Recall the Needham-Schroeder protocol:
- $A \rightarrow S : A, B, N_a$
- $S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}K_{as}\}K_{as}$
- $A \rightarrow B : \{K_{ab}, A\}K_{bs}$
- $B \rightarrow A : \{N_b\}K_{ab}$
- $A \rightarrow B : \{N_b - 1\}K_{ab}$

Needham-Schroeder is idealized as follows:
- $A \rightarrow S : \{N_a, (A \nrightarrow B), \#(A \nrightarrow B), \{A \nrightarrow B\}K_{bs}\}K_{as}$
- $A \rightarrow B : \{A \nrightarrow B\}K_{bs}$
- $B \rightarrow A : \{N_b, (A \nrightarrow B)\}K_{ab}$ from $B$
- $A \rightarrow B : \{N_b, (A \nrightarrow B)\}K_{ab}$ from $A$

The Nonce Verification Rule says:

$A \equiv (S \equiv A \nrightarrow B), \#(A \nrightarrow B), \{A \nrightarrow B\}K_{as}$

From step 2 of the (idealized) protocol:

$A \equiv (S \equiv A \nrightarrow B), \#(A \nrightarrow B), \{A \nrightarrow B\}K_{as}$

The Nonce Verification Rule says:

$A \equiv (\#(X)), A \equiv (S \equiv X)$

Since $A$ believes $N_a$ to be fresh, we get:

$A \equiv (S \equiv A \nrightarrow B)$
BAN Logic: Analyzing the Protocol

The *Jurisdiction Rule* says that:

\[
A \equiv (S \rightarrow X), A \equiv (S \equiv X) \quad \frac{}{A \equiv X}
\]

From this we obtain:

\[
A \equiv A \overset{K_{ab}}{\rightarrow} B
\]

\[
A \equiv \#(A \overset{K_{ab}}{\rightarrow} B)
\]

Since A has also seen the part of the message encrypted under B’s key, he can send it to B. B decrypts the message and obtains:

\[
B \equiv (S \sim A \overset{K_{ab}}{\rightarrow} B)
\]

meaning that B believes that S once sent the key.

At this point, we need the final dubious assumption:

\[
B \equiv \#(A \overset{K}{\rightarrow} B)
\]

With it, we can get:

\[
B \equiv A \overset{K_{ab}}{\rightarrow} B
\]

Lessons

*Use of a logic like BAN shows what is provable and also what must be assumed.*

*Using BAN effectively requires a lot of practice and insight into the protocol.*

Next lecture: PGP