Attack these protocols

Shamir-Rivest-Adleman three-pass

Goal: secrecy of M.
Assumed equality: $\{\{x\}_k\}_{k'} \equiv \{\{x\}_{k'}\}_k$.

1. $A \to B$: $\{M\}_{K_a}$
2. $B \to A$: $\{\{M\}_{K_a}\}_{K_b}$
3. $A \to B$: $\{M\}_{K_b}$

(attacker finds M)

Repeated authentication (several authors)

Goal: A and B make sure they are alive.

1. $A \rightarrow B$: N_a
2. $B \rightarrow A$: $N_b, \{N_a\}_{K_{ab}}$
3. $A \rightarrow B$: $\{N_b\}_{K_{ab}}$

(attacker makes B believe A is alive without A doing anything))

Woo-Lam (one-way authentication)

Goal: B makes sure that A is alive.

$$
\begin{aligned}
&1.\ B \rightarrow A\colon N_b \\
&2.\ A \rightarrow B\colon \{N_b\}_{K_{as}} \\
&3.\ B \rightarrow S\colon B, \{A, \{N_b\}_{K_{as}}\}_{K_{bs}} \\
&4.\ S \rightarrow B\colon \{N_b\}_{K_{bs}}
\end{aligned}
$$

(attacker makes B believe A is alive without A doing anything)
(how to repair?)

Wide-mouthed frog

Goal: key exchange

$$1.\ A \rightarrow S\colon A, \{T_a, B, K_{ab}\}_{K_{as}}$$
$$2.\ S \rightarrow B\colon \{T_s, A, K_{ab}\}_{K_{bs}}$$

Andrew Secure RPC

Goal: exchange of a new key K'_{ab}

1. $A \rightarrow B$: $A, \{N_a\}_{K_{ab}}$
2. $B \rightarrow A$: $\{N_a + 1, N_b\}_{K_{ab}}$
3. $A \rightarrow B$: $\{N_b + 1\}_{K_{ab}}$
4. $B \rightarrow A$: $\{K'_{ab}, N'\}_{K_{ab}}$

Yahalom

Goal: mutual authentication of A and B, key exchange

1. $A \rightarrow B$: A, N_a
2. $B \rightarrow S$: $B, N_b, \{A, N_a\}_{K_{bs}}$
3. $S \rightarrow A$: $N_b, \{B, K_{ab}, N_a\}_{K_{as}}, \{A, K_{ab}, N_b\}_{K_{bs}}$
4. $A \rightarrow B$: $\{A, K_{ab}, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$

(attacker impersonates Bob to Alice)

Needham-Schroeder symmetric key

Goal: mutual authentication of A and B, key exchange

1. $A \rightarrow S$: A, B, N_a
2. $S \rightarrow A$: $\{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B$: $\{K_{ab}, A\}_{K_{bs}}$
4. $B \rightarrow A$: $\{N_b\}_{K_{ab}}$
5. $A \rightarrow B$: $\{N_b + 1\}_{K_{ab}}$

(attacker impersonates Alice to Bob)

Kao-Chow Authentication

Goal: mutual authentication of A and B, key exchange

1. $A \rightarrow S$: A, B, N_a
2. $S \rightarrow B$: $\{A, B, N_a, K_{ab}\}_{K_{as}}, \{A, B, N_a, K_{ab}\}_{K_{bs}}$
3. $B \rightarrow A$: $\{A, B, N_a, K_{ab}\}_{K_{as}}, \{N_a\}_{K_{ab}}, N_b$
4. $A \rightarrow B$: $\{N_b\}_{K_{ab}}$

Woo-Lam (key exchange)

Goal: mutual authentication of A and B, key exchange

1. $A \rightarrow B$: A, N_a
2. $B \rightarrow A$: B, N_b
3. $A \rightarrow B$: $\{A, B, N_a, N_b\}_{K_{as}}$
4. $B \rightarrow S$: $\{A, B, N_a, N_b\}_{K_{as}}, \{A, B, N_a, N_b\}_{K_{bs}}$
5. $S \rightarrow B$: $\{B, N_a, N_b, K_{ab}\}_{K_{as}}, \{A, N_a, N_b, K_{ab}\}_{K_{bs}}$
6. $B \rightarrow A$: $\{B, N_a, N_b, K_{ab}\}_{K_{as}}, \{N_a, N_b\}_{K_{ab}}$
7. $A \rightarrow B$: $\{N_b\}_{K_{ab}}$

(attacker impersonates Alice to Bob, inserts own key)

Needham-Schroeder public key

Goal: mutual authentication of A and B

Assume public keys are bound to names using certificates or smth.

1. $A \to B$: $\{\!|A, N_a|\!\}_{K_B}$
2. $B \to A$: $\{\!|N_a, N_b|\!\}_{K_A}$
3. $A \to B$: $\{\!|N_b|\!\}_{K_B}$