Foundations of Computer Security

Lecture 60: The Needham-Schroeder Protocol

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Needham-Schroeder Protocol

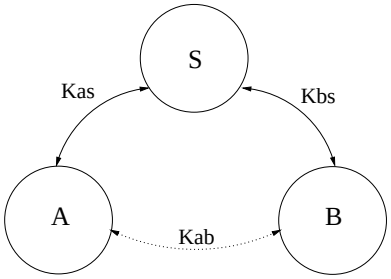
Many existing protocols are derived from one proposed by Needham and Schroeder (1978), including the widely used Kerberos authentication protocol suite.

N-S is a *shared-key authentication protocol* designed to generate and propagate a *session key*, i.e., a shared key for subsequent symmetrically encrypted communication.

Note that there is no public key infrastructure in place.

Assumptions of Needham-Schroeder

There are three principals: A and B, two principals desiring mutual communication, and S, a trusted key server.



It is assumed that A and B already have secure symmetric communication with S using keys K_{as} and K_{bs}, respectively.

Nonces and Timestamps

N-S uses *nonces* (short for "numbers used once"), randomly generated values included in messages.

If a nonce is generated and sent by A in one step and returned by B in a later step, A knows that B's message is *fresh* and not a replay from an earlier exchange.

Note that a nonce *is not a timestamp*. The only assumption is that it has not been used in any earlier interchange, with high probability.

Needham-Schroeder

Two questions to ask of any step in any protocol:

- *What is the sender trying to say with this message?*
- *What is the receiver entitled to believe after receiving the message?*

The Needham-Schroeder protocol is:

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. $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$

Here N_a and N_b are nonces.

Lessons

- Needham-Schroeder is a shared-key authentication protocol that has been very important historically.
- It illustrates:
  - the overall structure of protocols;
  - that some principals may have special roles to play;
  - the usefulness of nonces.

Next lecture: Attacks on Needham-Schroeder