AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D2.4: Interface

Abstract

We describe the AVISPA Tool Interface for the security protocol analysis back-ends used in the AVISPA project, namely OFMC, CL-AtSe, SATMC and TA4SP. The interface features a user friendly web front-end that is detailed described in a user manual format.

Deliverable details

Deliverable version: *v1.0*	Person-months required: *2*
Date of delivery: *14.07.2005*	Due on: *01.07.2005*
Classification: *public*	Total pages: *9*

Project details

Start date: *January 1st, 2003*
Duration: *30 months*
Project Coordinator: *Alessandro Armando*
Partners: *Università di Genova, INRIA Lorraine, ETH Zürich, Siemens AG*

Information Society Technologies

Project funded by the European Community under the *Information Society Technologies* Programme (1998-2002)

1 Introduction

The AVISPA Tool Web Interface is a graphical front-end to the Avispa Tool v1.0, which provides a suite of applications for the analysis of formal models of security protocols.

It consists of an interactive set of dynamically generated HTML [6] pages which allows the invocation of the four backends OFMC, CL-AtSe, SATMC and TA4SP with the respective options.

By using the interface, users can easily load a protocol specification among the ones provided or write a specification on their own, and invoke one of the backends. In case an attack is found, the attack trace is also output in a graphical format, using Message Sequence Charts.

Different users may have different needs and skills, and that's why we created two kinds of user interaction. The web interface is then composed of a *basic* and an *expert mode*. In this document we describe all the features of both modes and provide a reference manual for the installation and the use of the interface.

2 Web-based Interface

The web-based interface is an interactive set of HTML pages dynamically generated by PHP [5]. One of the main advantages of an on-line tool/interface is that users will always be using the latest version of the analysis tools and do not have to worry about handling different tools versions and doing manual installations. However, if desired, the interface can also be installed locally, on the user machine, for an off-line use.

To launch the web interface users only need to point their web-browsers to the appropriate URL. Currently the interface is on-line at `http://www.avispa-project.org/web-interface`. To install the interface locally, users need a running web-server on their machines.

2.1 Modes

There are two available modes in the web-interface, the *basic mode* and the *expert mode*. While the basic mode is conceived for the inexperienced user (the backends execute over any HLPSL specification with a default set of options), in the expert mode more skilled users can choose which backend to run and customise the analysis by selecting different options.

Tools	Options
OFMC	No Executability check, Unbounded Search Depth
CL-AtSe	IF simplification, Depth-first Search, Unbounded Search Depth
SATMC	SIM Solver, Graphplan Encoding, Abstraction/Refinement enabled, Compound Types enabled, Optimised Intruder disabled, Max Depth=10
TA4SP	Over-Approximation, Two Agents Only

Table 1: Default Tools Options in the Basic Mode

2.1.1 Basic Mode

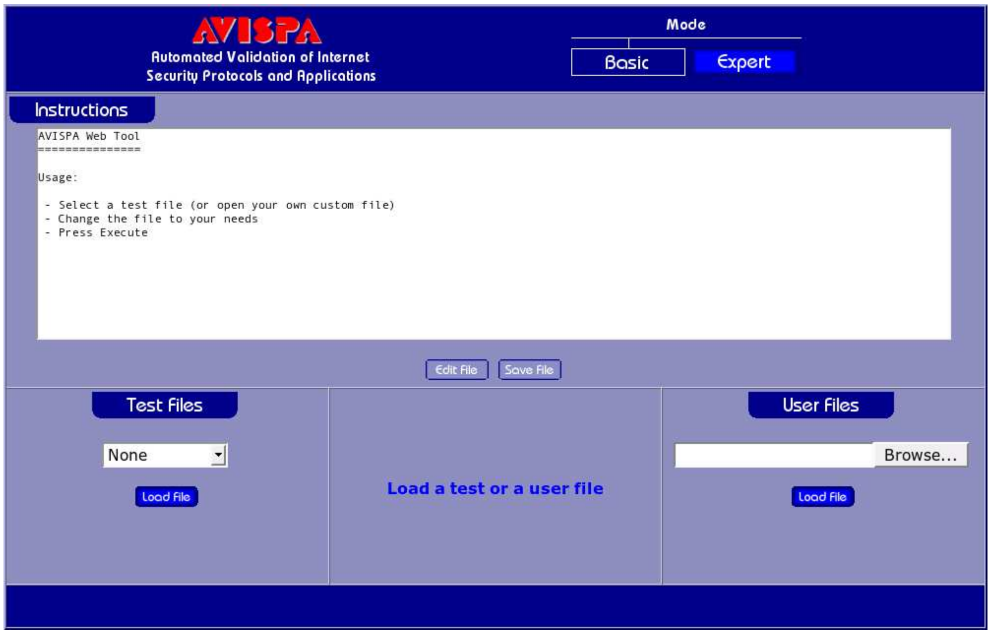
In the basic mode the interaction of the user is reduced to the minimum: he can load a protocol from the list provided and press the Execute button. The user can not change individual tool options. When the Execute button is pressed, the interface calls all backends using the default options specified by the tool developers (see Table 1).

Figure 1 shows the basic mode start screen. We can divide the basic mode start screen in 3 different parts.

1. The **upper bar**, contains the AVISPA logo and the buttons to switch between basic and expert mode.

2. The **presentation panel**, which is located just bellow the upper bar, initially presents the instructions on how to use the interface. This panel has multiple uses, it is also used to show the loaded protocol specifications and the results of the analysis process.

3. The **control panel**, the lower part of the page, contains two methods for protocol file selection: either the user can load a specification (available in a drop-down list on the left) from the testsuite, or he can load his own HLPSL protocol specification [3] from the local filesystem. The area in the middle of the control panel is dedicated to present instructions about what the user can do next, according to what the user is currently doing.



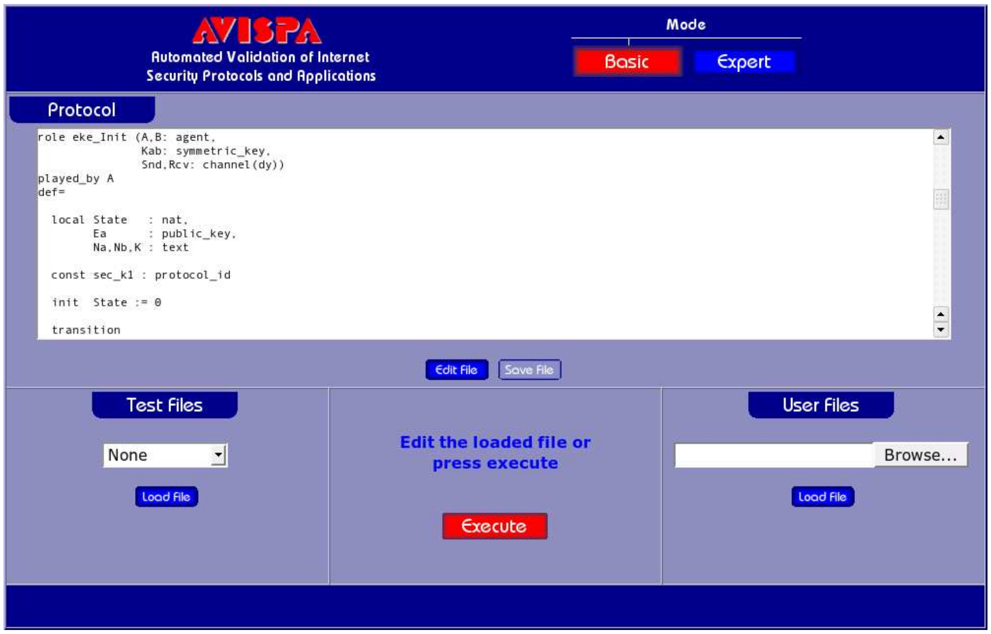
```
AVISPA Web Tool
===============

Usage:

 - Select a test file (or open your own custom file)
 - Change the file to your needs
 - Press Execute
```

Load a test or a user file

Figure 1: Basic Mode

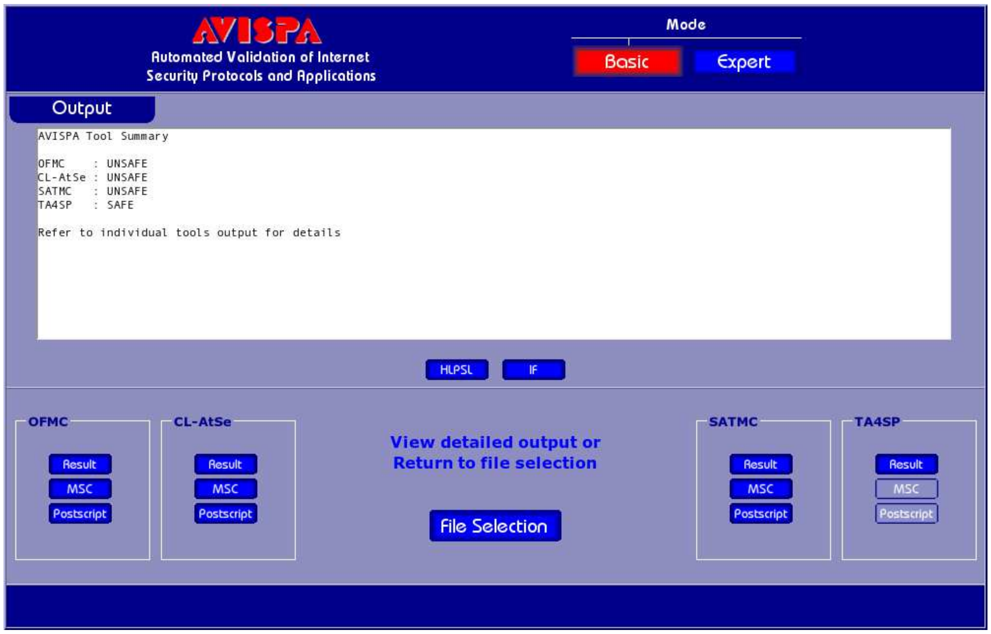
The web interface serves two purposes, the first being of a demonstration tool, and that's why there is an option to load test files, which were previously specified by the AVISPA team. The second purpose is the one of an interface for the AVISPA users to load their own files. Figure 2 shows what happens when a file is loaded in the interface. The file is shown in the presentation panel, the EDIT button is enabled and an EXECUTE button appears in the middle area of the control panel. Although the user can edit the specifications in the interface, the presentation panel is not conceived to be an advance editor, only basic edition capabilities are available in this panel. A third party text editor, like Emacs [4] , is recommended for advanced editing. Pressing the execute button runs all the four analysis tools over the same protocol specification and the results are shown in a new screen, Figure 3. The output screen shows a summary with the result of each tool and some buttons that enable the visualisation of the results in different formats. In the output screen the user can get:

- the protocol specification, the HLPSL file;
- the corresponding Intermediate File (IF);
- the output of each tool;
- the Message Sequence Chart (MSC) of the attack trace;



```
role eke_Init (A,B: agent,
               Kab: symmetric_key,
               Snd,Rcv: channel(dy))
played_by A
def=

  local State    : nat,
        Ea       : public_key,
        Na,Nb,K  : text

  const sec_k1 : protocol_id

  init  State := 0

  transition
```

Figure 2: Basic Mode - File Loaded



```
AVISPA Tool Summary

OFMC    : UNSAFE
CL-AtSe : UNSAFE
SATMC   : UNSAFE
TA4SP   : SAFE

Refer to individual tools output for details
```

Figure 3: Basic Mode - Output Summary

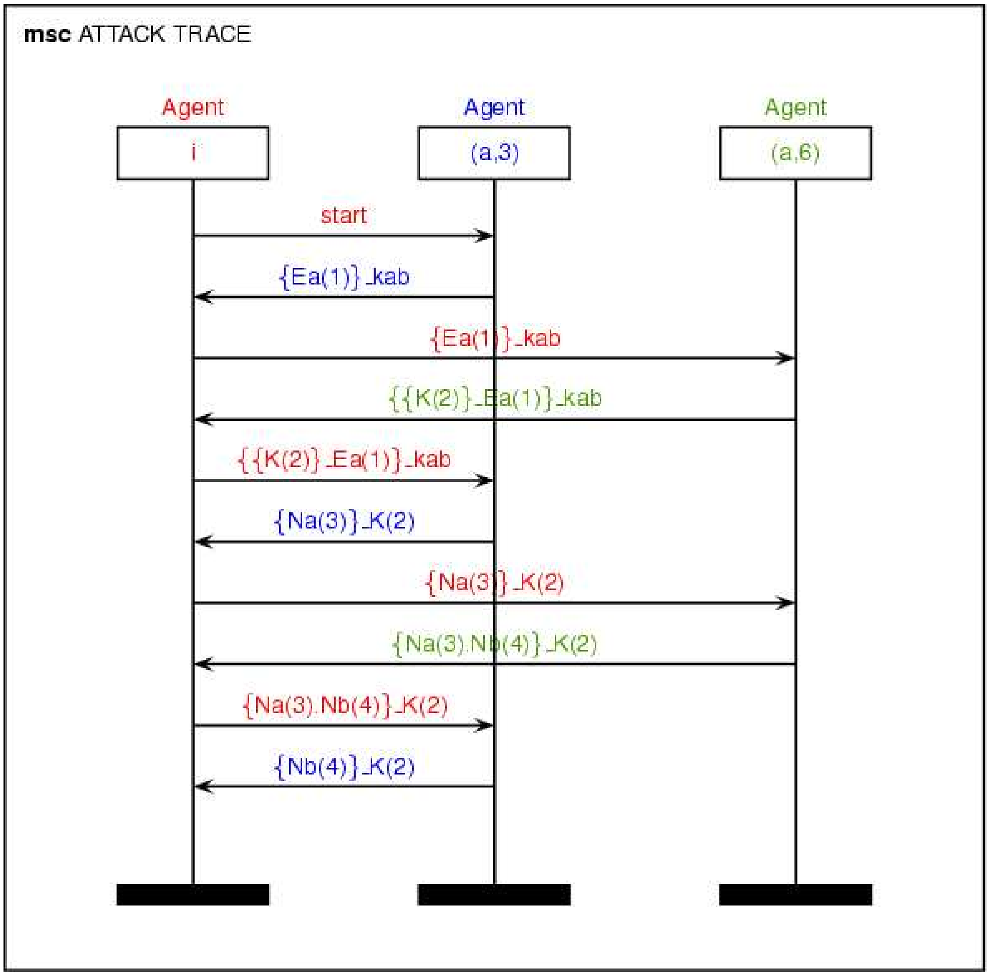


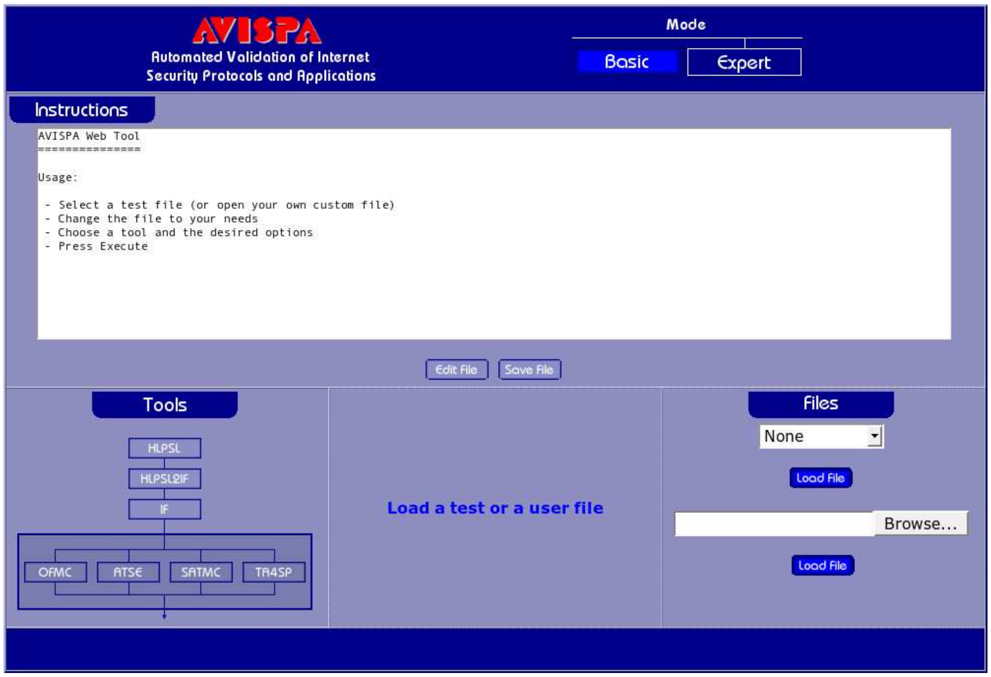
Figure 4: MSC Attack Trace

- a Postscript version of the MSC (for printing).

What can be visualised will vary according to the results of each tool. For instance, if one tool do not find an attack for the given protocol specification, the buttons to view the MSC and to download the Postscript are be greyed out. Figure 4 shows an example of an attack trace presented as a Message Sequence Chart. After executing one protocol analysis, the user can go back to the initial screen (the file selection screen) by using the File Selection button.

2.1.2 Expert Mode

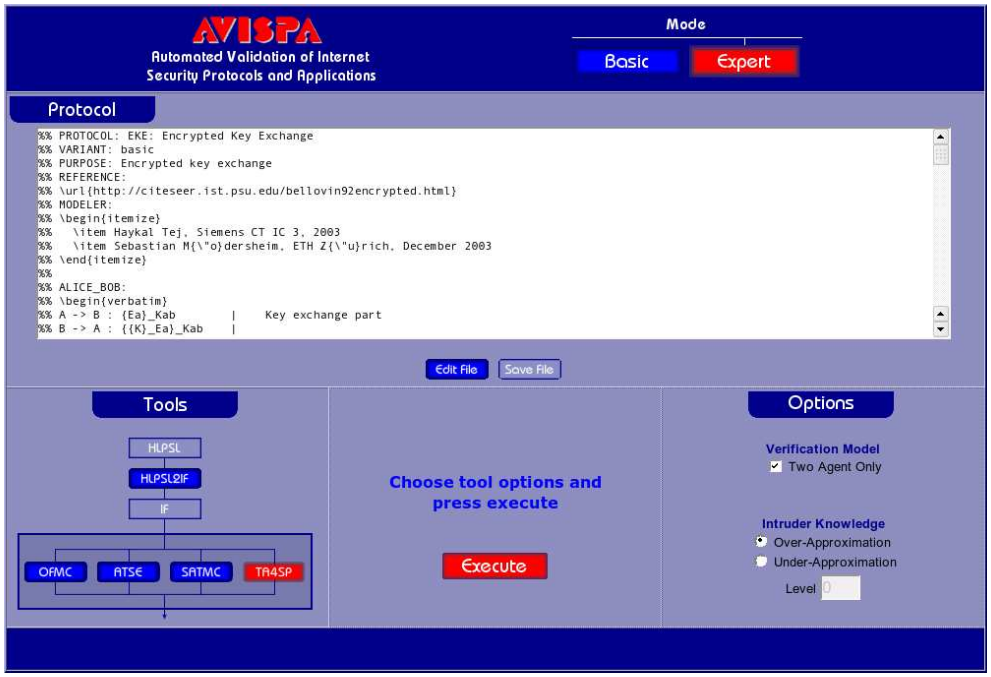
The expert mode offers a higher degree of customisation. Users can select several analysis modifiers before launching the tools. Although this mode does not permit to execute all the tools together, when the user selects a protocol specification, he can switch from one tool to another without the need of re-selecting the protocol file and without loosing his changes to the file. In that way, the user can quickly analyse the protocol in all tools by simply selecting another tool button after finishing the analysis in one tool. Figure 5 shows the initial screen of the expert mode. From the initial screen the user has no other choice than to load a protocol specification. After loading a protocol, the user can choose a particular tool in the left part of the control panel. In the expert mode, the left part of the control panel shows a graphical representation of the structure of the AVISPA Tool. The right side of the control panel shows both the test and user file load options and the middle part shows the help messages, as in the basic Mode. Once the user selects a tool, the tool options will appear in the right side of the control panel (see Figure 6). The user can then customise the options for the tool before firing the analysis with the Execute button. The Figure 7 shows the output screen for the expert mode. It is different from the basic



```
AVISPA Web Tool
===============

Usage:

 - Select a test file (or open your own custom file)
 - Change the file to your needs
 - Choose a tool and the desired options
 - Press Execute
```

Load a test or a user file

Figure 5: Expert Mode



```
%% PROTOCOL: EKE: Encrypted Key Exchange
%% VARIANT: basic
%% PURPOSE: Encrypted key exchange
%% REFERENCE:
%% \url{http://citeseer.ist.psu.edu/bellovin92encrypted.html}
%% MODELER:
%% \begin{itemize}
%%   \item Haykal Tej, Siemens CT IC 3, 2003
%%   \item Sebastian M{\"o}dersheim, ETH Z{\"u}rich, December 2003
%% \end{itemize}
%%
%% ALICE_BOB:
%% \begin{verbatim}
%% A -> B : {Ea}_Kab        |    Key exchange part
%% B -> A : {{K}_Ea}_Kab    |
```

Choose tool options and press execute

Verification Model
☑ Two Agent Only

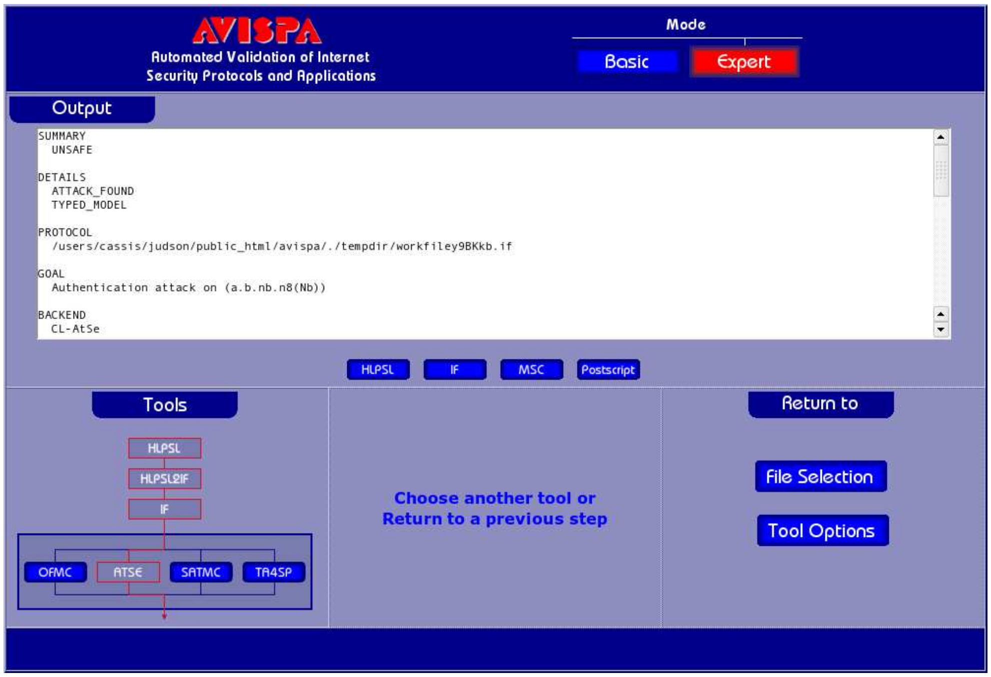
Intruder Knowledge
● Over-Approximation
○ Under-Approximation
Level 0

Figure 6: Expert Mode - Tool Options

mode in the following points:

- The tool output will be shown directly in the presentation panel
- The left-hand side of the control panel shows a graphical representation of the structure of the AVISPA Tool and shows the select tool.
- The right-hand side of the control panel shows an additional button that enables the user to go back to the latest options used for the selected tool.

All those features can be used on-line or off-line.



```
SUMMARY
  UNSAFE

DETAILS
  ATTACK_FOUND
  TYPED_MODEL

PROTOCOL
  /users/cassis/judson/public_html/avispa/./tempdir/workfiley9BKkb.if

GOAL
  Authentication attack on (a.b.nb.n8(Nb))

BACKEND
  CL-AtSe
```

Figure 7: Expert Mode - Output

References

[1] AVISPA. Deliverable 2.5: The output format. Available at `http://www.avispa-project.org`, 2004.

[2] Victor Bos and Sjouke Mauw. *A LaTeX macro package for Message Sequence Charts*. `http://www.win.tue.nl/~sjouke/mscpackage.html`, March 2004. Version 1.14.

[3] Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Mödersheim, and Laurent Vigneron. A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. In *Automated Software Engineering. Proceedings of the Workshop on Specification and Automated Processing of Security Requirements, SAPS'04*, pages 193–205, Austria, September 2004. Austrian Computer Society.

[4] `http://www.gnu.org/software/emacs/emacs.html`. The gnu emacs editor.

[5] `http://www.php.net/`. Php: Hypertext preprocessor.

[6] `http://www.w3.org/MarkUp/`. W3c html standard.