Needham-Schroeder 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 an 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 through authentication server S.
- The protocol uses shared keys encryption/decryption

**Needham-Schroeder protocol**
- Message 1
- Message 2
- Message 3
- Message 4
- Message 5

The Needham-Schroeder Protocol (with shared keys)

- Here $\kappa_A$ and $\kappa_B$ 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:

\[
\begin{align*}
A & \mathbin{\xrightarrow{K_{AB}} B} \\
B & \mathbin{\xrightarrow{K_{AB}} B}
\end{align*}
\]

Authentication goals

- Main: \( A \mathbin{\xrightarrow{K_{AB}} B} \) and \( B \mathbin{\xrightarrow{K_{AB}} B} \)

- Subsidiary: \( A \mathbin{\xrightarrow{K_{AB}} B} \) and \( B \mathbin{\xrightarrow{K_{AB}} B} \)

Protocol steps formalized

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

<table>
<thead>
<tr>
<th>Message</th>
<th>Idealized Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ( A \mathbin{\rightarrow} S, A, B, N_A )</td>
<td>( - )</td>
</tr>
<tr>
<td>2. ( S \mathbin{\rightarrow} A; { N_A, B, K_{AB}, { K_{AB}, A } }, K_B A )</td>
<td>( { N_A, A \mathbin{\xrightarrow{K_{AB}}} B, \text{fresh}(A), { K_{AB}, B } } K_B A )</td>
</tr>
<tr>
<td>3. ( A \mathbin{\rightarrow} B; { K_{AB}, A } K_B )</td>
<td>( { K_{AB}, B } K_B A )</td>
</tr>
<tr>
<td>4. ( B \mathbin{\rightarrow} A; { N_B } K_{AB} )</td>
<td>( { N_B, A \mathbin{\xrightarrow{K_{AB}}} B } K_{AB} )</td>
</tr>
<tr>
<td>5. ( A \mathbin{\rightarrow} B; { N_B } K_{AB} )</td>
<td>( { N_B, A \mathbin{\xrightarrow{K_{AB}}} B } K_{AB} )</td>
</tr>
</tbody>
</table>
First step of analysis

- Let $M = (N_A, A \rightarrow_{K_{AB}} B, \text{fresh}(A \rightarrow_{K_{AB}} B))$
- Then we have
  - $A$ believes $A \rightarrow_{K_{AB}} B$ (explicit assumption)
  - $A$ sees $M \rightarrow_{K_A}$
- Apply message-meaning rule:

  \[
  \frac{A \text{ believes } A \rightarrow_{K_{AB}} B, A \text{ sees } M \rightarrow_{K_A}}{A \text{ believes } (S \text{ said } M)}
  \]

Further steps

- We have
  - $A$ believes $\text{fresh}(N_A)$ (explicit assumption)
  - $M = (N_A, A \rightarrow_{K_{AB}} B, \text{fresh}(A \rightarrow_{K_{AB}} B))$

  By application of second decomposition rule we deduce:

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

Further steps

- By nonce-verification rule:

  \[
  \frac{A \text{ believes } \text{fresh}(M), A \text{ believes } (S \text{ said } M)}{A \text{ believes } (S \text{ believes } M)}
  \]

  - By the third decomposition rule

    \[
    \frac{A \text{ believes } (S \text{ believes } (N_A, A \rightarrow_{K_{AB}} B, \text{fresh}(A \rightarrow_{K_{AB}} B))), A \text{ believes } A \rightarrow_{K_{AB}} B}{A \text{ believes } A \rightarrow_{K_{AB}} B}
    \]

Final step

- By jurisdiction rule:

  \[
  \frac{A \text{ believes } (S \text{ controls } A \rightarrow_{K_{AB}} B), A \text{ believes } (S \text{ believes } A \rightarrow_{K_{AB}} B)}{A \text{ believes } A \rightarrow_{K_{AB}} B}
  \]

  - The first authentication goal is achievable!
Remaining authentication goals

- The statement $B \text{ believes } A \overset{K_{AB}}{\rightarrow} B$. is not derivable!
- One needs one extra assumption to derive it:
  
  $$B \text{ believes fresh}(A \overset{K_{AB}}{\rightarrow} B)$$
- 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.