Payment system governance – security economics at large

Ross Anderson
Cambridge
Payment Systems

• Early modern period: merchant bankers carried risks of financing trade
• 19th century: industrialised by letters of credit, insurance certificates, bills of lading, inspection certificates, the telegraph
• People could do business with remote merchants
• Late 20th century: the Internet and credit cards
• Would the banks earn lots as the trust provider?
A Natural Experiment

• Stronger US consumer protection
  – Judd v Citibank 1980
  – Reg E
• Weaker UK consumer protection
  – McConville et al v Barclays et al 1993
  – Banking code, Financial Ombudsman Service
• Other countries spread out: F, De, E, ZA …
• Payment Services Directive trying to harmonise
• Some system issues becoming clear
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 in the UK since EMV

Chip & PIN deployment period

Card–not–present
Counterfeit
Lost and stolen
Mail non–receipt
Check fraud
ID theft
Online banking

Losses (£m)

Total (£m)
2004: 563.1
2005: 503
2006: 491.2
2007: 591.4
2008: 704.3

Year
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
- Evaluations follow Common Criteria
- Should cost $25,000 per PED to defeat
Security economics

- Acquirers and issuers have different incentives
- PEDs ‘evaluated under the Common Criteria’ were trivial to tap
- Banks said in Feb 08 it wasn’t a problem…
- By July 2008 we saw tampered PEDs coming from the factory!
The ‘No PIN’ attack

- This attack lets crooks use a stolen card without knowing the pin
- We insert a device between card & terminal
- Card thinks: signature; terminal thinks: pin
- Works even for online transactions (and DDA)
Exposed on TV

Newsnight, BBC2, Feb 11 2010
A normal EMV transaction

1. Card details; digital signature
2. PIN entered by customer
3. PIN entered by customer; transaction description
4. PIN OK (yes/no); authorization cryptogram
5. Online transaction authorization (optional)
A ‘No-PIN’ transaction

1. Card details; digital signature
2. Wrong PIN entered by crook
3. Wrong PIN entered by crook
4. PIN OK (yes); authorization cryptogram
5. Online transaction authorization (optional)

- issuer
- merchant
- crook
- fake card
- card
- result
Blocking the ‘No PIN’ attack

- The card tells the issuer ‘signature used’ while the terminal tells the acquirer ‘pin used’
- In theory: might block at terminal, acquirer, issuer
- In practice: may have to be the issuer (as with terminal tampering, acquirer incentives are poor)
- Tactical problem: messages get mangled!
- Real problem: EMV spec now vastly too complex
- With 100+ vendors, 20,000 banks, millions of merchants … a tragedy of the commons
Regulators and Fraud

• Regulators were too ready to believe bank assurances about credit risk management
• There is a similar problem with operational security risk management
• Wherever regulators let them, banks are dumping the risk of fraud on customers – merchants and cardholders – and even on each other
• This is starting to create systemic risk
• What’s the optimal regulatory approach?
Payment research topics?

• Interesting case histories?
  – Korean online banking, CAP, proceeds of crime, …

• How to align incentives, foster innovation?
  – Cap interchange fees?
  – Do something about compliance costs?
  – Level the playing field for paypal, facebook,…?
  – Open standards?
  – Managed upgrade cycle for noncompetitive platforms?
  – Other governance routes?