Foundations of Computer Security

Lecture 62: The Otway-Rees Protocol

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

Otway-Rees

Another very important and much studied protocol is the Otway-Rees protocol. Below is one of several variants.

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

Here M is a session identifier; N_a and N_b are nonces.

What are the assumptions? What seems to be the goal? What might the principals believe after each step?

Attack on Otway-Rees

A malicious intruder can arrange for A and B to end up with different keys.

1. After step 3, B has received K_{ab}.
2. An intruder then intercepts the fourth message.
3. The intruder resends message 2, so S generates a new key K'_{ab}, sent to B.
4. The intruder intercepts this message too, but sends to A $M, \{N_a, K'_{ab}\}_{K_{as}}$.
5. A has K'_{ab}, while B has K_{ab}.

Another problem: although the server tells B that A used a nonce, B doesn't know if this was a replay of an old message.

A Flawed Protocol

Recall the following protocol, introduced previously.

1. $A \rightarrow B : \{\{K\}_{K_a^{-1}}\}_{K_b}$
2. $B \rightarrow A : \{\{K\}_{K_b^{-1}}\}_{K_a}$

Suppose an attacker C obtains the message (step 1): $\{\{K\}_{K_a^{-1}}\}_{K_b} = K'$. Then, C initiates a new run of the protocol with B:

1. $C \rightarrow B : \{\{K'\}_{K_c^{-1}}\}_{K_b}$
2. $B \rightarrow C : \{\{K'\}_{K_b^{-1}}\}_{K_c}$

The message that B sends back is:

$$\{\{K'\}_{K_b^{-1}}\}_{K_c} = \{\{\{\{K\}_{K_a^{-1}}\}_{K_b}\}_{K_b^{-1}}\}_{K_c} = \{\{K\}_{K_a^{-1}}\}_{K_c}$$

allowing C to extract the original K.

Lessons

- Otway-Rees is another important protocol historically.
- Like Needham-Schroeder it illustrates how difficult it is to build a secure cryptographic protocol.
- This is also illustrated by our simple public key protocol.

Next lecture: Protocol Verification