Protokollsicherheit  
Exercise Sheet 5

Exercise 5-1. (Proverif – Medium)  In the last tutorial, we were not able to finish the Proverif specification of the fourth and fifth protocols described in the first set of slides. Try them out by yourselves.

Exercise 5-2. (Proverif – Medium)  Consider the scenario where two principals $A$ and $B$ already share a session key $K_{AB}$, but they want to re-new this key by a fresh key $K'_{AB}$ and use this key instead. The following protocol is an attempt to do so, where the nonce $N_A$ is generated by $A$ and the nonces $N_B, N'_B$ are generated by $B$:

1. $A \rightarrow B : \{N_A\}_{K_{AB}}$
2. $B \rightarrow A : \{N_A + 1, N_B\}_{K_{AB}}$
3. $A \rightarrow B : \{N_B + 1\}_{K_{AB}}$
4. $B \rightarrow A : \{K'_{AB}, N'_B\}_{K_{AB}}$

This protocol is flawed in at least two ways. The first problem is that there is no assurance that the key $K'_{AB}$ is fresh. The second problem is a type attack. In particular, the intruder can use message 2 as the message 4, where $A$ thinks that $N_A + 1$ is a fresh key.

Specify the protocol above in Proverif and find these two attacks.

Exercise 5-3. (Proverif – Medium)  The following protocol is an attempt to fix the protocol shown in Exercise 5-2:

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow A : \{N_A, K'_{AB}\}_{K_{AB}}$
3. $A \rightarrow B : \{N_A\}_{K'_{AB}}$
4. $B \rightarrow A : N'_B$

The goal is the same as the previous protocol, namely, re-new the session key with a fresh key $K'_{AB}$. The last message is only used to indicate $A$ that $B$ is ready to continue communication with the new key.

Unfortunately, this protocol is also flawed! Find the attack using Proverif.

Exercise 5-4. (Proverif – Hard)  Find a fix to the protocol described in 5-3? Verify that your corrected protocol is indeed correct in Proverif.