

Authentication

- ❑ Establishing authenticated interactive communication;
- ❑ Authenticating one-way communication, such as e-mail;
- ❑ Third party authentication, such as a signed contract.

... use $\{M\}^K$ to denote $E(M, K)$

... based on *trusted authentication service S*.

From R. M. Needham and M. D. Schroeder, Using Encryption for Authentication in Large Networks of Computers, *Communications of the ACM* 21 (1978).

Interactive Communication I

Private key based

A, B and auth server S

[1] $A \rightarrow S: A, B, I_A$

sent in clear!

I_A is *nonce identifier*

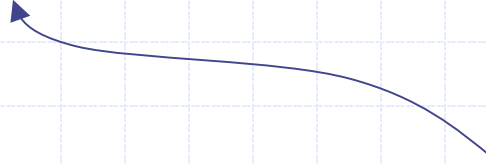
S looks up K_A, K_B and computes K_{AB} (*session key*)

[2] $S \rightarrow A: \{I_A, B, K_{AB}, \{K_{AB}, A\}^{K_B}\}^{K_A}$

protects against replay attack



protects against substitution of $A \rightarrow S$



Interactive Communication II

- [3] $A \rightarrow B: \{K_{AB}, A\}^{K_B}$ authenticates A's identity
since K_{AB} is unique,
authenticates conversation
- [4] $B \rightarrow A: \{I_B\}^{K_{AB}}$ protect against replay attack.
- [5] $A \rightarrow B: \{I_B + 1\}^{K_{AB}}$

Interactive Communication III

Main security hole: suppose X breaks K_{AB} . (while this may take considerable time, it is a vulnerability).

Then:

[3] $X \rightarrow B: \{K_{AB}, A\}^{K_B}$

X replays old identifier

[4] $B \rightarrow \cancel{A} X: \{I_B\}^{K_{AB}}$

X intercepts message

[5] $X \rightarrow B: \{I_B - 1\}^{K_{AB}}$

... and X has reused K_{AB} to set up a session with B .

Interactive Communication IV

[1] $A \rightarrow B: A$

[2] $B \rightarrow A: \{A, I_B\}^{K_B}$

[3] $A \rightarrow S: A, B, I_A, \{A, I_B\}^{K_B}$

[4] $S \rightarrow A: \{I_A, B, K_{AB}, \{K_{AB}, A, I_B\}^{K_B}\}^{K_A}$

[5] $A \rightarrow B: \{K_{AB}, A, I_B\}^{K_B}$

... requires B to maintain I_B for the duration of connection setup.

Interactive Communication V

Kerberos is similar, but requires synchronized clocks:

[1] $A \rightarrow S: A, B$

[2] $S \rightarrow A: \{T, L, B, K_{AB}, \{T, L, A, K_{AB}\}^{K_B}\}^{K_A}$

timestamp points to T
lifetime points to L

[3] $A \rightarrow B: \{A, T\}^{K_{AB}}, \{K_{AB}, A, I_B\}^{K_B}$

[4] $B \rightarrow A: \{T + 1\}^{K_{AB}}$

One-way communication

Private key: the value $\{K_{AB}, A\}^{K_B}$ must have come from an authentication server that authenticated A.

Attach to message that is encrypted with K_{AB} . The resulting message is self-authenticating both to the sender and receiver.

Public key: include nonce I in message and encrypt with PK_B . Attach to message:

$$\{A, I, \{B\}^{SK_A}\}^{PK_B}$$

Digital Signatures

Private key: based on *characteristic function* $V(M)$ such that it is hard to find a sensible message M' where $V(M) = V(M')$.

[1] $A \rightarrow S: A, \{V(M)\}^{K_A}$

[2] $S \rightarrow A: \{A, V(M)\}^{K_S}$ *signature block*

... when B gets M, it *opens* the signature block:

[3] $B \rightarrow S: \{A, V(M)\}^{K_S}$

[4] $S \rightarrow A: \{A, V(M)\}^{K_B}$

Public key: use product cipher $\{\{M\}^{SK_A}\}^{PK_B}$