# Needham-Schroeder authentication protocol and its formal analysis



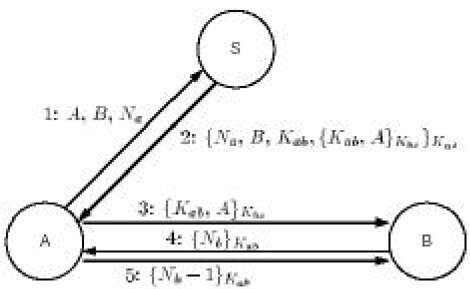
# Needham-Schroeder protocol

- The goal of the protocol is to establish mutual authentication between two parties A and B in the presence of adversary, who can
  - Intercept messages;
  - Delay messages;
  - Read and copy messages;
  - Generate messages,

  But who does not know
  - secret keys of principals, which they share with the authentication server S.
- A and B obtain a secret shared key though authentication server S.
- The protocol uses shared keys encryption/decryption



# Needham-Schroeder protocol




The Needham-Schroeder Protocol (with shared keys)



# Needham-Schroeder protocol

- Message 1 $A \rightarrow S: A, B, N_A$
- Message 2 $S \rightarrow A: \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_B}\}_{K_A}$
- Message 3 $A \rightarrow B: \{K_{AB}, A\}_{K_B}$
- Message 4 $B \rightarrow A: \{N_B\}_{K_{AB}}$
- Message 5 $A \rightarrow B: \{N_B - 1\}_{K_{AB}}$

Here $K_A$ and $K_B$ are keys of *A* and *B* shared with S, resp.
$N_A$ and $N_B$ are nonces, introduced by *A* and *B*, resp.
$K_{AB}$ is a secret session key for *A* and *B* provided by *S*

# How it works

- A makes contact with the authentication server S, sending identities A and B and *nonce* $N_A$;
- S responds with a message encrypted with the key of A. The message contains session key $K_{AB}$ (to be used by A and B) and certificate encrypted with B's key conveying the session key and A's identity;
- A sends the certificate to B;
- B decrypts the certificates and sends his own nonce encrypted by the session key to A; (*nonce handshake*);
- A decrypts the last message and sends *modified nonce* back to B.

--------------------------------------------------------------------------------

By the end of the message exchange both A and B share the secret key and both are assured in the presence of each other.



# Formal analysis using BAN logic

Explicit assumptions:

| *A believes:* | *B believes:* | *S believes:* |
|---|---|---|
| $A \overset{K_A}{\leftrightarrow} S$ | $B \overset{K_B}{\leftrightarrow} S$ | $A \overset{K_A}{\leftrightarrow} S$, $B \overset{K_B}{\leftrightarrow} S$ |
| $S$ **controls** $A \overset{K_{AB}}{\leftrightarrow} B$ | $S$ **controls** $A \overset{K_{AB}}{\leftrightarrow} B$ | $A \overset{K_{AB}}{\leftrightarrow} B$ |
| $S$ **controls** **fresh**$(A \overset{K_{AB}}{\leftrightarrow} B)$ | | **fresh**$(A \overset{K_{AB}}{\leftrightarrow} B)$ |
| **fresh**$(N_A)$ | **fresh**$(N_B)$ | |



# Authentication goals

Main: $A$ **believes** $A \overset{K_{AB}}{\leftrightarrow} B$ and $B$ **believes** $A \overset{K_{AB}}{\leftrightarrow} B$

Subsidiary: $A$ **believes** $B$ **believes** $A \overset{K_{AB}}{\leftrightarrow} B$ and

$B$ **believes** $A$ **believes** $A \overset{K_{AB}}{\leftrightarrow} B$



# Protocol steps formalized

Transform each message into an idealized message, containing only nonces and statements (implicitly asserted by a sender)

| *Message* | *Idealized Message* |
|---|---|
| 1. $A \rightarrow S$: $A, B, N_A$ | – |
| 2. $S \rightarrow A$: $\{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_B}\}_{K_A}$ | $\{N_A, A \overset{K_{AB}}{\leftrightarrow} B$, **fresh**$(A \overset{K_{AB}}{\leftrightarrow} B)$, $\{A \overset{K_{AB}}{\leftrightarrow} B\}_{K_B}\}_{K_A}$ |
| 3. $A \rightarrow B$: $\{K_{AB}, A\}_{K_B}$ | $\{A \overset{K_{AB}}{\leftrightarrow} B\}_{K_B}$ |
| 4. $B \rightarrow A$: $\{N_B\}_{K_{AB}}$ | $\{N_B, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AB}}$ |
| 5. $A \rightarrow B$: $\{N_B - 1\}_{K_{AB}}$ | $\{N_B, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AB}}$ |

# First step of analysis

Let $M = (N_A, A \overset{K_{AB}}{\leftrightarrow} B, \textbf{fresh}(A \overset{K_{AB}}{\leftrightarrow} B))$

Then we have

- $A$ **believes** $A \overset{K_A}{\leftrightarrow} S$, (explicit assumption)
- $A$ **sees** $\{M\}_{K_A}$ (upon receiving Message 2)

Apply message-meaning rule:

$$\frac{A \textbf{ believes } A \overset{K_A}{\leftrightarrow} S,\ A \textbf{ sees } \{M\}_{K_A}}{A \textbf{ believes } (S \textbf{ said } M)}$$



# Further steps

We have

- $A$ **believes** fresh$(N_A)$ (explicit assumption)
- $N_A$ is a part of $M = (N_A, A \overset{K_{AB}}{\leftrightarrow} B, \textbf{fresh}(A \overset{K_{AB}}{\leftrightarrow} B))$

By application of second decomposition rule we deduce:

$$A \textbf{ believes fresh}(M)$$



# Further steps

- By nonce-verification rule:

$$\frac{A \textbf{ believes fresh } (M),\ A \textbf{ believes } (S \textbf{ said } M)}{A \textbf{ believes } (S \textbf{ believes } M)}$$

- By the third decomposition rule

$$\frac{A \textbf{ believes } (S \textbf{ believes } (N_A,\ A \overset{K_{AB}}{\leftrightarrow} B, \textbf{fresh}(A \overset{K_{AB}}{\leftrightarrow} B)))}{A \textbf{ believes } (S \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B)}$$



# Final step

By jurisdiction rule:

$$\frac{A \textbf{ believes } (S \textbf{ controls } A \overset{K_{AB}}{\leftrightarrow} B),\ A \textbf{ believes } (S \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B)}{A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B}$$

The first authentication goal is achievable!

# Remaining authentication goals

- The statement $B$ **believes** $A \overset{K_{AB}}{\leftrightarrow} B$. is not derivable!
- One needs one extra assumption to derive it:

$$B \textbf{ believes fresh}(A \overset{K_{AB}}{\leftrightarrow} B).$$

- Derivation of subsidiary goals is left as an exercise:



# Conclusion

The formal analysis we have just done should not be

- neither underestimated:
  - We have shown that the protocol is **correct** under explicit assumptions and concrete formalization;
- nor overestimated:
  - The analysis is as good as formal (idealized) model and explicit assumptions are;
  - The adequacy of the model and assumptions may be an issue here.