Access Control and Privacy Policies (8)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also homework is there)

Last Week

Andrew Secure RPC Protocol: A and B share a key K_{AB} and want to identify each other

- A sends B : A, N_A
- B sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$
- A sends B : $\{N_A\}_{K'_{AB}}$

Protocols

A sends B : . . .

- by convention A, B are named principals Alice. . . but most likely they are programs, which just follow some instructions

Protocols

A sends B : . . .
B sends A : . . .
:

- by convention A, B are named principals Alice... but most likely they are programs, which just follow some instructions
- indicates one "protocol run", or session, which specifies some order in the communication
- there can be several sessions in parallel (think of wifi routers)

Last Week

A and B share the key K_{AB} and want to identify each other

- A sends B : A, N_A
- B sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$
- A sends B : $\{N_A\}_{K'_{AB}}$

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A

I sends A : B, N_A

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A

I sends A : B, N_A

A sends I : $\{N_A, K'_{AB}\}_{K_{AB}}$

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A $\qquad$ I sends A : B, N_A

I sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$ $\qquad$ A sends I : $\{N_A, K'_{AB}\}_{K_{AB}}$

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A
I sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$
A sends I : $\{N_A\}_{K'_{AB}}$

I sends A : B, N_A
A sends I : $\{N_A, K'_{AB}\}_{K_{AB}}$

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A	I sends A : B, N_A
I sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$	A sends I : $\{N_A, K'_{AB}\}_{K_{AB}}$
A sends I : $\{N_A\}_{K'_{AB}}$	I sends A : $\{N_A\}_{K'_{AB}}$

Defeating Challenge-Response

A reflection attack: an intruder I impersonates B.

A sends I : A, N_A	I sends A : B, N_A
I sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$	A sends I : $\{N_A, K'_{AB}\}_{K_{AB}}$
A sends I : $\{N_A\}_{K'_{AB}}$	I sends A : $\{N_A\}_{K'_{AB}}$

Sounds stupid: "...answering a question with a counter question"

Identify Friend or Foe

198?: war between Angola (supported by Cuba) and Namibia (supported by SA)

Identify Friend or Foe

198?: war between Angola (supported by Cuba) and Namibia (supported by SA)

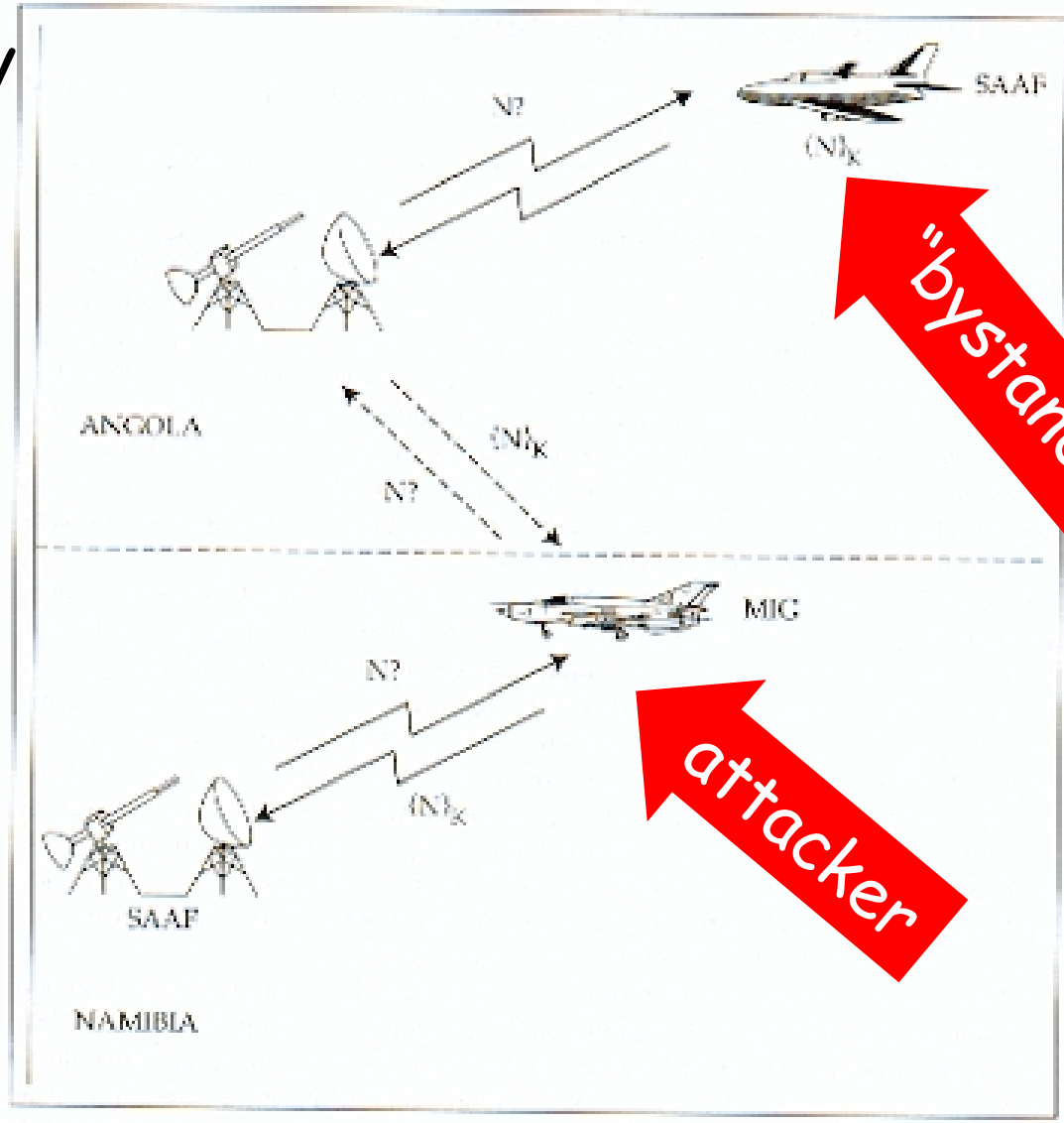

Figure 2.2 The MIG-in-the middle attack.

Identify Friend or Foe

198?: war between Angola (supported by Cuba) and Namibia (supported by SA)

being outsmarted by Angola/Cuba ended SA involvement

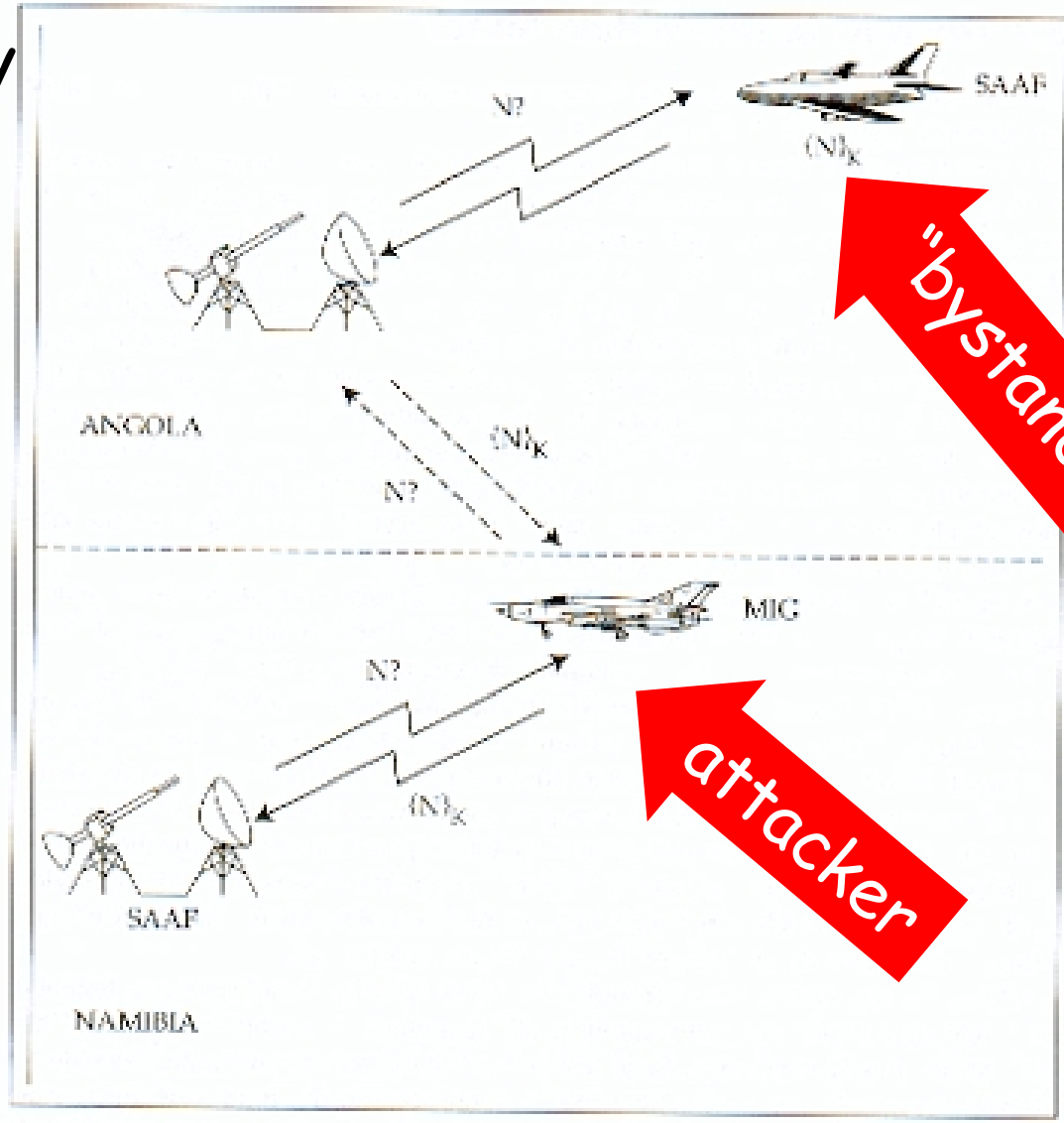

Figure 2.2 The MIG-in-the middle attack.

Encryption to the Rescue?

- A sends B : $\{A, N_A\}_{K_{AB}}$ encryption
- B sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$
- A sends B : $\{N_A\}_{K'_{AB}}$

Encryption to the Rescue?

- A sends B : $\{A, N_A\}_{K_{AB}}$ encryption
- B sends A : $\{N_A, K'_{AB}\}_{K_{AB}}$
- A sends B : $\{N_A\}_{K'_{AB}}$

means you need to send a separate "Hello" signal (bad), or worse share a single key between many entities

Possible Kinds of Attacks

- reflection attacks
- man-in-the-middle attacks
- replay attacks
- timing attacks
- changing environment / changing assumptions