

F. Autreau
P. Lafourcade
JL. Roch

P. Lafourcade.

SET 7

Date: 17.11.2008

SETUP All files needed for this session are available on the lecture web page:
http://www-verimag.imag.fr/~plafourc/teaching/Master_Pro_2_2008_2009.php

1. First check you have internet connection with cache: www-cache.ujf-grenoble.fr:3128
2. Download the script called: `install-verif-tools08-09.sh`
3. Put it in your home file and execute it.

```
sh install-verif-tools08-09.sh
```

4. Export variable written on my webpage

Recall For using Avispa the command line is `avispa`, for scyther is `scyther-guy.py` and for proverif is `analyzer`. With Avispa you need to specify the tool used for instance by typing “`avispa toto.txt -ofmc`”. You should use proverif in horn clause using the following command “`analyzer -in horn toto.txt`”.

Exercise 1

AVISPA:

1. Use AVISPA (<http://www.avispa-project.org/>) to analyze Needham Schroder protocol, called NSPK with the 4 Tools (OFMC, Cl-Atse, SATMC and TA4SP) using the web interface and also the command line.
Hint: For the command line use `avispa -help` in an xterm.
2. Understand the different results given by the Tools.
3. Copy the NSPK protocol in a file called NSPK-Lowe and correct by yourself the protocol with Lowe correction, using AVISPA in command line on your computer.
4. Check your corrected version and compare your result with NSPK-fix given on AVISPA web site.

Exercise 2

SCYTHER:

Now open in Scyther the file `protocol1.spdl` downloaded on the lecture webpage using:

```
scyther-gui.py protocol1.spdl
```

- a) Verify the security claims in the protocol using Scyther (Press F1). You find several attacks. Explain the attacks: why is the property violated in each case?
- b) Copy the protocol file to your own directory, and call it `protocol1fixed.spdl`. In the file, make sure you change 'protocol1' to 'protocol1fixed'. Improve the protocol such that the property now holds, and use Scyther to show that your improved protocol indeed meets the requirements.

Hint: Examine the first message: $\{\mathbf{R}, ni\}_{pk(R)}$ or compare the protocol to the fixed Needham-Schroeder protocol shown in the lecture.

Exercise 3

SCYTHER: Open in Scyther the file `protocol2.spdl` downloaded on the lecture webpage. This protocol contains a rather large messages and contains many random numbers (nonces) and hash functions. Not all of these elements are necessary to guarantee the correctness of the protocol.

- Suggest five efficiency improvements (in terms of message size or complexity) for the protocol, and motivate your choice. Test each suggested improvement using Scyther. If any of your suggestions fails, explain why.

Exercise 4

Proverif with Horn Clauses:

1. Check the file `needham.horn` with `proverif` (cf my web page).

Hint use `analyzer -help` to get some help in a terminal:

```
analyzer -in horn needham.horn
```

2. Understand the attack found
3. Correct it.

Exercise 5

Consider now the following modified version of NSPK protocol, called NSPKXor.

```
A --> B: {Na, A}_Kb
B --> A: {Nb, xor(Na, B)}_Ka
A --> B: {Nb}_Kb
```

Use OFMC and Cl-Atse to check this protocol in presence of XOR.

Exercise 6

AVISPA, Cl-Atse and OFMC:

1. Model in Avispa the following protocol, where KS is the public key of the server.

```
A --> S : A, B, {A + NA }KS
A --> S : {NA + B}KS , {NA + c}KS
B --> S : B, A, {B + NB }KS
B --> S : {NB + A}KS , {NB + c}KS
S --> A : K + {NA }KS
S --> B : K + {NB }KS
```

2. Does exist an attack?
3. Modify the protocol in order to model the following property $\{A + NA\}KS = \{A\}KS + \{NA\}KS$
4. Do you find an attack?

Exercise 7

Proverif and XOR:

Using the framework propose by Ralf Kuesters in the following article: “R. Küsters and T. Truderung: Reducing Protocol Analysis with XOR to the XOR-free Case in the Horn Theory Based Approach. In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS 2008).” You find the tool at the following URL: http://www.infsec.uni-trier.de/publications_tml/KuestersTruderung-XORPROVERIF-2008.zip

1. Install swi-prolog (<http://www.swi-prolog.org/>), it means:

- As root install alien : `su -c "apt-get install alien"`
- Download the RPM package on the webpage.
- Convert .rpm in .deb using alien: `alien pkg.rpm`
- Install the debian package: `dpkg -install pkg.deb`

2. Download the file, unzip it and read the README file.
3. Edit the file xlpt and change the first line by:

```
#! /usr/local/bin/pl -q -s
```

4. Try examples given with the tool (you should modify the tool file, by indicating the current path of swi-prolog)
5. Model in Horn clause the following protocol (same as in previous exercise), using example given by Ralf Kuesters.

$A \rightarrow S : A, B, \{A + NA\}_{KS}$
 $A \rightarrow S : \{NA + B\}_{KS}, \{NA + c\}_{KS}$
 $B \rightarrow S : B, A, \{B + NB\}_{KS}$
 $B \rightarrow S : \{NB + A\}_{KS}, \{NB + c\}_{KS}$
 $S \rightarrow A : K + \{NA\}_{KS}$
 $S \rightarrow B : K + \{NB\}_{KS}$

6. Does exist an attack?

7. Modify the protocol in order to model the following property $\{A + NA\}_{KS} = \{A\}_{KS} + \{NA\}_{KS}$

8. Do you find an attack?