

COMP3441/9441 Tutorial Week 7

Attacks on Authentication and Key Exchange Protocols

1. Needham-Schroder Public Key Protocol

- (a) Describe Gavin Lowe's attack on the Needham-Schroder public key protocol. The protocol goes as follows (K^+ denotes public key, K^- denotes private key):
- i. $A \rightarrow S : A, B$
 - ii. $S \rightarrow A : \{K_B^+, B\}_{K_S^-}$
 - iii. $A \rightarrow B : \{N_A, A\}_{K_B^+}$
 - iv. $B \rightarrow S : B, A$
 - v. $S \rightarrow B : \{K_A^+, A\}_{K_S^-}$
 - vi. $B \rightarrow A : \{N_A, N_B\}_{K_A^+}$
 - vii. $A \rightarrow B : \{N_B\}_{K_B^+}$
- (b) How can this problem be fixed?

2. Needham-Schroder Shared Key Protocol

- (a) Describe the Denning-Sacco attack on the Needham-Schroder shared key protocol. The protocol goes as follows (N is random number generated by A):
- i. $A \rightarrow S : A, B, N_A$
 - ii. $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
 - iii. $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
 - iv. $B \rightarrow A : \{N_B\}_{K_{AB}}$
 - v. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$
- (b) Is it enough to add timestamps to correct this flaw?
- (c) What is the problem of using timestamps in authentication protocols? Would the following solution (proposed by a student in this class) help overcome this problem?
- i. $A \rightarrow B : \{A, time_A\}_{K_{AB}}$
 - ii. $A \rightarrow B : \{A, time_A + 1\}_{K_{AB}}$
 - iii. A's times need not match B's, B only checks that the times differ by 1.

3. Diffie-Helman Key Exchange Protocol

- (a) Describe the man-in-the-middle attack on the Diffie-Helman key exchange algorithm. The protocol goes as follows:
- i. Let p be a prime and $2 \leq g \leq p - 1$
 - ii. $A \rightarrow B : p, g$
 - iii. $A \rightarrow B : g^{X_A} \pmod p$
 - iv. $B \rightarrow A : g^{X_B} \pmod p$
 - v. A and B compute shared key $K = g^{X_A X_B} \pmod p$
- (b) How can this problem be fixed?