www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D8.4: Year 1 Project Workshop

Abstract

We report on the Year 1 Project Workshop of the AVISPA Project. The workshop was held at INRIA-Lorraine (Nancy) on January 23, 2004, and was devoted to recent advances on the specification of security protocols and their properties, as well as on the techniques for their automatic analysis. The technical program of the workshop was enriched by the talks of two internationally reknown invited speakers. The results of the workshop have been significant in terms of dissemination, cross-fertilisation of ideas, spill-over effects, and establishment of new sinergies with other research teams.

Deliverable details

Deliverable version: *v1.0*	Person-months required: *0.3*
Date of delivery: *20.08.2004*	Due on: *31.01.2004*
Classification: *public*	Total pages: *4*

Project details

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

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

Contents

1 Introduction

One of the main objectives of AVISPA is the timely dissemination of the results of the project. This is achieved through a variety of means: the project website, the project workshops, the Project Presentation, the Technological Implementation Plan, and scientific publications. Project workshops are particularly important as they allow for a direct communication and cross-fertilisation of ideas among workshop participants.

The Year 1 Project Workshop of AVISPA was held at INRIA-Lorraine (Nancy) on January 23, 2004. The workshop was devoted to recent advances on the specification of security protocols and their properties, as well as on the techniques for their automatic analysis. The goal of the workshop was to bring together researchers working in the drafting, specification, and verification of Internet security-sensitive applications in order to compare different approaches and methodologies and foster cross-fertilisation of ideas.

The workshop was co-organised with the QSL, a research project sponsored by the French government and the Lorraine region that intends to foster research groups studying methods and techniques to improve the quality of (software-intensive) systems and to promote regional partnerships in research. Around a dozen of research teams from large laboratories in Lorraine (LORIA, LITA, CRAN) are involved in QSL. The QSL project maintains a web-site `qsl.loria.fr`, whose main goal is to give a wide access to resources (mainly verification software) related to system safety and security. This platform should ease the selection of tools for enforcing the quality of software by external users. Hence this QSL platform will give a good opportunity to advertise the methodology and tools developed within AVISPA.

2 Description of the event

The program of the workshop (see Table 1) consisted of a general introduction to the AVISPA Project, a number of talks devoted to the presentation of the achievements of the project, a panel discussion, and two invited talks given by two internationally renown researchers, namely

- Prof. Peter Ryan from the University of Newcastle (UK), and
- Dr. Yassine Lakhnech from VERIMAG (Grenoble, France).

In his talk, Prof. Ryan surveyed the open problems in the formal analysis of security protocols such as limitations of the standard Dolev-Yao intruder model, together with possible ways to overcome them (e.g. to exploit algebraic properties of cryptographic operators, typing, and guessing attacks). He also discussed the need of a unifying approach to defining security properties, and the need to consider more elaborate assumptions on the environment. Quite interestingly most of the issues raised during the talk are in the agenda of AVISPA and a lively discussion on the possible approaches to tackle these problems was conducted at the end of the talk.

Table 1: Program of the workshop

Morning		
09:00-09:10	M. Rusinowitch (LORIA)	*Welcome*
09:10-09:30	A. Armando (UNIGE)	*Overview of AVISPA*
09:30-10:30	P. Ryan (U. Newcastle)	*Security Protocols: Prospects and Challenges*
11:00-11:50	J. Cuellar (Siemens)	*Analysis of Industrial Protocols*
11:50-12:30	L. Vigneron (INRIA)	*Specification Languages for Internet Security Protocols*

Afternoon		
14:00-15:00	Y. Lakhnech (VERIMAG)	*Symbolic verification of cryptographic protocols with and without time stamps*
15:00-15:30	S. Mödersheim (ETHZ)	*The Lazy Intruder*
16:00-16:30	Y. Chevalier (INRIA)	*Constraint Solving for Protocol Analysis*
16:30-17:00	L. Compagna (UNIGE)	*SAT-based Model-Checking for Security Protocols Analysis*
17:00-17:15	L. Viganò (ETHZ)	*Summing up and Future Work*
17:15-18:00	Discussion	

Dr. Lakhnech presented a symbolic decision procedure for bounded cryptographic protocols that can deal with secrecy, authentication, and any property that can be described as a safety property. The procedure is based on a symbolic representation of sets of configurations in a decidable logic and can be extended to time-sensitive protocols. The relationships between Dr. Lakhnech's procedure and the techniques developed within AVISPA were thoroughly discussed at the end of the talk.

Participation in the workshop was open to the public. Furthermore, a number of researchers actively working in the area were explicitly invited to attend. The number of attendees was about 30 coming from a variety of research institutions: the University of Genova (Italy), ETHZ (Zürich, Switzerland), INRIA-Lorraine (Nancy, France), LIFC (Besançon, France), Siemens AG (München, Germany), University of Newcastle (UK), VERIMAG (Grenoble, France), University of Metz, University Nancy 2, University Henri Poincaré and Institut National Polytechnique de Lorraine (Nancy).

In order to advertise the event, a publicly available web site devoted to the workshop has been set up at the URL `http://qsl.loria.fr/Externe/Evennements/JourneeQSL/Journee23-01-2004`. The web page contains the scientific program of the workshop as well as the slides used by the speakers.

3 Results

The workshop proved very successful in a variety of ways:

Dissemination. The goals of the AVISPA projects, its technical achievements and their practical significance were thoroughly presented at the workshop.

Cross-fertilisation of ideas. The informal atmosphere of the workshop and the participation of researchers actively working on the topic stimulated an open discussion of ideas. For instance, the similarities between the symbolic decision procedure with timestamps developed by Dr. Lakhnech with that developed at UNIGE by Dr. Delzanno for the same class of protocols were thoroughly analysed. Similarly, the problems and the possible solutions concerning the modelling and use of algebraic properties and abstraction were openly discussed among the workshop participants, and this led to insights into the problem that will play a crucial role in the successful development of the corresponding techniques within AVISPA in the following months.

Spill-over effects. Yassine Lakhnech is a site leader for VERIMAG in the national RNTL project PROUVE on protocol verification. He was favourably impressed by the presentations and has planned to reuse some features of the HLPSL language developed in the context of AVISPA in the protocol description language developed in the context PROUVE (this is because several protocols can be expressed in HLPSL that are not expressible in the language initially developed for PROUVE).

New Synergies. The workshop has boosted the involvement of LIFC (Besançon, France) in the AVISPA project. This group, which is now associated to INRIA Lorraine, has been developing a protocol verification technology based on tree-automata, which, as will be described in forthcoming deliverables, is currently being connected as a new back-end of the AVISPA Tool.