Foundations of Computer Security

Lecture 61: Attacks on Needham-Schroeder

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

Attacks on Protocols

Recall our earlier list of things to ask about a protocol.

- Are both authentication and secrecy assured?
- Is it possible to impersonate one or more of the parties?
- Is it possible to interject messages from an earlier exchange (replay attack)?
- What tools can an attacker deploy?
- If any key is compromised, what are the consequences?

Flaws in Needham-Schroeder

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

Denning and Sacco pointed out that the compromise of a session key has bad consequences. An intruder can reuse an old session key and pass it off as a new one as though it were fresh.

Suppose C has cracked K_{ab} from last week's run of the protocol, and has squirreled away message 3 from that session: $\{K_{ab}, A\}_{K_{bs}}$.

3. $C \longrightarrow B : \{K_{ab}, A\}_{K_{bs}}$
4. $B \longrightarrow C : \{N_b\}_{K_{ab}}$
5. $C \longrightarrow B : \{N_b - 1\}_{K_{ab}}$

B will believe it is talking to A.

Flaws in Needham-Schroeder

Problem: Message 3 is not protected by nonces. There is no way for B to know if the K_{ab} it receives is current. An intruder has unlimited time to crack an old session key and reuse it as if it were fresh.

Example Attack: an employee runs the first few steps of the protocol multiple times, gathering up tickets $\{K_{ab}, A\}_{K_{bs}}$ for each different server B in the system. If he's fired, he can still log onto all of the company's servers.

Flaws in Needham-Schroeder

Bauer, et al. pointed out that if key K_{as} were compromised, anyone could impersonate A and establish communication with any other party.

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

These flaws persisted for almost 10 years before they were discovered.

Is it Fair?

The "attacks" discovered by Denning and Sacco and by Bauer, et al. ask what happens if a key is broken.

Is it fair to ask that question? Isn't a presumption of any cryptographic protocol that the encryption is strong?

How might you address these flaws if you were the protocol designer?

Lessons

- Researchers have pointed out flaws in the N-S protocol.
- They illustrate how hard it is to make a protocol secure.

Next lecture: The Otway-Rees Protocol