Problem 1. [15 points]

Does assertion $\text{Inv } B_3$ hold for program Protocol, where

$$B_3 : (\exists (A.S) \Rightarrow \psi(A.S))$$

Solution

It holds.

We have already shown that $\text{Inv } \psi(K)$ holds (in the Note). So $\text{Inv } \psi(K+1)$ also holds. [5 points]

Neither $A$ nor $B$ send out anything encrypted by $K+1$. [5 points]

So the only way the attacker can compute $\text{enc}(K+1, A.nA + A.nB)$ is if $A.nA + A.nB$ is some silly thing like $\text{dec}(K+1, K+1)$. But this is not the case because $A.nA$ is randomly computed and the attacker cannot influence it. [5 points]
Problem 2. [15 points].

Does assertion Inv $B_4$ hold for Protocol, where

$B_4 : \forall (i \in \text{hst.keys}) : [B,S] = \text{hst}[i] \Rightarrow ([A,S] \in \text{hst}[0..i-1])$

Solution attempt 1

Let’s try to prove it.

Suppose $[B,\text{enc}(K+1,xA+xB)]$ enters hst at time $t_0$, where $B.nB$ equals $xB$ and $B.nA$ equals $xA$. So at $t_0$, $B$ receives $[A,B,2,\text{enc}(K,xB),\ldots]$.

Suppose $B.nB$ was set to $xB$ at time $t_1$ ($< t_0$). At $t_1$, $B$ receives $[A,B,1,xA]$ and responds with $[B,A,1,xB,\text{enc}(K,xA)]$. During $(t_1,t_0)$, $B$ is idle (otherwise its $nB$ would not be $xB$ at $t_0$).

At some time $t_2$ where $t_1 < t_2 < t_0$ holds, $A$ sends $[A,B,2,\text{enc}(K,xB),\ldots]$. (The attacker couldn’t have sent it because it does not have $K$ (proved earlier)). So at $t_2$, $A$ receives $[B,A,1,xB,\text{enc}(K,A.nA)]$ and adds $[A,\text{enc}(K+1,A.nA+xB)]$ to hst.

So if $A.nA$ equals $xA$ (which is what $B.nA$ equals), then Inv $B_4$ would hold. Could the attacker arrange it so that $A.nA$ is not $xA$? Think about it.

Solution

Let’s try to disprove it. Below, “msg $I$” means the message sent in step $I$.

1. Initial step.
   After this: $A.nA = yA; [A,B,1,yA]$ in chan.
2. $B$ receives msg 1 (i.e., msg sent in step 1).
   After this: $B$ is at 2; $B.nA = yA; B.nB = yB; [B,A,1,yB,\text{enc}(K,yA)]$ in chan.
3. Attacker receives msg 2 and sends $[A,B,2,zA,\ldots]$ where $zA$ is not $yA$.
4. $B$ receives msg 3 and goes back to 1 without updating hst (because $zA$ does not equal $\text{enc}(K,yB)$).
   After this: $B$ is at 2; $B.nA = zA; B.nB = zB; [B,A,1,zB,\text{enc}(K,zA)]$ in chan.
7. Attacker receives msg 6, changes the last field to $\text{enc}(K,yA)$ (which it had read in step 3), and sends $[B,A,1,zB,\text{enc}(K,yA)]$.
8. $A$ receives msg 7 and updates hst (because it gets the response it expects).
   After this: hst = $[[A,\text{enc}(K+1,yA+zB)]; [A,B,2,\text{enc}(K,zB),\ldots]$ in chan.
9. $B$ receives msg 8 and adds $[B,\text{enc}(K+1,zA+zB)]$ to hst.
   After this: hst = $[[A,\text{enc}(K+1,yA+zB)]; [B,\text{enc}(K+1,zA+zB)].$

$A_4$ does not hold.

So Inv $A_4$ does not hold.

Can you come up with a simpler counter-example evolution?