Publication: 23.1.2019
Submission: 6.2.2019

Exercise Sheet 2: Security Protocol Analyses

Verification using CSP/FDR

The modelling of the Needham Schroeder protocol for the refinement checker FDR was discussed in detail during the lecture on January 16th and and also in the exercise on January 21st. The source file is available at the following link.

`https://www.informatik.tu-cottbus.de/~helke/swsec/nsp.csp`

Take this file as a template and adapt the model to describe the behaviour of the naive version of the Needham Schroeder protocol (symmetric variant, see Slide 4 of the lecture on January 9th). Note you should model all three protocol steps, which means that you have to model three different processes (*initiator*, *responder* and *server*). The aim of the modeling and the subsequent analysis is to show a weakness of this protocol variant. You should focus on a *Man-in-the-middle attack*. How this attack works was also presented during the lecture on January 9th.

If you plan to install FDR on your own computer, please follow the instructions at

`http://www.cs.ox.ac.uk/projects/fdr/`

Note the newest distribution is FDR4. There is also a documentation for the FDR available.

If you don't like to install FDR on your own machine, you should use the installation on the computers of the pool room (use linux CentOS). Note that FDR3 is installed under the path

/home/helke/tools/fdr/bin

By invoking *fdr3* you start the GUI variant of the program. It is also possible to use FDR without GUI (only in batch-mode). To do this, you must invoke *refines*.

Verification using BAN Logic

Use the BAN logic to derive the following property for the Kerberos protocol.

B **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$

Based on this, you have further to derive the following property.

B **believes** A **believes** $A \overset{K_{AB}}{\longleftrightarrow} B$

The reduction rules, the idealized version of the protocol and the assumptions for the Kerberos protocol are already given. Furthermore, you need the following product rule.

$$\frac{P \textbf{ believes } Q \textbf{ believes } (X, Y)}{P \textbf{ believes } Q \textbf{ believes } Y}\,.$$

General Instructions

The exercises should be solved in group work. A PDF document is expected as a solution for the second subtask. For the first subtasks, you submit the CSP/FDR codes you have created. Please do not forget to include the title page with the names of the group members. Solutions shall be submitted no later than 6 February 2019.

BAN-Logic

Rules

Message Meaning Rules

$$\frac{P \textbf{ believes } Q \overset{K}{\longleftrightarrow} P,\ P \textbf{ sees } \{X\}_K}{P \textbf{ believes } Q \textbf{ said } X} \quad \text{(symm.)}$$

$$\frac{P \textbf{ believes } Q \overset{K}{\mapsto} P,\ P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ believes } Q \textbf{ said } X} \quad \text{(asymm.)}$$

$$\frac{P \textbf{ believes } Q \overset{Y}{\rightleftharpoons} P,\ P \textbf{ sees } \langle X \rangle_Y}{P \textbf{ believes } Q \textbf{ said } X} \quad \text{(shared secrets)}$$

Nonce Verification Rule

$$\frac{P \textbf{ believes fresh } X,\ P \textbf{ believes } Q \textbf{ said } X}{P \textbf{ believes } Q \textbf{ believes } X}$$

Jurisdiction Rule

$$\frac{P \textbf{ believes } Q \textbf{ controls } X,\ P \textbf{ believes } Q \textbf{ believes } X}{P \textbf{ believes } X}$$

Component Visibility Rules

$$1.\ \frac{P \textbf{ sees } (X, Y)}{P \textbf{ sees } X} \qquad 2.\ \frac{P \textbf{ sees } (X, Y)}{P \textbf{ sees } Y} \qquad 3.\ \frac{P \textbf{ sees } \langle X \rangle_Y}{P \textbf{ sees } X}$$

$$4.\ \frac{P \textbf{ believes } Q \overset{K}{\longleftrightarrow} P,\ P \textbf{ sees } \{X\}_K}{P \textbf{ sees } X}$$

$$5.\ \frac{P \textbf{ believes } Q \overset{K}{\mapsto} P,\ P \textbf{ sees } \{X\}_K}{P \textbf{ sees } X}$$

$$6.\ \frac{P \textbf{ believes } Q \overset{K}{\mapsto} P,\ P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ sees } X}$$

Freshness Rule

$$\frac{P \textbf{ believes fresh } X}{P \textbf{ believes fresh } (X, Y)}$$

Annotation Rule

$\{X\}$

$P \to Q : Y$

$\{X, Q \textbf{ sees } Y\}$

Additional Product Rule

$$\frac{P \textbf{ believes } Q \textbf{ believes } (X, Y)}{P \textbf{ believes } Q \textbf{ believes } Y}$$

Idealized Kerberos-Protocol

1. $S \to A : \{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B, \{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{BS}})\}_{K_{AS}}$
2. $A \to B : (\{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{BS}}, \{(T_A, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{AB}})$
3. $B \to A : \{(T_A, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{AB}}$

Assumptions for Kerberos-Protocol

$$
\begin{array}{ll}
A\ \textbf{believes}\ A \xleftrightarrow{K_{AS}} S, & B\ \textbf{believes}\ B \xleftrightarrow{K_{BS}} S, \\
S\ \textbf{believes}\ A \xleftrightarrow{K_{AS}} S, & S\ \textbf{believes}\ B \xleftrightarrow{K_{BS}} S, \\
S\ \textbf{believes}\ A \xleftrightarrow{K_{AB}} B, & \\
A\ \textbf{believes}\ (S\ \textbf{controls} A \xleftrightarrow{K_{AB}} B), & \\
B\ \textbf{believes}\ (S\ \textbf{controls} A \xleftrightarrow{K_{AB}} B), & \\
A\ \textbf{believes fresh}\ (T_S), & B\ \textbf{believes fresh}\ (T_S), \\
B\ \textbf{believes fresh}\ (T_A), & A\ \textbf{believes fresh}\ (T_A).
\end{array}
$$