Crypto protocols

ACS R209: Computer Security –
Principles and Foundations
Ross Anderson

Security Protocols

- Security protocols are the intellectual core of security engineering
- They are where cryptography and system mechanisms meet
- They allow trust to be taken from where it exists to where it's needed
- But they are much older than computers…

Real-world protocol

- Ordering wine in a restaurant
  - Sommelier presents wine list to host
  - Host chooses wine; sommelier fetches it
  - Host samples wine; then it's served to guests
- Security properties?

Real-world protocol

- Ordering wine in a restaurant
  - Sommelier presents wine list to host
  - Host chooses wine; sommelier fetches it
  - Host samples wine; then it's served to guests
- Security properties
  - Confidentiality – of price from guests
  - Integrity – can't substitute a cheaper wine
  - Non-repudiation – host can't falsely complain

Car unlocking protocols

- Principals are the engine controller E and the car key transponder T
- Static ($T \rightarrow E$: KT)
- Non-interactive

  $T \rightarrow E$: T, $\{T,N\}_{KT}$
- Interactive

  $E \rightarrow T$: N

  $T \rightarrow E$: $\{T,N\}_{KT}$
- N is a ‘nonce’ for ‘number used once’. It can be a sequence number, a random number or a timestamp

Two-factor authentication

$S \rightarrow U$: N

$U \rightarrow P$: N, PIN

$P \rightarrow U$: $\{N, PIN\}_{KP}$

Key management protocols

- Suppose Alice and Bob each share a key with Sam, and want to communicate?
  - Alice calls Sam and asks for a key for Bob
  - Sam sends Alice a key encrypted in a blob only she can read, and the same key also encrypted in another blob only Bob can read
  - Alice calls Bob and sends him the second blob
- How can they check the protocol's fresh?

Needham-Schroder

- 1978: uses ‘nonces’ rather than timestamps

  $A \rightarrow S$: A, B, NA

  $S \rightarrow A$: $\{NA, B, K_{AB}, \{K_{AB}, A\}_{KBS}\}_{KAS}$

  $A \rightarrow B$: $\{K_{AB}, A\}_{KBS}$

  $B \rightarrow A$: $\{NB\}_{KAB}$

  $A \rightarrow B$: $\{NB - 1\}_{KAB}$

- The bug, and the controversy…

Identify Friend or Foe (IFF)

- Basic idea: fighter challenges bomber

  $F \rightarrow B: N$

  $B \rightarrow F: \{N\}_K$

- What can go wrong?

Identify Friend or Foe (IFF)

- Basic idea: fighter challenges bomber

  $F \rightarrow B$: N

  $B \rightarrow F$: $\{N\}_K$

- What if the bomber reflects the challenge back at the fighter's wingman?

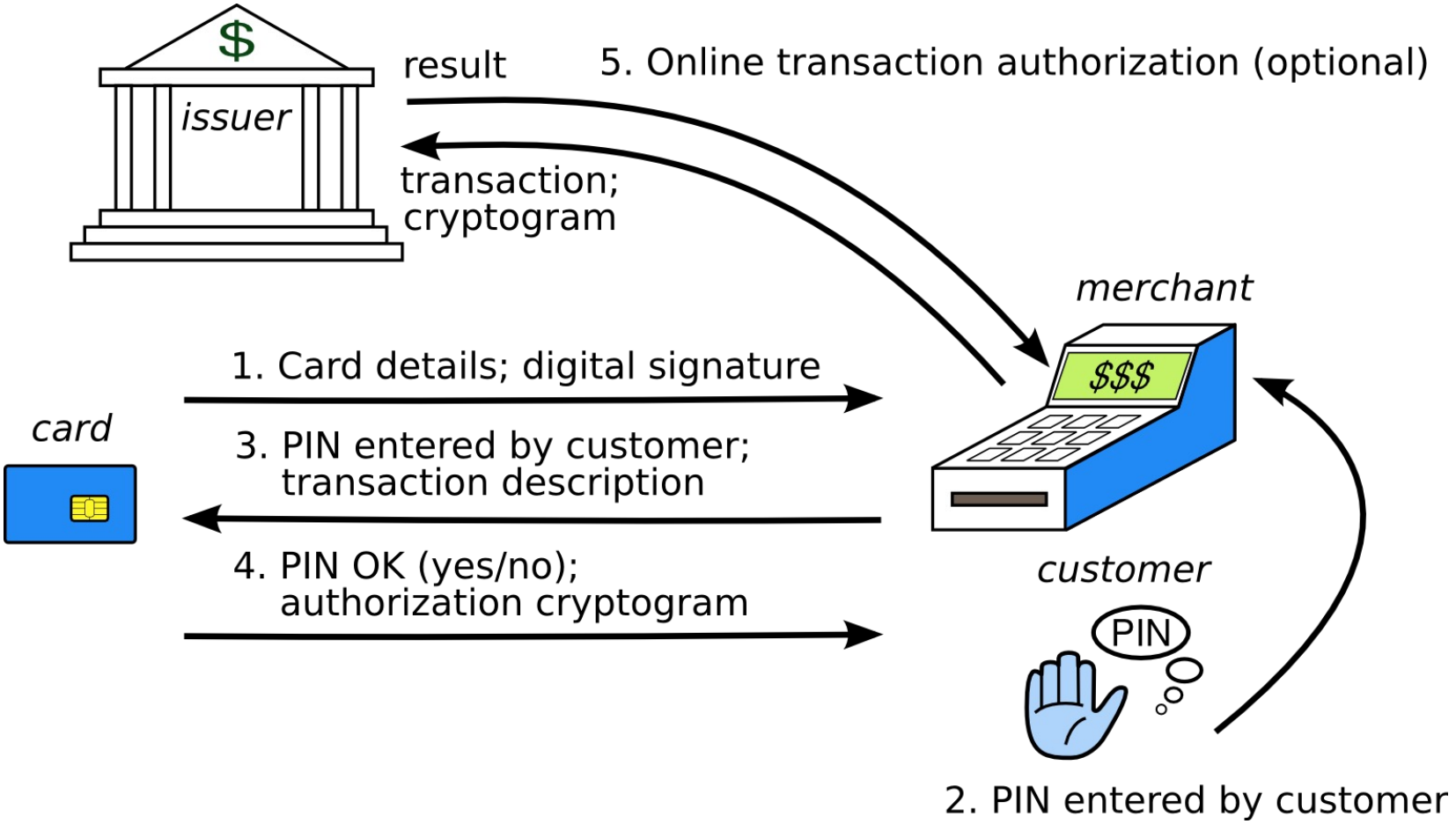
  $F \rightarrow B$: N

  $B \rightarrow F$: N

  $F \rightarrow B$: $\{N\}_K$

  $B \rightarrow F$: $\{N\}_K$

A normal EMV transaction



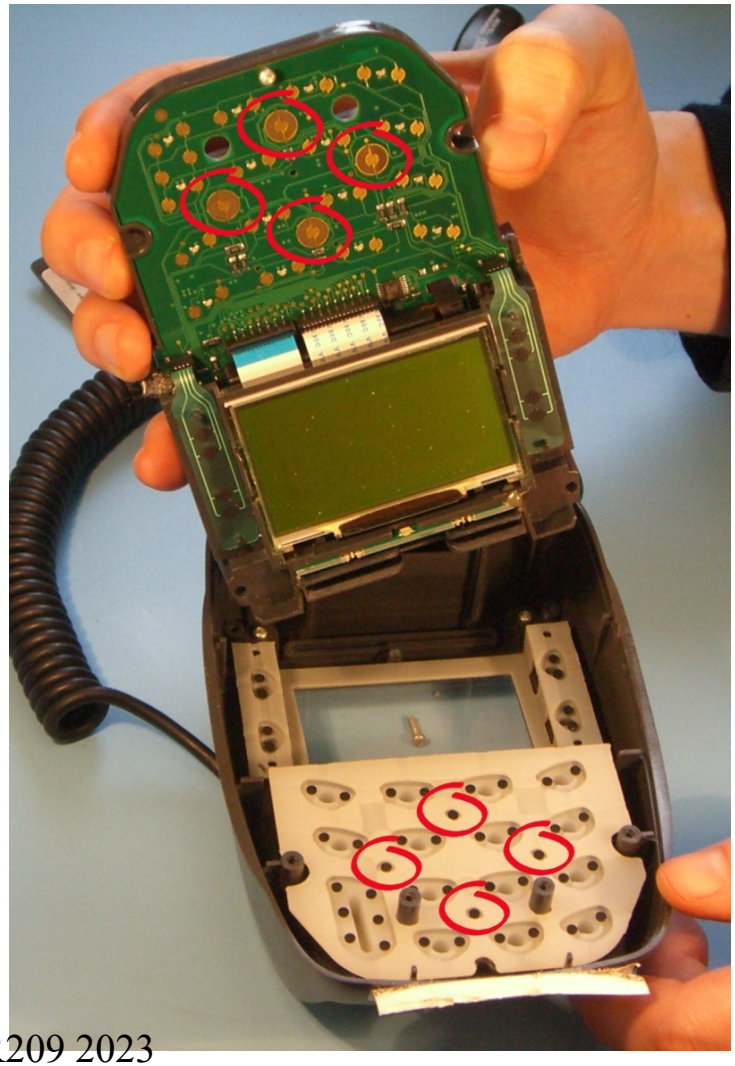
What about a false terminal?

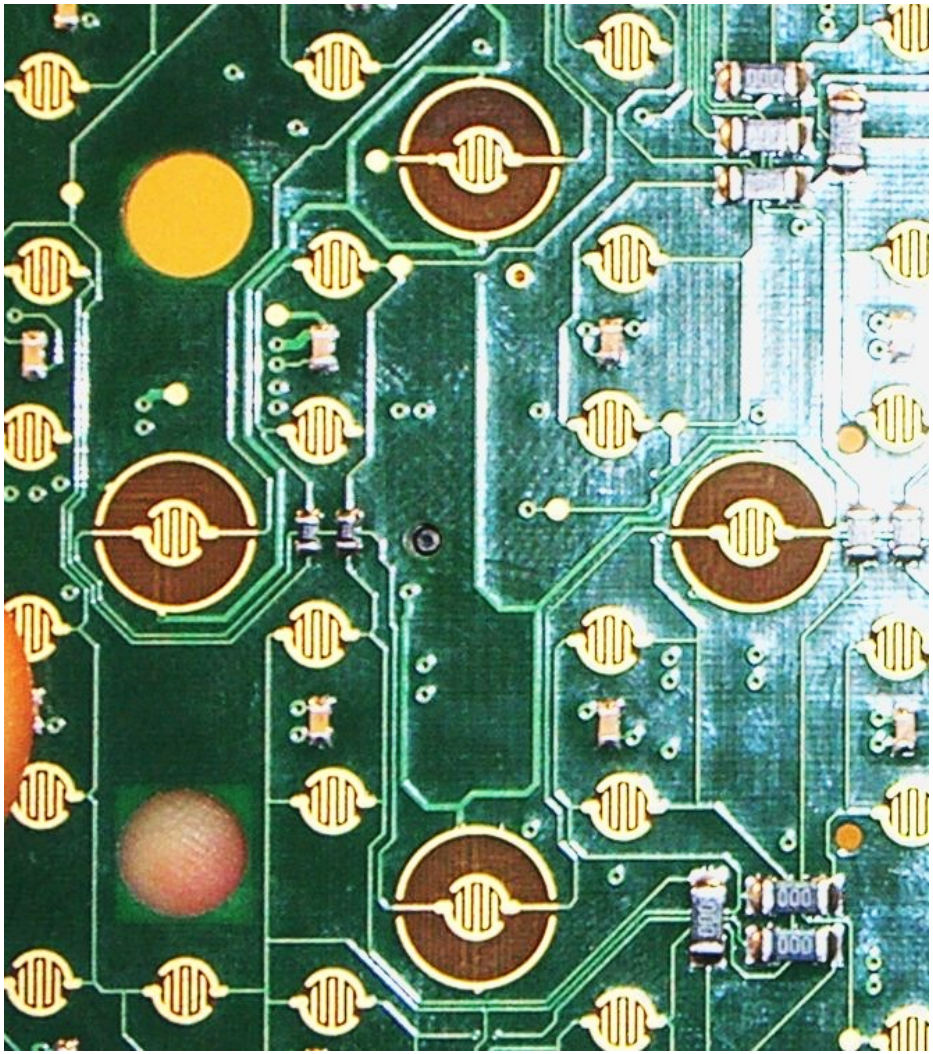
- Replace a terminal's insides with your own electronics
- Capture cards and PINs from victims
- Use them to do a man-in-the-middle attack in real time on a remote terminal in a merchant selling expensive goods

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!
- So far, mag-strip fallback fraud has been easy
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier was blamed)
- Then ‘Tamil Tigers’
- After fraud at BP Girton: we investigate

Tamper switches (Ingenico i3300)

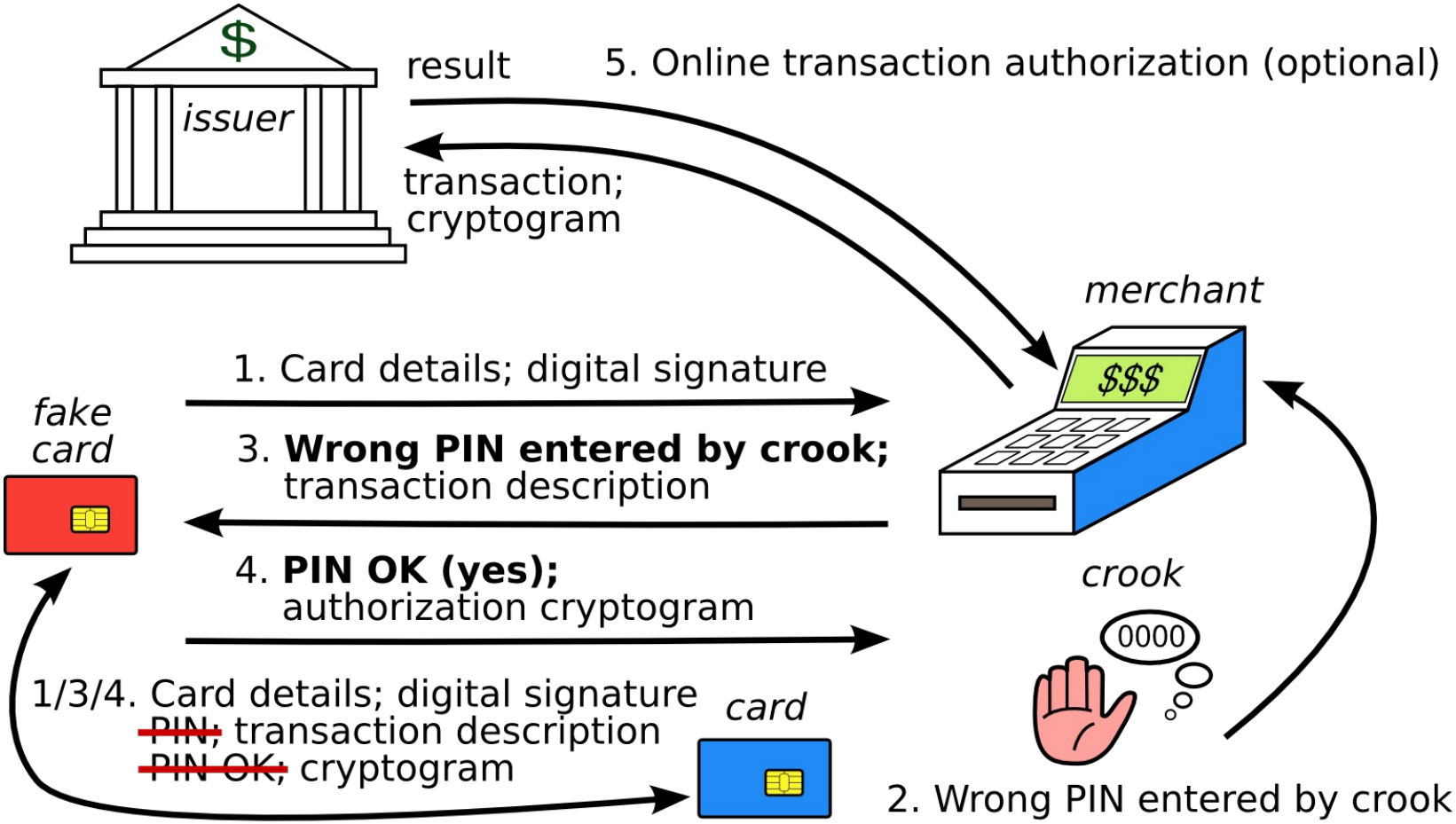




TV demo: Feb 26 2008

- 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 (2010)



Fixing 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 introduced a fix July 2010; removed Dec 2010 (too many false positives?); banks asked for student thesis to be taken down from web instead
- Real problem: EMV spec now far too complex
- With 100+ vendors, 20,000 banks, millions of merchants … everyone passes the buck (or tries to sell ECC…)

Chosen protocol attack

- Suppose that we had a protocol for users to sign hashes of payment messages (such a protocol was proposed in 1990s):

  $C \rightarrow M$: order

  $M \rightarrow C$: X [= hash(order, amount, date, …)]

  $C \rightarrow M$: $sig_K\{X\}$

- How might this be attacked?

Chosen protocol attack (2)

The Mafia demands you sign a random challenge to prove your age for porn sites!