AVISPA

IST–2001–39252

Automated Validation of
Internet Security Protocols and Applications

Project Presentation

Deliverable 8.2

Abstract

This document is the Project Presentation of AVISPA. It summarises the project objectives, the description of work and the expected results. It also describes the duration, cost and partners of the project.

Deliverable details

Report version: **1.0 (final)**

Date of delivery: **March 27th, 2003** Due on: **March 31st, 2003**

Classification: **public** Total pages: **4 (2 pages paper+ 2 slides)**

Person-months required: **1**

Project details

Contract Start Date: **Jan 1st, 2003** Duration: **30 months**

Project Co-ordinator: **Alessandro ARMANDO**

Partners: **University of Genova, ETH Zürich, INRIA, Siemens AG**

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

Automated Validation of Internet Security Protocols and Applications

IST–2001–39252
Shared-cost FET Open Project

www.avispa-project.org

Project Presentation

Abstract

This project aims to develop a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. This technology will speed the development of the next generation of network protocols, improve their security, and therefore increase the public acceptance of advanced, distributed IT applications based on them. We will achieve this by advancing specification and deduction technology to the point where industry protocols can be specified and automatically analyzed. This technology will be integrated into a robust automated tool, tuned on practical, large-scale problems, and migrated to standardization bodies, whose protocol designers are in dire need of such tools.

Objectives

The project has five main objectives:

1. to develop a rich specification language for formalizing protocols, security goals, and threat models of industrial complexity;
2. to advance the state-of-the-art in automated deduction techniques to scale up to this complexity;
3. to build a tool based on these techniques that will allow industry and standardization organizations to automatically validate or detect errors in their products;
4. to tune this tool and demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols;
5. to begin the migration of this technology into standardization organizations such as the IETF so that both the scientific and the industrial community can benefit from the advances achieved by this project.

Description of work

The work will be carried out by accomplishing the following tasks:

- we will design a high-level language for specifying Internet security protocols, and implement a translator from protocol descriptions to a declarative format amenable to formal analysis;
- we will develop a technology for automated protocol error detection based on three automated deduction techniques operating on the translator's output. The techniques are on-the-fly model-checking, theorem-proving with constraints and model-checking methods based on propositional satisfiability checking; they will be integrated into a single analysis tool called AVISPA;
- to verify protocols we will develop techniques for infinite-state verification, like use of abstractions and infinite-state symbolic model-checking, and integrate them in our tool;
- a set of representative security problems drawn from IETF drafts will be selected and used to thoroughly evaluate the AVISPA tool according to well-defined and measurable criteria.

Milestones and expected results

The main milestones are the delivery and assessment of 3 versions of the AVISPA tool at months 12, 20 and 27, with a final milestone on the project's success at month 30.
We expect to specify at least 80 security problems out of the selected library, and solve at least 75% of these problems in less than 1 hour CPU time each.

Participants

1. Università di Genova, Italy *(project coordinator)*
2. INRIA Lorraine, France
3. ETH Zürich, Switzerland
4. Siemens AG, Germany

Cost

Total cost: € 2,047,586, of which € 808,000 provided by the EC.

Project start and duration

Project start: Jan 1st, 2003; duration: 30 months.

Coordinator

Dr. Alessandro ARMANDO
MRG-DIST, Università di Genova
viale F. Causa, 13 - 16145 Genova (Italy)
phone +39 – 010 – 353 2216
fax +39 – 010 – 353 2948
e-mail armando@dist.unige.it