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 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

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 \( S \), respectively.
- \( N_A \) and \( N_B \) are nonces, introduced by \( A \) and \( B \), respectively.
- \( K_{AB} \) 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:
Authentication goals

• Main: $A$ believes $A \leftrightarrow B$ and $B$ believes $A \leftrightarrow B$

• Subsidiary: $A$ believes $B$ believes $A \leftrightarrow B$ and $B$ believes $A$ believes $A \leftrightarrow B$
Protocol steps formalized

• Transform each message into an idealized message, containing only nonces and statements (implicitly asserted by a sender)
First step of analysis

• Let \( M = (N_A, A \leftrightarrow B, \text{fresh}(A \leftrightarrow B)) \)

• Then we have
  
  \[ \textbf{A believes } A \leftrightarrow S, \ A \text{ sees } \{M\}^{K_A} \]

• Apply message-meaning rule:

\[ \textbf{A believes } A \leftrightarrow S, \ A \text{ sees } \{M\}^{K_A} \]

\[ \textbf{A believes } (S \text{ said } M) \]
Further steps

• We have

  \[ A \text{ believes } \text{fresh}(N_A) \]  
  \[ N_A \] is a part of  

  \[ M = (N_A, A \leftrightarrow K_{AB} B, \text{fresh}(A \leftrightarrow K_{AB} B)) \]  

(implicit assumption)

By application of second decomposition rule we deduce:

  \[ A \text{ believes } \text{fresh}(M) \]
Further steps

• By nonce-verification rule:

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

• By the third decomposition rule

\[
A \text{ believes } (S \text{ believes } (N_A, \ A \overset{K_{AB}}{\leftrightarrow} B, \text{ fresh}(A \overset{K_{AB}}{\leftrightarrow} B))) \\
\hline
A \text{ believes } (S \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B)
\]
Final step

• By jurisdiction rule:

\[
\text{\[A\ \text{believes (S controls } A \xleftrightarrow{KAB} B)\]}
\text{\[, A believes (S believes } A \xleftrightarrow{KAB} B)\]}
\text{\[A\ \text{believes } A \xleftrightarrow{KAB} B\]}

• The first authentication goal is achievable!
Remaining authentication goals

• The statement \( B \text{ believes } A \xleftrightarrow{K_{AB}} B \) is not derivable!

• One needs one extra assumption to derive it:

\[ B \text{ believes fresh}(A \xleftrightarrow{K_{AB}} B). \]

• 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.