Security Protocols

2016/2017

C. Ene *ML. Potet*

Exercices

All files needed for this session are available at: `http://www-verimag.imag.fr/~ene/m2p/`
The Avispa web page is `http://www.avispa-project.org/`

Each provided file begin with a commentary that contains the description of the protocol. All the properties are specified in the *Goal* section, and they are checked sequentially.

Exercise 1

1. Download and open the file NSPK_1.hlpsl where there is only one session between two honest participants. Check that Avispa does not find any attack on the protocol using the OFMC or CL-ATSE back-end.

2. Download and open the file NSPK_2.hlpsl . Now the intruder is involved and the property we check is the secret of the exchanged nonces. Analyze the protocol and interpret the results you get.

3. Download and open the file NSPK_3.hlpsl . We check the same scenario, but the property we are interested in, is the authentication one. Analyze the protocol and compare the results you get with the previous one.

4. Try to fix the attacks above, and check your corrected version using Avispa. Compare your correction with the NSPK-fix proposed on AVISPA web site in the section Library of protocols.

Exercise 2

1. Download and open the file Ex2_A.hlpsl . The property we check is the secret of the generated session key. Analyze the protocol and interpret the results you get.

2. The file Ex2_B.hlpsl contains a slightly corrected version. Analyze this version of the protocol and interpret the results you get (try to explain why the previous attack is not possible anymore).

3. The file Ex2_C.hlpsl contains the same protocol as Ex2_B.hlpsl, but now we check for the mutual authentication property. Analyze the protocol and interpret the results you get.

4. Try to fix the attack above, and check your corrected version using Avispa.

Exercise 3

1. Download and open the file NSPKxor.hlpsl . Analyze the protocol and interpret the results you get.

2. Specify the secrecy property for responder's nonce, verify this property and interpret the results you get. In order to do this, you have to add a new *protocol_id* in the *environment* role and to complete the description of the roles and the *goal* section.

3. Specify the authentication property for responder (of initiator to responder) using the initiators's nonce (Na), verify this property and interpret the results you get.

4. Specify the authentication property for responder (of initiator to responder) using the responder's nonce (Nb), verify this property and interpret the results you get.

5. Declare Na variable as nonce (use the type *text*), and verify the obtained protocol using the OFMC back-end and the "–typed_model" option set to yes or no, and interpret the results.

Exercise 4

1. Download and open the file AS_RPC_1_W.hlpsl . Analyze the protocol and interpret the results you get.

2. Change the weak authentication property of responder to initiator on Kpab to the strong authentication property and verify this property. Interpret the results you get.

3. Add and translate in HLPSL the following steps at the end of the protocol:

   ```
   5. A --> B : {Nap}_|Kpab|
   6. B --> A : {Succ(Nap)}_|Kpab|
   ```

   Verify the strong authentication property of responder to initiator on Kpab, for the new obtained protocol. Explain the results you get.

Exercise 5

Translate in HLPSL the Diffie-Helman protocol, where Na, Nb and Secret are nonces of type text and G is also of type text, but public.

```
1. A --> B : G^|Na|, {N}_|Kb|
2. B --> A : G^|Nb|, {N}_|Ka|
3. A --> B : {Secret}_|(G^Na)^Nb|
```

1. Simulate your protocol.

2. Specify the secret property of the variable Secret.

3. Check this property.

4. Simulate the Man-in-the-middle attack.

5. Try to correct the protocol in order to get secrecy of Secret, and verify your corrected version.