Assignment 2, part 4

By Staffan Lundström

There is a bug in the protocol. Consider the following situation:

C has intercepted and saved a messages from previous authentications between A and B, where A initiated the conversation, so C has $\{r1_{A,}\, B\}_A$.

Now A and C are talking. A sends ($\{r2_A, C\}_A$, A's cert) to C.

Meanwhile C sends ($\{r1_A, B\}_A$, A's cert) to B
B answers ($\{r1_A, r_B, A\}_B$, B's cert) to C

Now C replies ($\{r2_A, r_B, A\}_C$, C's cert) to A.
A answers $\{r_B\}_A$ to C.

C uses $\{r_B\}_A$ to send $\{r_B\}_A$ to B.

What has happened is that B and C are talking and B think that C is A.

This bug could be fixed by adding A and B in the last message of the three authentication messages. That means $\{r_B, A, B\}_A$ instead of $\{r_B\}_A$ if A and B are initiating a session, where A started.