Security 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

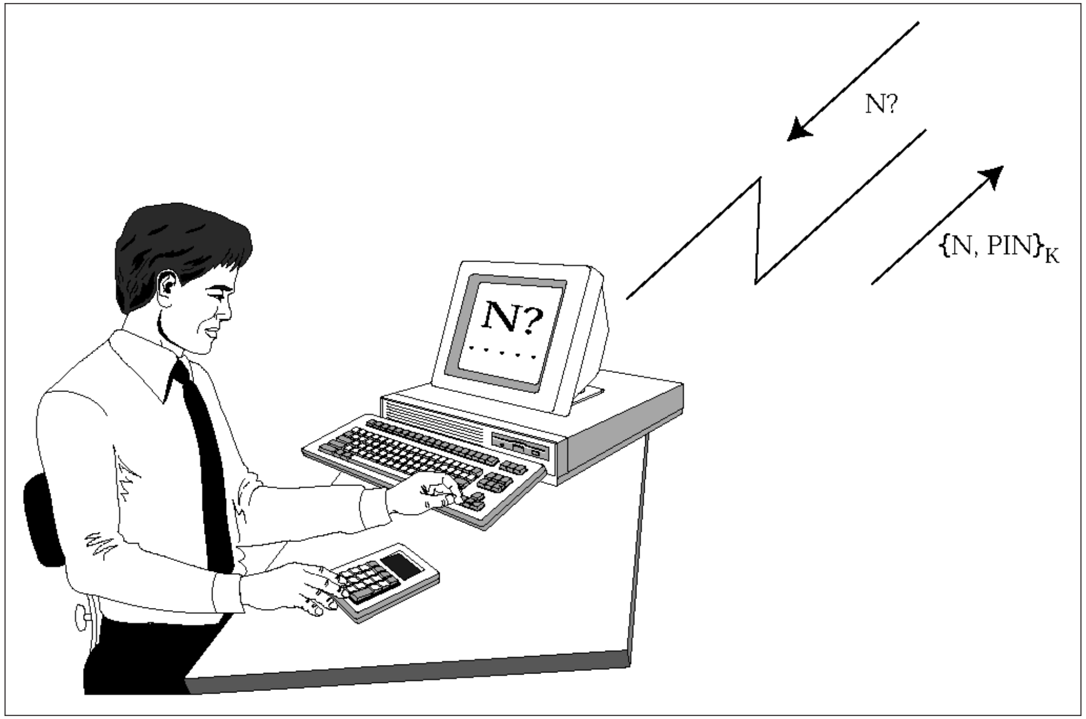
- Principals are the engine controller E and the car key transponder T
- Static ($T \rightarrow E$: KT)
- Non-interactive

  $T \rightarrow E$: 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
- For more see Koscher et al., Miller/Valasek, and my book

Two-factor authentication



S → U: N

U → P: N, PIN

P → 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?

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

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

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

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

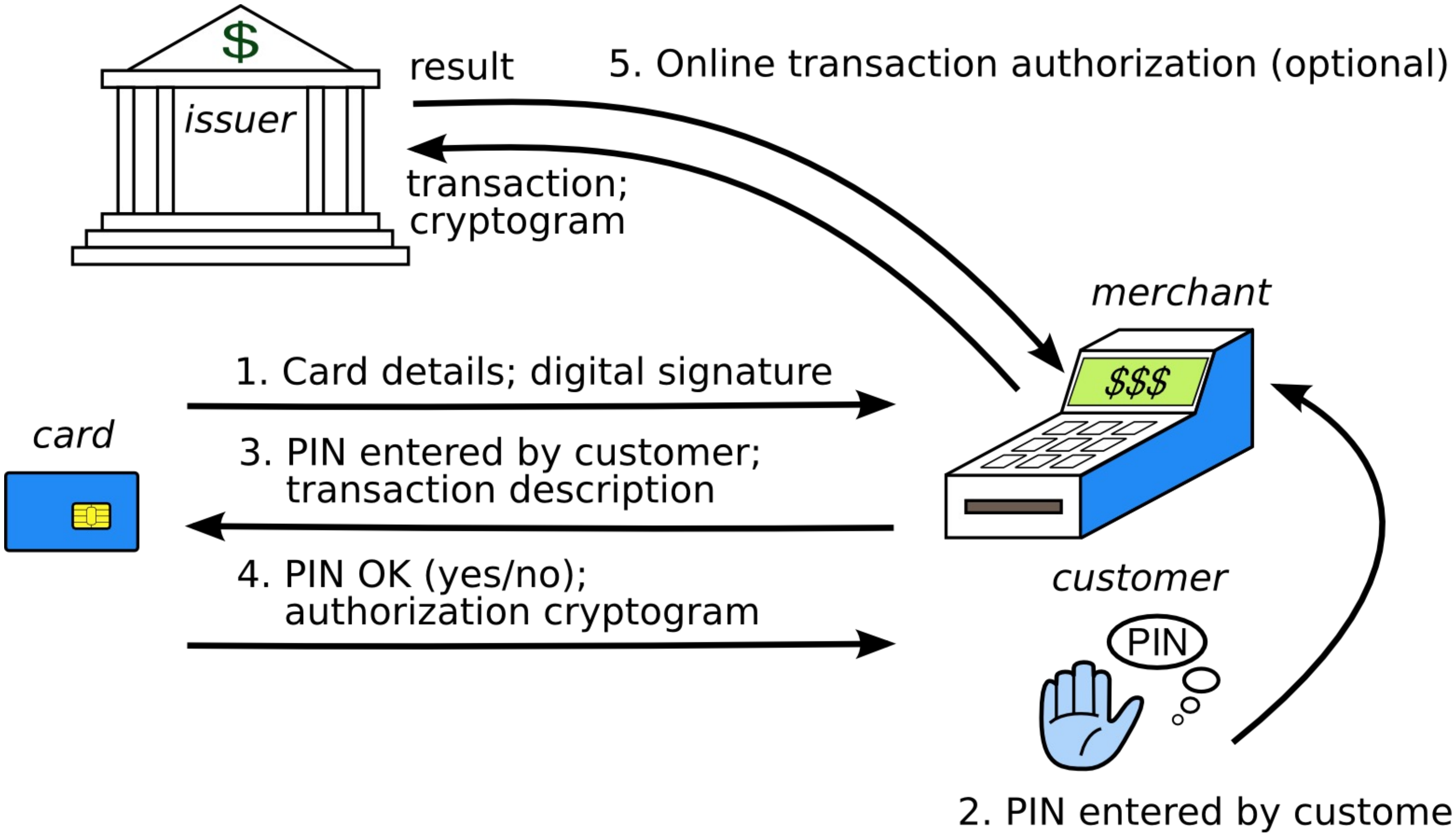
  $\mathrm{F} \rightarrow \mathrm{B}$: N

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

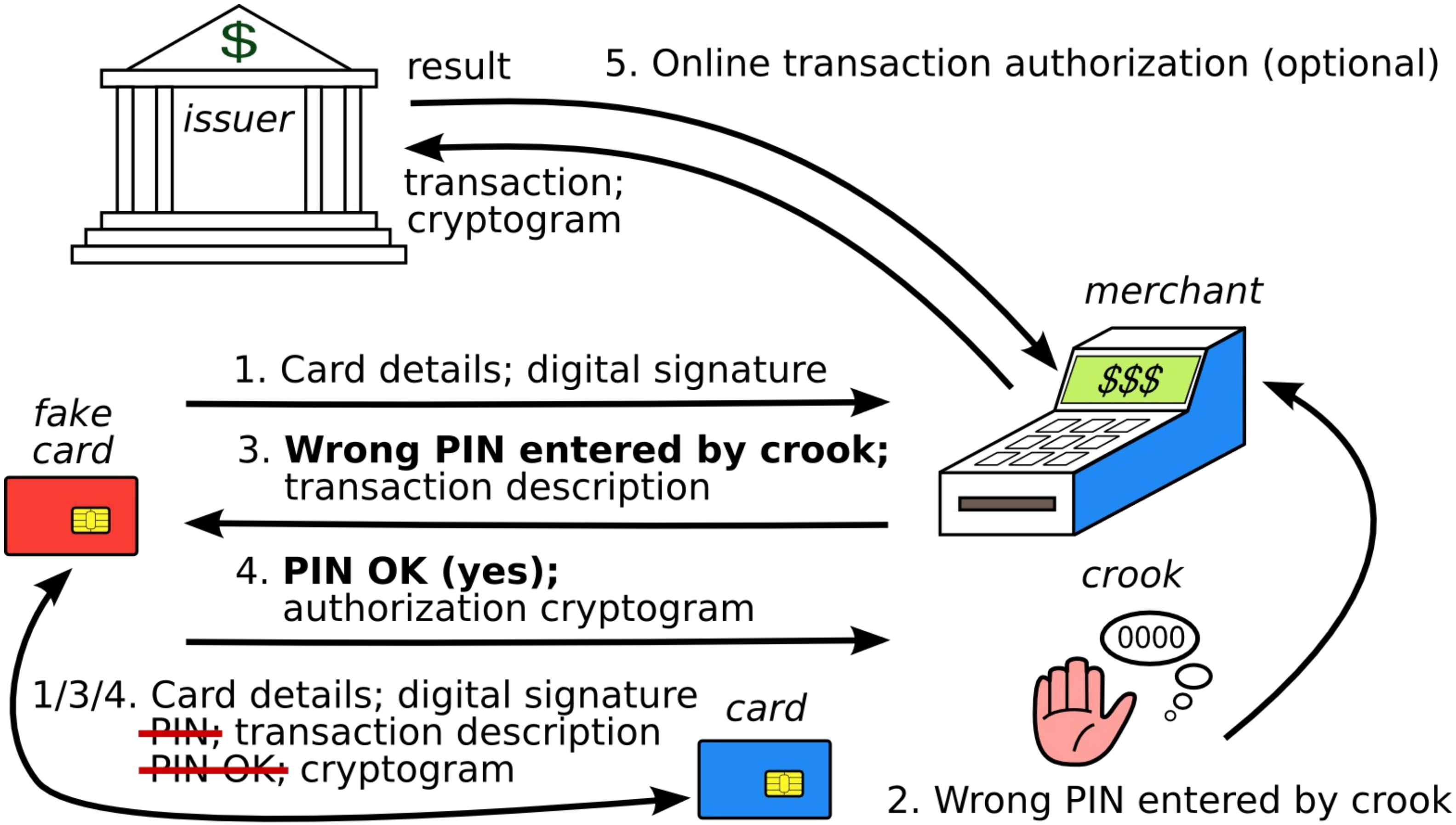
  $F \rightarrow \mathrm{B}$: $\{N\}_K$

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

A normal EMV transaction


issuer
$
result
5. Online transaction authorization (optional)
transaction;
cryptogram
merchant
$$$
1. Card details; digital signature
card
3. PIN entered by customer;
transaction description
4. PIN OK (yes/no);
authorization cryptogram
customer
PIN
2. PIN entered by customer

The ‘No-PIN’ attack (2010)



issuer

result

5. Online transaction authorization (optional)

transaction;
cryptogram

merchant

$$$

fake
card

1. Card details; digital signature

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

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

crook

0000

1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram

card

2. Wrong PIN entered by crook

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
- Took until 2016 to fix (for UK transactions)

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

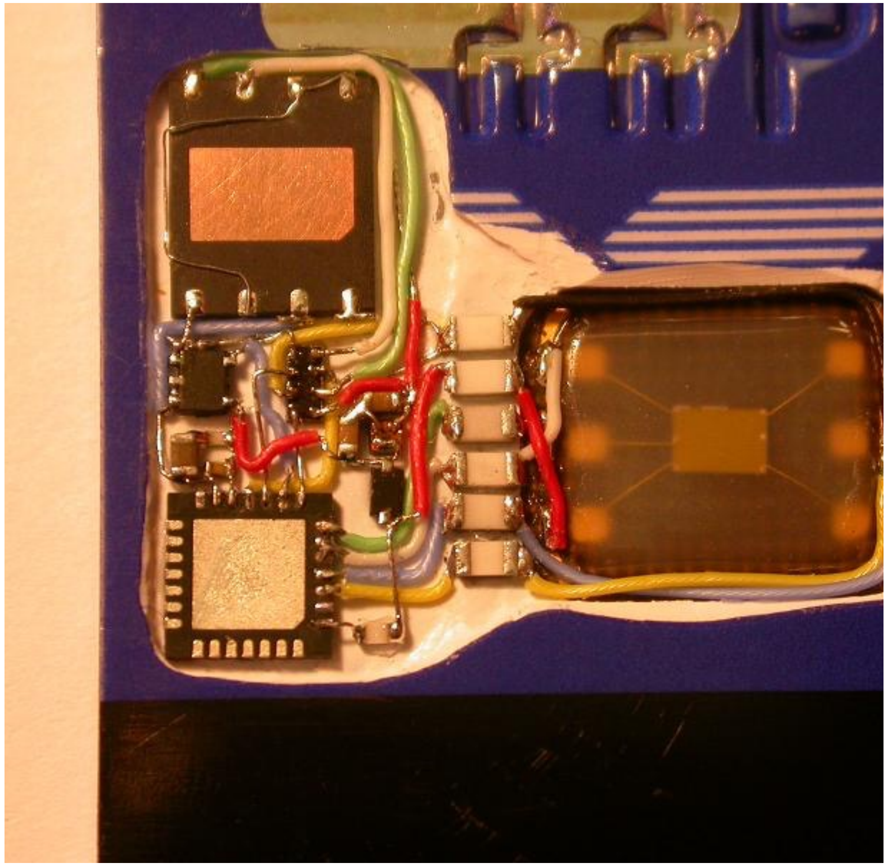
ATMs and Random Numbers (2)

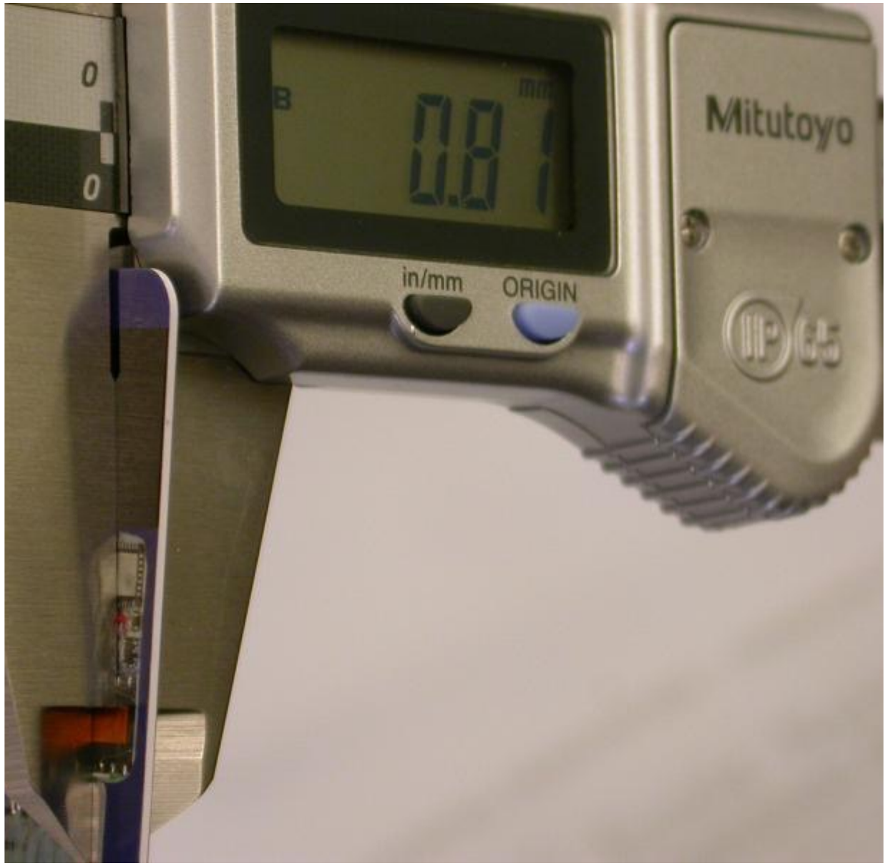
- Log of disputed transactions at Majorca:

```
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, finding half of ATMs use counters!

ATMs and Random Numbers (3)





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
- 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
- This happened to about 20 customers of a Bournemouth lap-dancing club too...

Safety engineering

- Markets do safety in some industries (aviation) way better than others (medicine)
- Cars were dreadful until Nader's 'Unsafe at Any Speed' led to the NHTSA
- In the EU, we have broad frameworks such as the Product Liability Directive (all goods), sectoral laws such as a Directive on type approval for cars, plus many detailed rules
- So what happens when we add software?

When cars get hacked

- 2011: Carshark needed physical access, so seen as ‘academic’
- 2015: Charlie Miller and Chris Valasek hacked a jeep Cherokee via Chrysler’s Uconnect
- Suddenly people cared…
- Chrysler recalled 1.4m vehicles for software fix