

Attacks on Authentication and Key Exchange Protocols

Gavin Lowe's attack on Needham-Schroder public key protocol

The attack involves an intruder that is able to impersonate A . Message exchanges with the public key server are ignored.

- 1.iii $A \rightarrow I : \{N_A, A\}_{K_I^+}$
- 2.iii $I(A) \rightarrow B : \{N_A, A\}_{K_B^+}$
- 2.vi $B \rightarrow I(A) : \{N_A, N_B\}_{K_A^+}$
- 1.vi $I \rightarrow A : \{N_A, N_B\}_{K_A^+}$
- 1.vii $A \rightarrow I : \{N_B\}_{K_I^+}$
- 2.vii $I(A) \rightarrow B : \{N_B\}_{K_B^+}$

The fix involves adding B 's identity to the response from B to A .

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : \{K_B^+, B\}_{K_S^-}$
3. $A \rightarrow B : \{N_A, A\}_{K_B^+}$
4. $B \rightarrow S : B, A$
5. $S \rightarrow B : \{K_A^+, A\}_{K_S^-}$
6. $B \rightarrow A : \{N_A, N_B, B\}_{K_A^+}$
7. $A \rightarrow B : \{N_B\}_{K_B^+}$

Denning-Sacco attack on Needham-Schroder shared key protocol

The attack assumes that the intruder I has recorded session 1 and that K_{AB} is compromised. After session 2, B believes that he shares K_{AB} only with A .

- 1.i $A \rightarrow S : A, B, N_A$
- 1.ii $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
- 1.iii $A \rightarrow I(B) : \{K_{AB}, A\}_{K_{BS}}$
Assume that K_{AB} is compromised.
- 2.iii $I(A) \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
- 2.iv $B \rightarrow I(A) : \{N_B\}_{K_{AB}}$
- 2.v $I(A) \rightarrow B : \{N_B - 1\}_{K_{AB}}$

The fix involves replacing the nonces with timestamps:

1. $A \rightarrow S : A, B$

$$2. S \rightarrow A : \{B, K_{AB}, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}}$$

$$3. A \rightarrow B : \{K_{AB}, A, T\}_{K_{BS}}$$

However, this fix (called the Denning-Sacco shared key protocol) had another flaw, it was susceptible to a multiplicity attack discovered by Gavin Lowe:

$$1.i A \rightarrow S : A, B$$

$$1.ii S \rightarrow A : \{B, K_{AB}, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}}$$

$$1.iii A \rightarrow B : \{K_{AB}, A, T\}_{K_{BS}}$$

$$2.iii I(A) \rightarrow B : \{K_{AB}, A, T\}_{K_{BS}}$$

Lowe's fix was to add a nonce handshake at the end of the exchange:

$$1. A \rightarrow S : A, B$$

$$2. S \rightarrow A : \{B, K_{AB}, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}}$$

$$3. A \rightarrow B : \{K_{AB}, A, T\}_{K_{BS}}$$

$$4. B \rightarrow A : \{N_B\}_{K_{AB}}$$

$$5. A \rightarrow B : \{N_B - 1\}_{K_{AB}}$$

Another fix proposed by Needham and Schroder used an initial handshake between A and B containing a nonce (N_B) to prevent the freshness attack:

$$1. A \rightarrow B : A$$

$$2. B \rightarrow A : \{A, N_B\}_{K_{BS}}$$

$$3. A \rightarrow S : A, B, N_A, \{A, N_B\}_{K_{BS}}$$

$$4. S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, N_B, A\}_{K_{BS}}\}_{K_{AS}}$$

$$5. A \rightarrow B : \{K_{AB}, N_B, A\}_{K_{BS}}$$

$$6. B \rightarrow A : \{N_B\}_{K_{AB}}$$

$$7. A \rightarrow B : \{N_B - 1\}_{K_{AB}}$$

Man-in-the-middle attack on Diffie-Helman key exchange protocol

The protocol does not guarantee authenticity:

$$1. I(A) \rightarrow B : p, g$$

$$2. I(A) \rightarrow B : g^{X_I} \pmod p$$

$$3. B \rightarrow I(A) : g^{X_B} \pmod p$$

$$4. \text{Shared key } K = g^{X_I X_B} \pmod p$$

$$1. A \rightarrow I(B) : p, g$$

$$2. A \rightarrow I(B) : g^{X_A} \pmod p$$

$$3. I(B) \rightarrow A : g^{X_I} \pmod p$$

$$4. \text{Shared key } K = g^{X_A X_I} \pmod p$$