Jan Rehwaldt, 2012-04-13, University of Tartu
Exercise 6, Principles of Secure Software Design

Will B be convinced that K_{AB} is fresh?

According to the attack description below K_{AB} may be hijacked by an attacker masquerading the initiator Ann. Therefore K_{AB} may not be fresh when using this protocol.

$$
\begin{array}{ll}
(1) & A \rightarrow B\colon\ A, N_a \\
(2) & B \rightarrow S\colon\ B, N_b, \{A, N_a, \}_{K_{bs}} \\
(3) & S \rightarrow A\colon\ N_b, \{B, K_{ab}, N_a\}_{K_{as}}, \{A, K_{ab}, N_b\}_{K_{bs}} \\
(4) & A \rightarrow B\colon\ \{A, K_{ab}, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}
\end{array}
$$

1. Ann send name A and nonce N_A (random number used to prove freshness) to Bob
2. Bob replies to server his name, an own nonce N_B, K_{BS} and {A + N_A} encrypted with Key K_{BS}
3. Server sends to Ann N_B, {B, K_{AB}, N_A} encrypted with K_{AS} and {A, K_{AB}, N_B} encrypted with K_{BS}
   a. {B, K_{AB}, N_A} shows name of target (B), session key (K_{AB}) and freshness of message (N_A)
   b. {A, K_{AB}, N_B} should be passed on to Bob
4. Ann sends chunk {A, K_{AB}, N_B} and N_B encrypted with session key to Bob

$$
\begin{array}{ll}
(1) & A \rightarrow B\colon\ \ A, N_a \\
(2) & B \rightarrow S\colon\ \ B, N_b, \{A, N_a\}_{K_{bs}}
\end{array}
$$

$$
\begin{array}{ll}
(1') & E_a \rightarrow B\colon\ A, (N_a, N_b) \\
(2') & B \rightarrow E_s\colon\ B, N'_b, \{A, N_a, N_b\}_{K_{bs}}
\end{array}
$$

$$
\begin{array}{ll}
(3) & \text{Omitted.} \\
(4) & E_a \rightarrow B\colon \{A, N_a(= K_{ab}), N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}
\end{array}
$$

For attacking this protocol attacker E may intercept the messages and send own messages in-between acting like Ann (after step 2).

1. Ann send name A and nonce N_A (random number used to prove freshness) to Bob
2. Bob replies to server own nonce N_B, K_{BS} and {A + N_A} encrypted with Key K_{BS}
   a. Attacker masquerades as Ann sending $N_E = N_A + N_B$ to Bob
   b. Bob replies to attacker his name, an new nonce N_{B2}, K_{BS} and {N_A + N_A} encrypted with Key K_{BS}
3. ~~Omitted~~: ~~Server sends to Ann N_B, {B, K_{AB}, N_A} encrypted with K_{AS} and {A, K_{AB}, N_B} encrypted with K_{BS}~~
4. Ann sends chunk {A, K_{AB}, N_B} and N_B encrypted with session key to Bob
5. Attacker sends encrypted chunk from omitted message {B, K_{AB}, N_B} and N_B encrypted with N_A, which became the session key K_{AB}, to Bob
6. Attacker overtook the communication masquerading Ann

Source:

A Taxonomy of Replay Attacks

Paul Syverson
Code 5543
Naval Research Laboratory
Washington, DC 20375
(syverson@itd.nrl.navy.mil)

What attack is possible if the intruder learns an old session key?

Session may be recovered, **overtaken by impersonation** or if messages are stored for requesting them depending on the session they may be obtained later on. Additionally if the session key is used for de- and encryption caught encrypted messages may be decrypted with this information. Therefore session keys may be assumed as being secret, especially after their expiration.