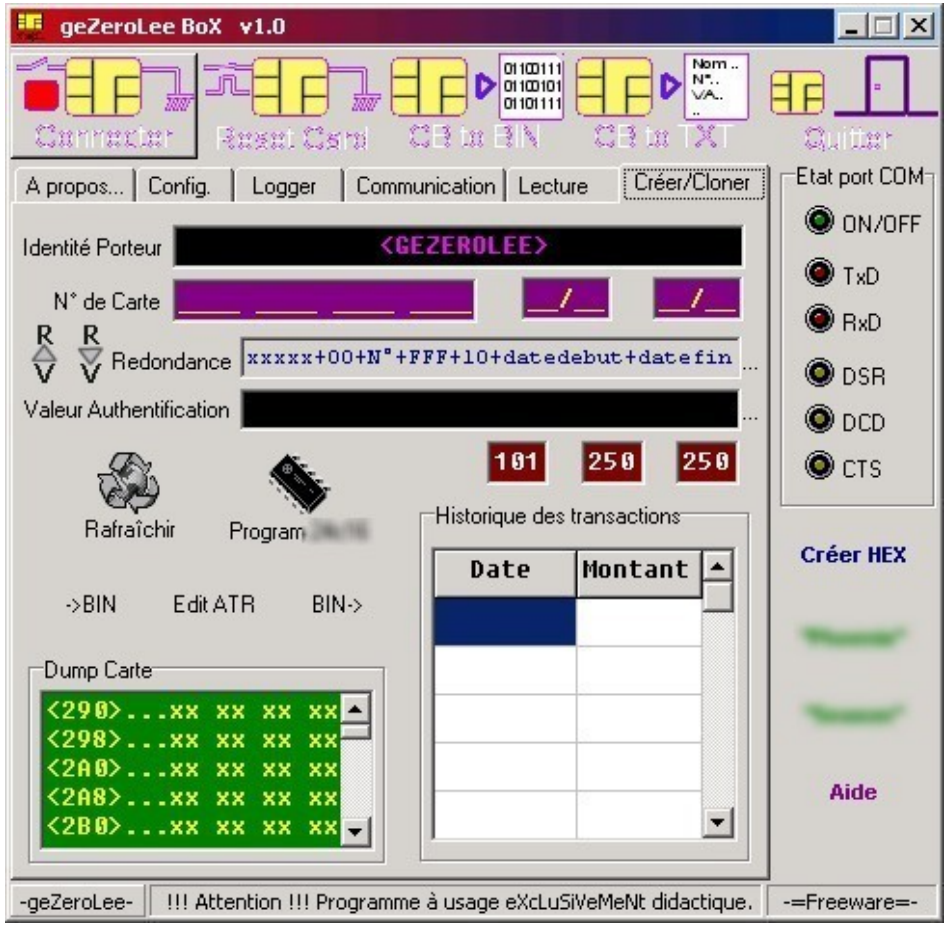


Simplified Chip & PIN transaction



The YES-card attack

- Criminals can copy EMV chip cards
- This fake card will contain the correct digital signature
- Also, it can be programmed to accept any PIN (hence “YES”)
- However, the fake card can be detected by online transaction authorization



The YES-card attack

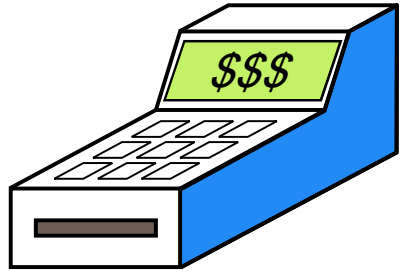
merchant

fake card

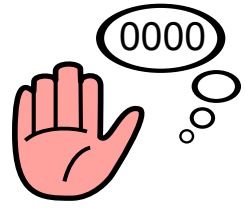
1. Card details; digital signature

3. **Wrong PIN entered by crook;** transaction description

4. **PIN OK (yes); Wrong cryptogram**



crook



2. Wrong PIN entered by crook

Defending against the YES-card

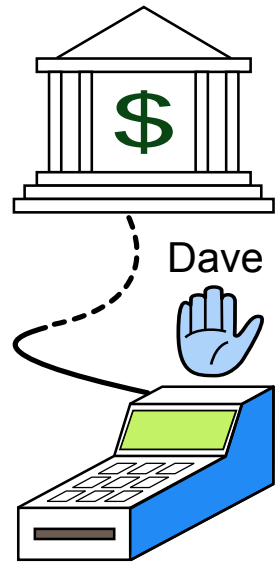
- YES-cards are responsible for a relatively small amount of fraud
- Can be detected by online transaction authorization
- Can also be detected by more advanced chip cards which can produce a dynamic digital signature
  - DDA (dynamic data authentication), as opposed to SDA (static data authentication)
  - Previously DDA cards were prohibitively expensive, but now cost about the same as SDA cards
- PIN verification can be performed online too, rather than allowing the card to do so
  - Need to securely send the PIN back to the issuer
  - UK ATMs use online PIN verification
  - UK point-of-sale terminals use offline PIN verification

Our attack was shown on BBC1's consumer program, which aired February 2007

"We got our highest ratings of the run for the story (6.2 million, making it the most watched factual programme of last week)... it's provoked quite a response from viewers." – Rob Unsworth, Editor, "Watchdog"

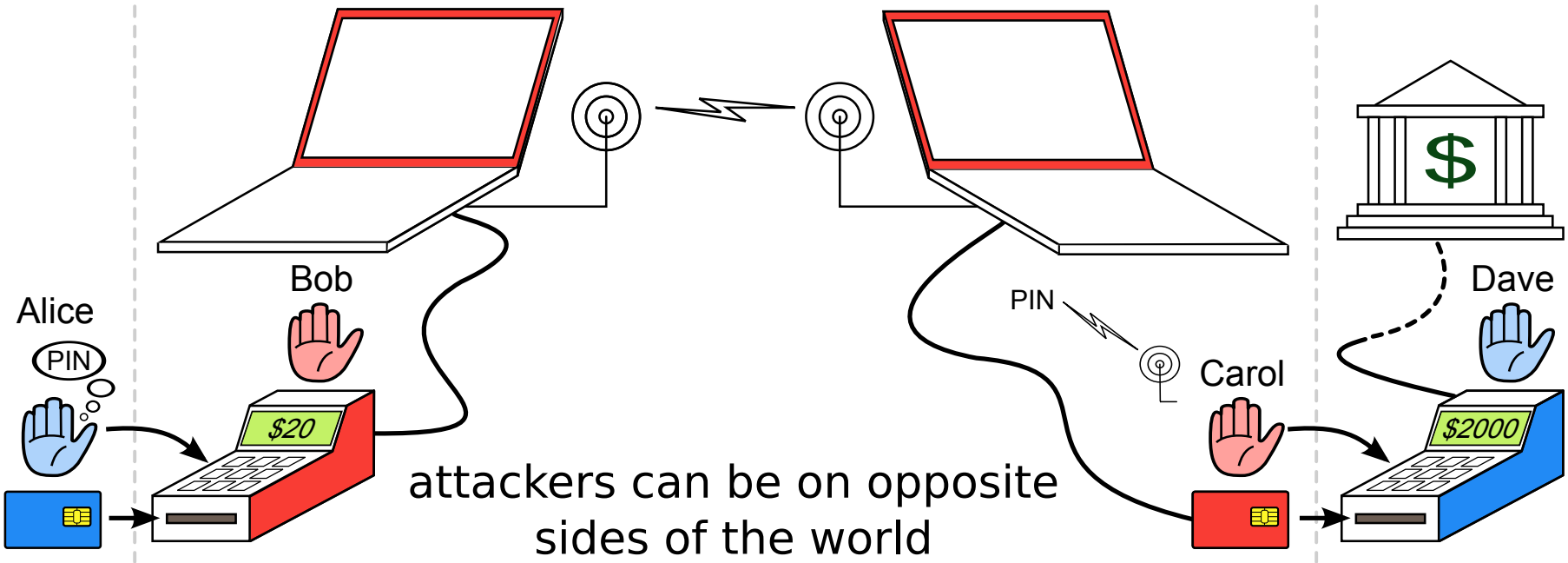
Our demonstration helped many cardholders reach a favourable resolution with banks

The relay attack: Alice thinks she is paying $20, but is actually charged $2 000 for a purchase elsewhere



Honest cardholder Alice and merchant Dave are unwitting participants in the relay attack

The relay attack: Alice thinks she is paying $20, but is actually charged $2 000 for a purchase elsewhere



Alice inserts her card into Bob's *fake* terminal, while Carol inserts a fake card into Dave's *real* terminal. Using wireless communication the $2 000 purchase is debited from Alice's account

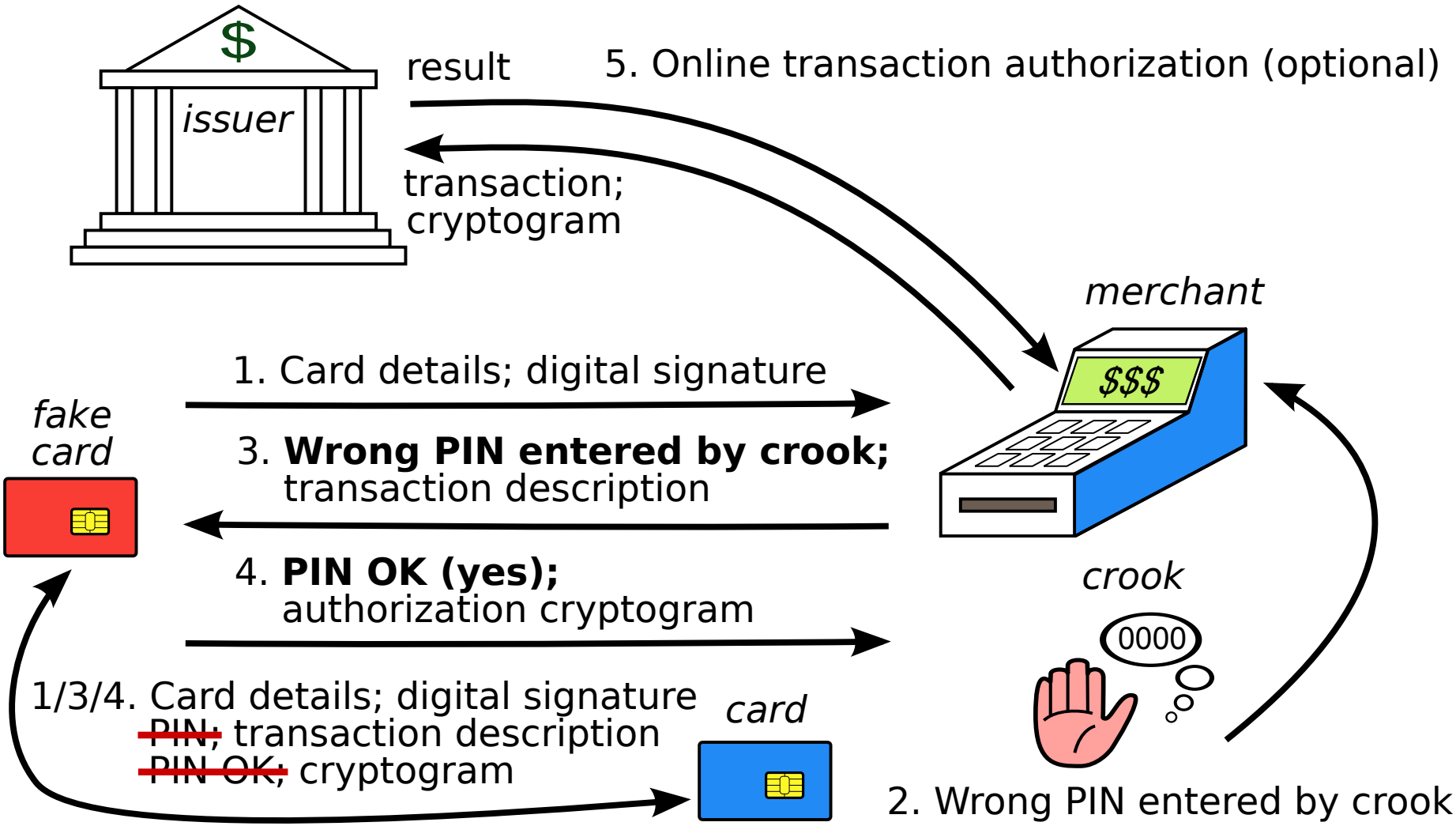
The no-PIN attack

- The no-PIN attack allows criminals to use a stolen card without knowing its PIN
- It requires inserting a device between the genuine card and payment terminal
- This attack works even for online transactions, and DDA cards

BBC Newsnight filmed our demonstration for national TV

BBC Newsnight, BBC2, 11 February 2010

The no-PIN attack



Why does this attack work?

- Complexity
  - 4 000 pages of specification!
  - Data needs to be combined from several different sources and specifications (EMV, MasterCard, ISO, APACS)
  - Despite quantity, no specification actually describes the necessary checks
- Bad design of ags
  - Card produces a ag (card verification results CVR) which says whether PIN verification succeeded
  - But this ag is in an issuer-specific format and so cannot be parsed by the terminal
  - Flag produced by terminal (TVR) is set either if PIN verification succeeded or terminal skipped check
  - Other ags may exist (country-specific, covered by APACS and ISO), but evidently are not checked in practice
- Implementation problems
  - Since issuers dont check ags, terminals mis-report state

Current and proposed defences

- Skimming
  - iCVV: Slightly modifying copy of magnetic strip stored on chip
  - Disabling fallback: Preventing magnetic strip cards from being used in EMV-enabled terminals
  - Better control of terminals: Prevent skimmers from being installed
- YES-card
  - Dynamic Data Authentication (DDA): Place a public/private keypair on every card
  - Online authorization: Require that all transactions occur online
- No-PIN attack
  - Defences currently still being worked on
  - Extra consistency checks at issuer may be able to spot the attack
  - Combined DDA/Application Cryptogram Generation (CDA): Move public key authentication stage to the end

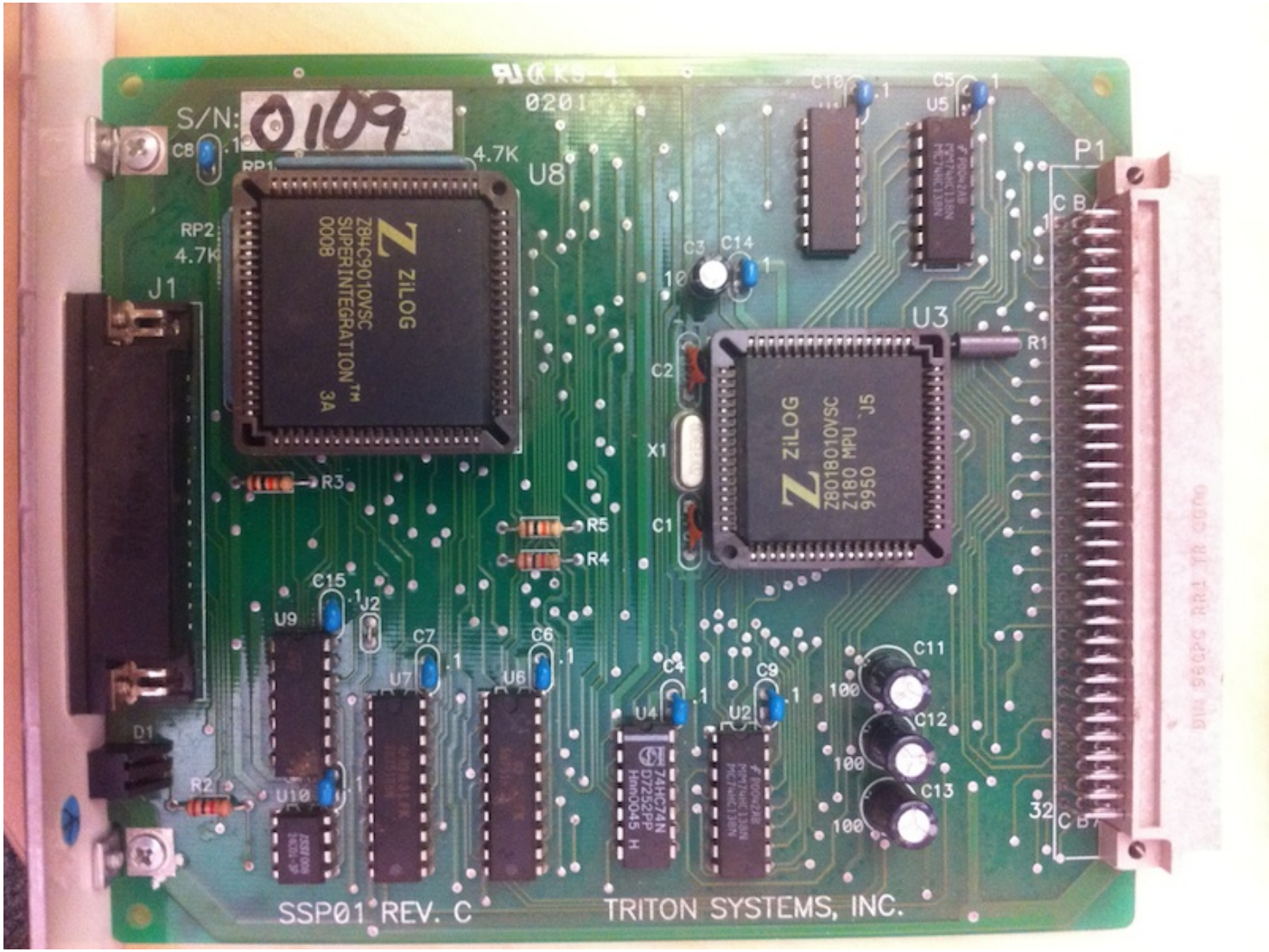
Random numbers?

Date	Time	UN
2011-06-29	10:37:24	`F1246E04`
2011-06-29	10:37:59	`F1241354`
2011-06-29	10:38:34	`F1244328`
2011-06-29	10:39:08	`F1247348`

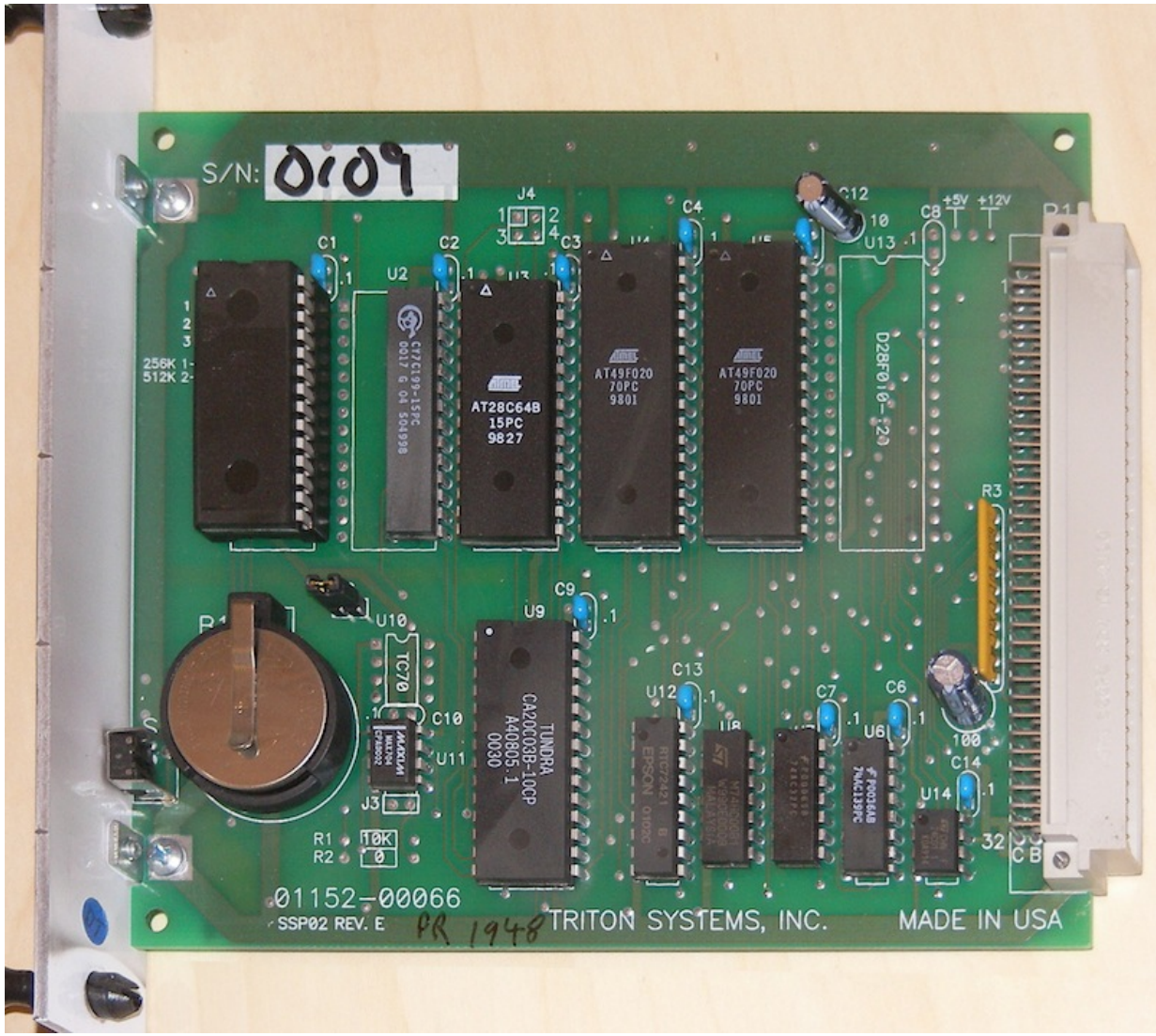
Reverse engineering

NCR ATM

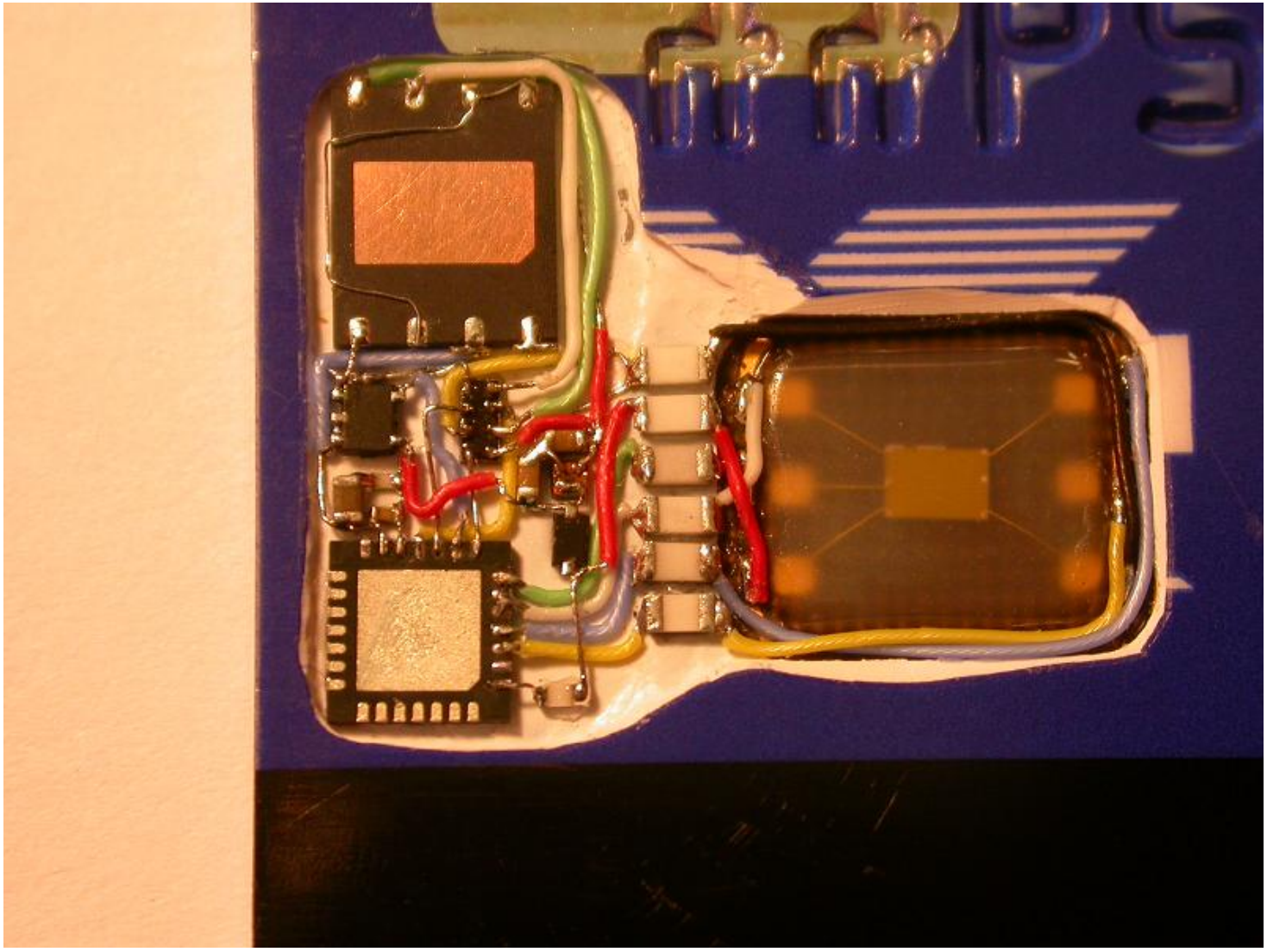
Triton ATM (CPU board)



Triton ATM (DES board)



Surveying the problem



Characteristic C

SRC2 EXP6		SRC2 EXP6B	
0	77028437	0	5D01BBCF
1	0D0AF8F9	1	760273FE
2	5C0E743C	2	730E5CE7
3	4500CE1A	3	380CA5E2
4	5F087130	4	580E9D1F
5	3E0CB21D	5	6805D0F5
6	6A05BAC3	6	530B6EF3
7	74057B71	7	4B0FE750
8	76031924	8	7B0F3323
9	390E8399	9	630166E1

Other ATMs

Counters		Weak RNGs	
ATM4	`eb661db4`	ATM1	`690d4df2`
ATM4	`2cb6339b`	ATM1	`69053549`
ATM4	`36a2963b`	ATM1	`660341c7`
ATM4	`3d19ca14`	ATM1	`5e0fc8f2`
ATM5	`F1246E04`	ATM2	`6f0c2d04`
ATM5	`F1241354`	ATM2	`580fc7d6`
ATM5	`F1244328`	ATM2	`4906e840`
ATM5	`F1247348`	ATM2	`46099187`
		ATM3	`650155D7`
		ATM3	`7C0AF071`
		ATM3	`7B021D0E`
		ATM3	`1107CF7D`

POS terminal

Stronger RNGs	
POS1	013A8CE2
POS1	01FB2C16
POS1	2A26982F
POS1	39EB1E19
POS1	293FBA89
POS1	49868033

Cashing out

- Pre-play card: load with cryptograms for expected UNs
- Malware attack: tamper with ATM or POS terminal to produce predictable UNs
- Tamper with ATMs or POS in supply chain
- Collusive merchant, modifies software
- Tamper with communications

Mitigating the attack

- Detection:
  - Suspicious jumps in transaction counter
  - Lack of issuer authentication
- Prevention:
  - Relying party (issuer) generates the UN
  - Audit trail shows where UNs came from
- Industry response so far has been mixed
  - Details disclosed in early 2012
  - Some surprised by the problem
  - Others less so
  - Some knew of this problem but did not admit it

More information: “Chip and Skim: cloning EMV cards with the pre-play attack”, arXiv:1209.2531

Conclusions

Systems based on EMV are open to a variety of attacks

- While the specification does not forbid implementing resistance measures, it offers little help
- In practice, implementers have slipped up, and customers have been left liable
- EMVs complexity, and large variety of options are particularly problematic
- In particular, not specifying security checks, and making essential data items optional, are a fundamental problem of EMV
- While the specification could be patched to fix the particular vulnerabilities identified, fixing the systemic problems needs a re-write of the protocol and specification
- For online banking, transaction authentication is now essential, which requires a trustworthy display

More: `http://www.cl.cam.ac.uk/research/security/banking/`