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 then computers…

A Simple Authentication

- An infrared token used in some multi-storey parking garages to enable subscribers to raise the barrier.
- First transmits its serial number & then transmits an authentication block that consists of the same serial number, followed by a random number, all encrypted using a key that is unique to the device.
- T → G : T, {T, N}KT
- The in-car token sends its name, T, followed by the encrypted value of T concatenated with N, where N stands for “number used once,” or nonce.

A Simple Authentication

- Key management: A typical garage token's key KT is simply its serial number encrypted under a global master key, KM, known to the central server:
- KT = {T}KM
- This is known as **key diversification**.
- Gives a very simple way of implementing access tokens, and is very widely used in smartcard-based systems as well.

A Simple Authentication: Common Mistake

- Checking that the nonce is different from last time,
- Given two valid codes A and B, the series ABABAB. . . was interpreted as a series of independently valid codes.
- In one car lock, the thief could open the door by replaying the last-but-one code.

Car unlocking protocols: Challenge Response

- 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'.

- As the car key is inserted into the steering lock, the engine management unit sends a challenge, consisting of a random n-bit number to the key using a short-range radio signal.
- The car key computes a response by encrypting the challenge.

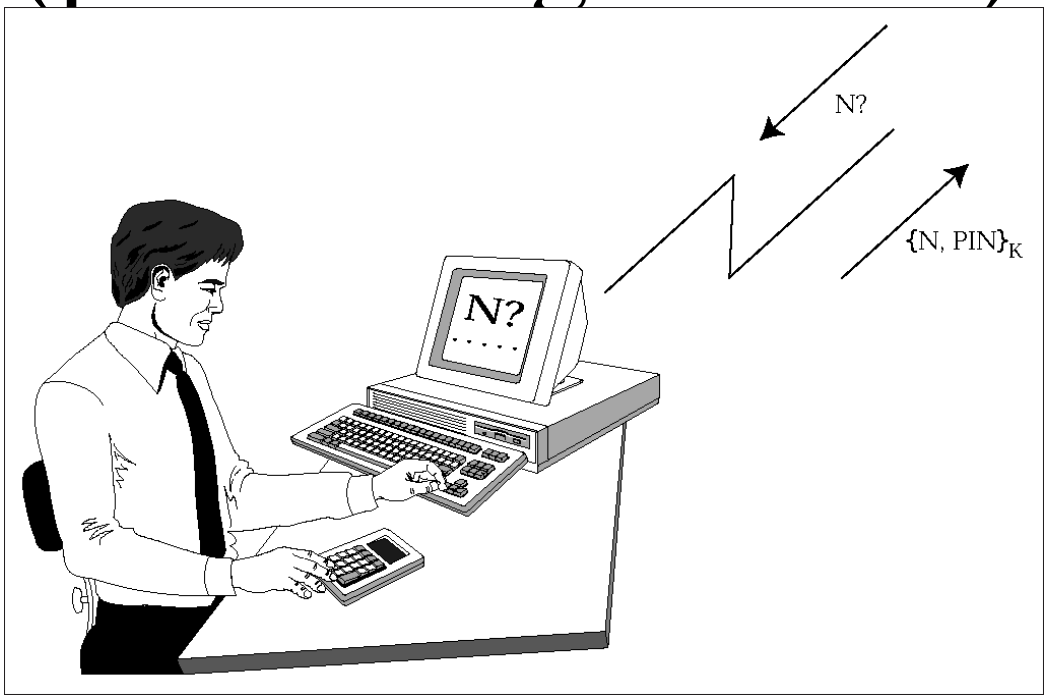
What goes wrong

- In cheap devices, N may be random or a counter – one-way communication and no clock
- It can be too short, and wrap around
- If it's random, how many do you remember? (the valet attack)
- Counters and timestamps can lose sync leading to DoS attacks
- There are also weak ciphers – Eli Biham's 2008 attack on the Keeloq cipher (2^{16} chosen challenges then 500 CPU days' analysis – some other vendors authenticate challenges)

Problems

- This is still not bulletproof.
- In one system, the random numbers generated by the engine management unit turned out to be rather predictable, so it was possible for a thief to interrogate the key in the car owner's pocket, as he passed, with the anticipated next challenge.

Two-factor authentication (password generator)



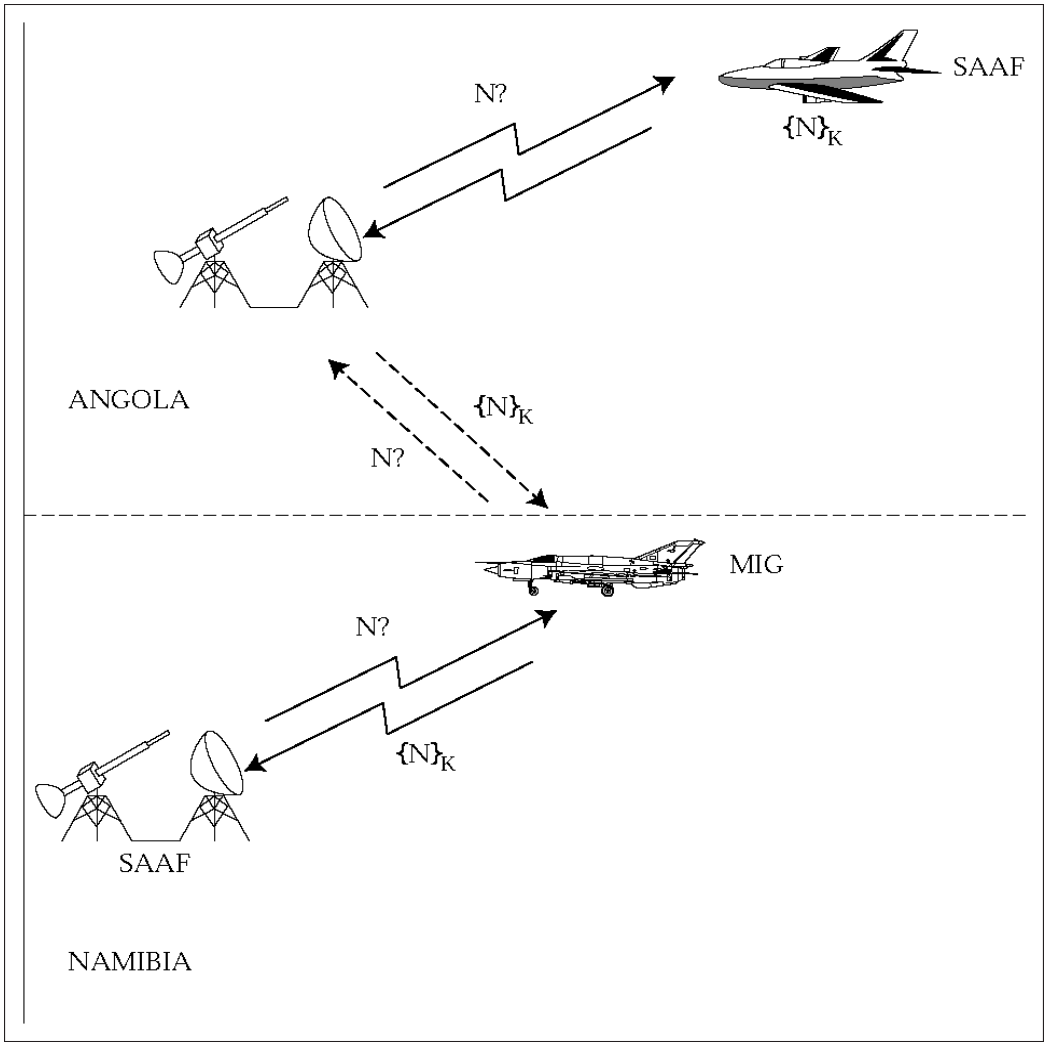
S Server
P Pwd Genertaor
U User

$S \rightarrow U: N$

$U \rightarrow P: N, PIN$

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

IFF (2)



- Several MIGs had loitered in southern Angola, just north of the South African air defense belt, until a flight of SAAF Impala bombers raided a target in Angola.
- Then the MIGs turned sharply and flew openly through the SAAF's air defenses, which sent IFF challenges.
- The MIGs relayed them to the Angolan air defense batteries, which transmitted them at a SAAF bomber;
- the responses were relayed back in real time to the MIGs, which retransmitted them and were allowed through

IFF (3)

- The middleman attack is very general – Conway discussed how to beat a grandmaster at postal chess
- The fix for the man-in-the-middle attack is often application specific
- E.g. NATO mode 12 IFF: 32 bit encrypted challenge (to prevent enemy using IFF to locate beyond radar range) at rate of 250 per second

Identify Friend or Foe (IFF)

- Basic idea: fighter challenges bomber

  $F \rightarrow B: N$

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

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

  $F \rightarrow B: N$

  $B \rightarrow F: N$

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

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

Overcoming Reflection Attack

- In many cases, it is sufficient to include the names of the two parties in the authentication exchange.
- Require a friendly bomber to reply to the challenge:
- F → B : N with a response such as:
- B → F : {B, N}K
- Thus, a reflected response {F, N} (or even {F', N} from the fighter pilot's wingman) could be detected.

Reflection Attacks

- Mutual authentication: Mutual Id of two Suppose, that a simple challenge-response IFF system designed to prevent anti-aircraft gunners attacking friendly aircraft also had to be deployed in a fighter-bomber.
- Now suppose that the air force simply installed one of its air gunners' challenge units in each aircraft and connected it to the fire-control radar.
- But now an enemy bomber might reflect a challenge back at our fighter, get a correct response, and then reflect that back as its own response:

Source: Ross Anderson