TECHNISCHE UNIVERSITÄT DRESDEN

**Faculty of Computer Science** Institute for System Architecture, Operating Systems Group

# Chip and PIN is broken

Steven Murdoch, Saar Drimer, Ross Anderson, Mike Bond

# Europay – Mastercard – Visa (EMV)

- 730 million cards worldwide
- Solution to all the banks' problems:
  - Chip to prevent copying of a card
  - PIN to prevent abuse of stolen cards
- PIN to prove customer's liability

# Card Fraud in the UK

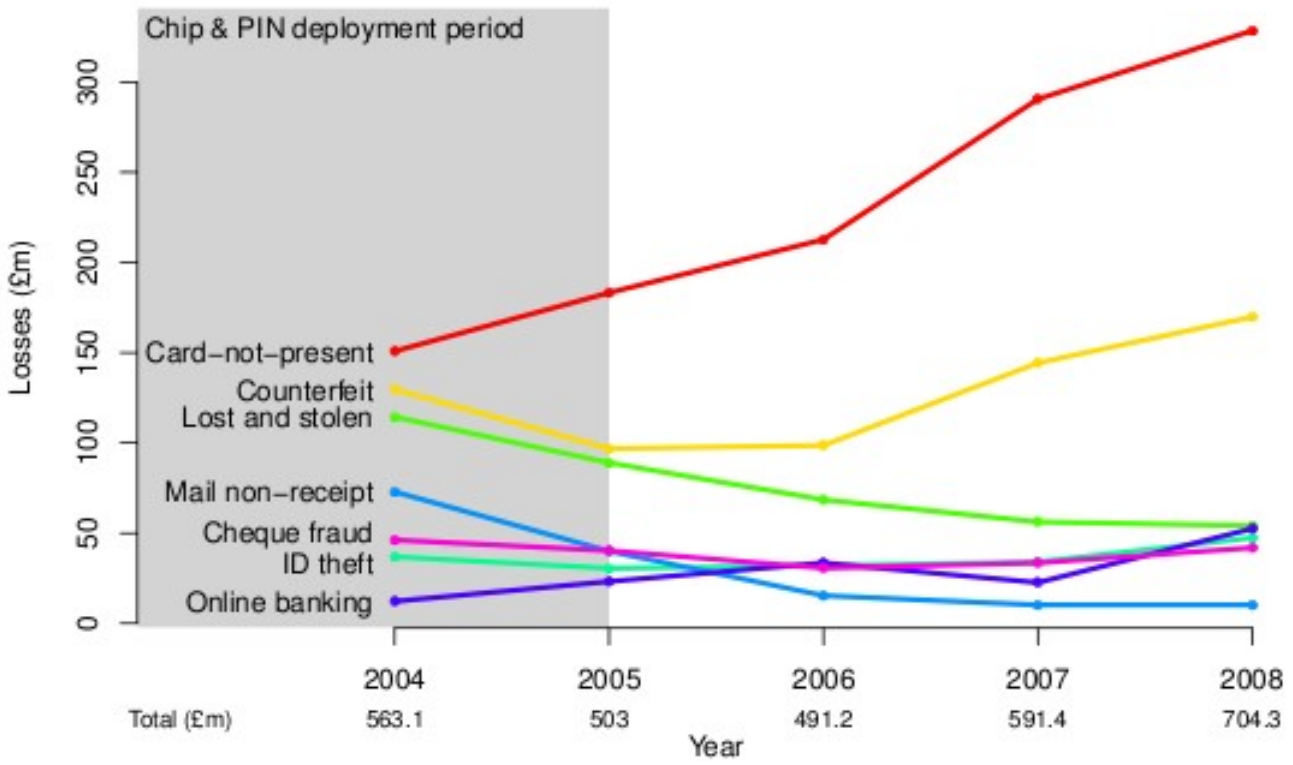



Figure 1. Fraud statistics on UK-issued cards [6]

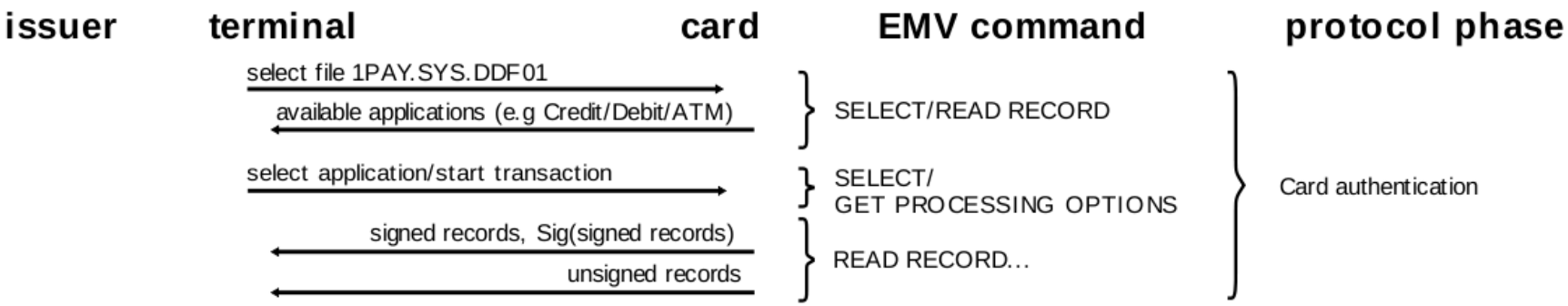
# PIN and Chip protocol from 10,000 ft

1. Card authentication
   → prove that card is correct

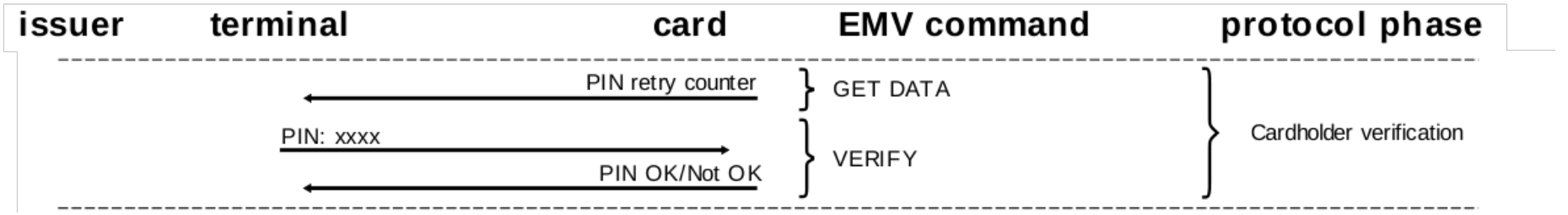
2. Cardholder verification
   → prove that customer owns the card

3. Transaction authorization
   → prove that transaction is valid

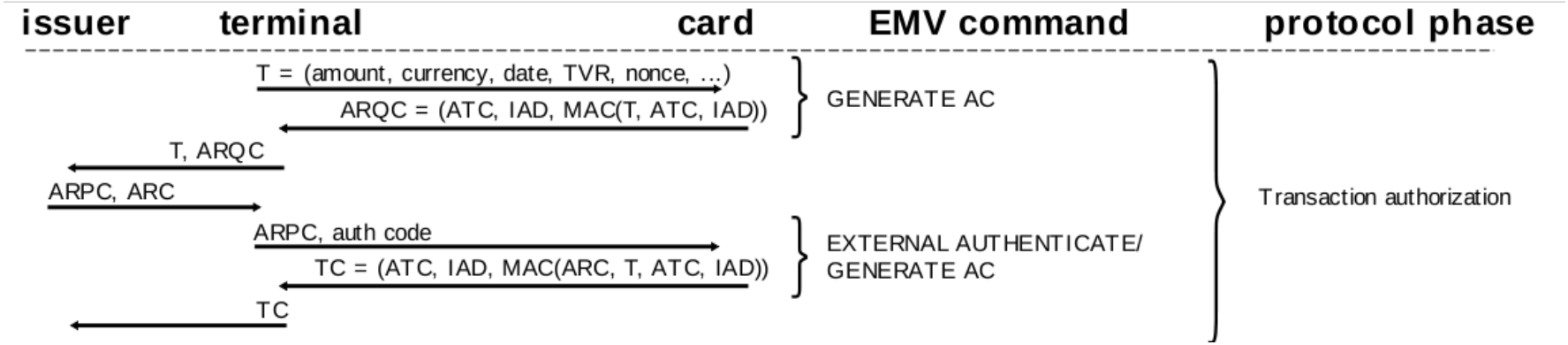
# Card authentication



# Cardholder verification



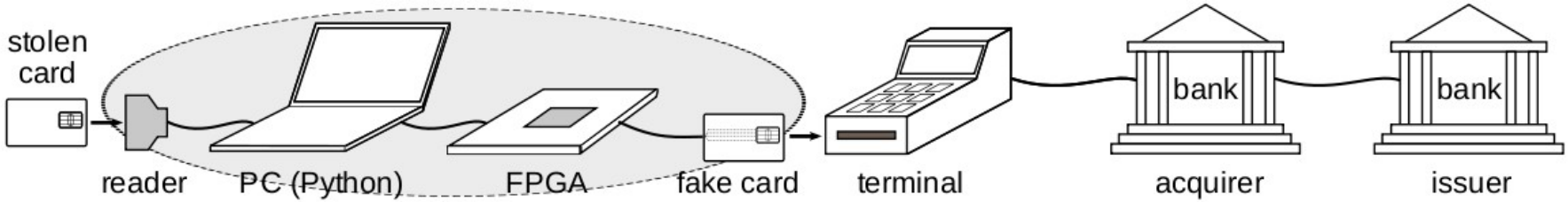
# Transaction authentication

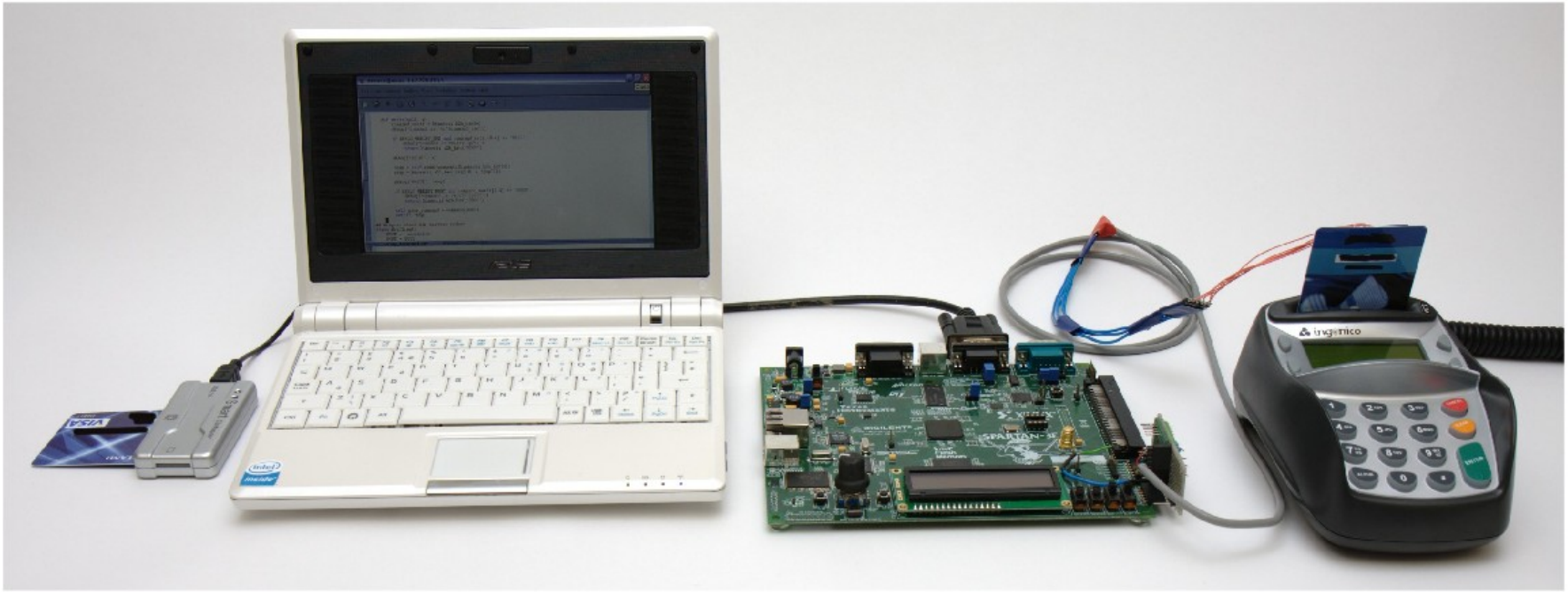


# The attack

- TVR only records auth failures
- IAD may contain info about PIN auth used
  - Issuer-specific, terminal cannot check
- MITM: intercept PIN request and send 0x9000 to terminal
- Result:
  - Terminal: PIN ok
  - Card: PIN never requested
  - Bank: no TVR failure, no PIN auth

# Hardware used



# What caused the vulnerability?

- Closed protocol specification process
- Huge spec
  - 707 pages for core EMV spec
  - 2,126 pages testing documentation
  - 810 pages VISA public extensions
- No documentation of threat / security model

# Fixes?

- Economic factor:
  - Customers can be held liable
  - No incentive for costly redeployment
  - Cooperation of banks and terminal vendors
- Let terminal parse IAD
  - As the name says: **issuer**-specific data
- Incorporate Cardholder Verification Method Results into ARQC
  - Possible with EMV, requires only cards and issuer backends to be fixed
  - Will stil take a long time

# Discussion

- How to educate the uneducated?
- Is there formal protocol validation?
  - Would it have helped?