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

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

$B$ will believe it is talking to $A$.

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

$A \rightarrow S : A, B, N_a$

$S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_K_{as}\}_K_{as}$

$A \rightarrow B : \{K_{ab}, A\}_K_{bs}$

$B \rightarrow A : \{N_b\}_K_{sb}$

$A \rightarrow B : \{N_b - 1\}_K_{sb}$

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

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?

- 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