CS259 - Security Analysis of Network Protocols

Winter Quarter, 2006
Solutions for Homework #2

January 31, 2006

Problem 1

In this problem, you were asked to modify the AVISPA code so as to demonstrate the Needham Schroeder man in the middle attack. The given AVISPA code does not specify sessions that involve honest principals starting conversations with an intruder. This prevents the model checker from being able to find a flaw in the given model. A reasonable modification is to *add* the following lines to the definition of the environment role.

```
/\ session(a,i,ka,ki)
/\ session(i,a,ki,ka)
/\ session(i,b,ki,kb)
/\ session(b,i,kb,ki)
```

Strictly speaking, adding the first line will find you the attack. In general, it is good to model all the different conversations that could possibly take place.

Problem 2

In this problem, you were asked to implement Lowe's fix to Needham Schroeder. The fix involves modifying certain message formats to include the identity of the responder.

- In the definition of role Alice, change line 37 from:

```
    2.  State  = 2 /\ RCV({Na.Nb'}_Ka) =|>
```

  to

```
    2.  State  = 2 /\ RCV({B.Na.Nb'}_Ka) =|>
```

- In the definition of role Bob, change line 58 from:

```
    State':= 3 /\ Nb' := new() /\ SND({Na'.Nb'}_Ka)
```

  to

```
    State':= 3 /\ Nb' := new() /\ SND({B.Na'.Nb'}_Ka)
```