University of Stuttgart
Institute of
Information Security

Security and Privacy
Summer Term 2018
Prof. Dr. Ralf Küsters

Homework 1

Submission into the *red SEC mailbox* in front of Room 2.041 until May 15, 2018, 14:00.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants
  (see ILIAS for contact information).
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk losing points.

Remarks for This Homework

You need the AVISPA tool *cl-atse* to solve two of the following problems. You can find the tool, including some sample specifications of the Needham-Schroeder and the Needham-Schroeder-Lowe protocols, in the ILIAS course. Note that a short demonstration of the tool, including its specification language, will be given in the lecture. You may want to wait with solving the tasks about AVISPA until after the demonstration.

To execute *cl-atse* under linux, you first have to adjust the environment variables in your shell as follows:

```
# Assumption: avispa.zip has been extracted into a folder "avispa" in your home directory.
#
# Extend execution path
export PATH=$PATH:$HOME/avispa
# Set path of hlpsl2if
export HLPSL2IF=$HOME/avispa/hlpsl2if
```

If you get an error from the "libncurses.so.5" library while running cl-atse, please ensure that you have the 32 bit version of libncurses 5 installed. For example, in case you are running Ubuntu (or one of its derivatives) you can use the following command to install the correct version of the library:

```
sudo apt install lib32ncurses5
```

The solutions to the problems that use AVISPA should be uploaded to the ILIAS course as a single .zip file per group. All other solutions should be handed in just as for Homework 0.

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

Problem 1: Specification of Protocols (4 points)

Provide a formal specification of the Woo and Lam Mutual Authentication Protocol (see Homework 0) according to the formal definition of protocols as introduced in class. More precisely, specify one instance of an initiator A talking to B (and S), one instance of a responder B talking to A and S, and one instance of a server S talking to B (and A).

Problem 2: Attacks on Protocols (4 points)

Provide a formal description of the informally described attack on the Woo and Lam Mutual Authentication Protocol (see sample solution of Homework 0 as presented in the exercise) in terms of the formal definition of attacks presented in class. Use *two* copies of the instance of a responder B talking to A (and S) as specified for Problem 1. Your attack should show that the Woo and Lam Mutual Authentication Protocol as specified belongs to $\mathrm{INSECURE}$.

Problem 3: Security Proof by Hand (4 points)

We consider the protocol $P = (\{\Pi_1, \Pi_2\}, \mathcal{W})$ with

$$\begin{aligned} \mathcal{W} &= \{I, A, B\} \\ \Pi_1 &= I \rightarrow \{\langle K, A\rangle\}^s_{K_{AB}} \\ \Pi_2 &= \{\langle x, A\rangle\}^s_{K_{AB}} \rightarrow \{\text{secret}\}^s_x \ , \end{aligned}$$

where $I, A, B, K, K_{AB},$ secret are constants and x is a variable. Prove that P, as modeled above, is secure, i.e., that there does not exist a successful attack on P as defined in the lecture, and hence, $P \notin \textsc{Insecure}$. In your proof, you may use informal arguments about the derivability and non-derivability of messages.

Problem 4: AVISPA Tool: Woo and Lam Attack (4 points)

Use the AVISPA tool to uncover the known attack on the Woo and Lam Mutual Authentication Protocol (i.e., the attack from the sample solution of Homework 0 as presented in the exercises).

Provide the .hlpsl file containing the Woo and Lam protocol and the output of the AVISPA tool in the solution that you upload to ILIAS.

Remark: Use the options `-notype -v -ns -short` for `cl-atse`.

Problem 5: AVISPA Tool: Woo and Lam Fix (4 points)

Propose a fix for the Woo and Lam protocol. Use the AVISPA tool to check that your solution works, i.e., it prevents the attack that you uncovered in the previous problem.

In your solution, provide a short description of your proposed fix, the .hlpsl file containing your fixed protocol, and the output produced by AVISPA.

Remark: Use the options `-notype -v -ns -short` for `cl-atse`.

Problem 6: Reduction from G3C (4 points)

Show that the problem INSECURE is NP-hard by reduction from the graph 3-coloring problem G3C. (G3C is the set of graphs which are 3-colorable, i.e., the nodes of the graph can be colored with 3 colors such that every pair of connected nodes has different colors. It is well known that G3C is NP-complete.)

Hint: The reduction from G3C is similar to the reduction from 3SAT. You have to encode a graph G by a protocol P_G such that $P_G \in$ INSECURE if and only if $G \in$ G3C.