AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D8.6: Year 3 Project Workshop

Abstract

We report on the Year 3 Project Workshop of the AVISPA Project. The workshop, titled "The Second Workshop on Automated Reasoning for Security Protocol Analysis" (ARSPA'05), will be held on July 16, 2005, in the context of The 32nd International Colloquium on Automata, Languages and Programming (ICALP'05), in Lisbon, Portugal. The workshop will bring together researchers and practitioners from both the security and the automated reasoning communities, from academia and industry, who are working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols. The workshop proceedings have been published as volume 135(1) of the Electronic Notes in Theoretical Computer Science. Moreover, the workshop organisers are planning a Special Issue of an international journal to collect original papers on automated reasoning techniques and tools for the analysis of security protocols.

Deliverable details

Deliverable version: *v1.0*	Person-months required: *0.4*
Date of delivery: *30.06.2005*	Due on: *30.04.2005*
Classification: *public*	Total pages: *15*

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)

[This page has been intentionally left blank.]

Contents

1 Introduction

The Year 3 Project Workshop, titled "The Second Workshop on Automated Reasoning for Security Protocol Analysis" (ARSPA'05), will be held on July 16, 2005, in the context of The 32nd International Colloquium on Automata, Languages and Programming (ICALP'05), in Lisbon, Portugal. The workshop will be devoted to recent advances on the specification of security protocols and their properties as well as on the techniques for their automatic analysis. The workshop will bring together researchers and practitioners from both the security and the automated reasoning communities, from academia and industry, who are 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.

Pierpaolo Degano (of the University of Pisa, Italy, who, as described in the deliverables [1, 2], is one of the principal investigators in the related projects Mefisto and Degas) and Luca Viganò (ETHZ) were appointed program chairs of the workshop well in advance in order to plan and undertake the necessary organisational measures.

Following the call published by the ICALP'05 Workshop Chair, a workshop proposal (see Annex A) was prepared by the Program chairs. Upon acceptance of the proposal, the organisation of the event started with the creation of the workshop web site (URL: `http://www.avispa-project.org/arspa`) and the preparation and publication of the call for papers (see Annex B).

The Program Chairs appointed a Program Committee that brought together a number of leading researchers in the field, namely: Alessandro Armando (UNIGE), David Basin (ETHZ), Jorge R. Cuellar (SIEMENS), Pierpaolo Degano, Roberto Gorrieri (University of Bologna, Italy), Joshua D. Guttman (The MITRE Corporation, USA), Sjouke Mauw (University of Eindhoven, The Netherlands), Hanne Riis Nielson (Technical University of Denmark), Michael Rusinowitch (INRIA), and Luca Viganò.

By the deadline, 20 papers were submitted from 13 countries in Africa, Asia, Australia, Europe, and North America. All the submissions were evaluated by at least three referees (the Program Committee members enjoyed the collaboration of 18 additional referees) and the Program Committee then selected 7 research contributions for presentation at the workshop.

2 Description of the event

The program of the workshop (see Table 1) will consist of the presentation of the 7 accepted contributions, and by two invited talks given by two internationally reknown researchers, namely

- Dr. Michael Backes from the IBM Zurich Research Laboratory, Switzerland.

- Prof. John C. Mitchell from the Stanford University, U.S.A.

Participation in the workshop will be open to the public, and ARSPA'05 is expected to be one of the most successful of the ICALP'05 workshops, with approximately 40 participants.

Table 1: Program of the workshop

Morning		
9:00-9:15	P. Degano and L. Viganò	*Opening*
9:15-10:05	J. C. Mitchell	*Protocol Analysis: Wireless Networking and Mobility* (Invited Talk)
10:05-10:45	C. Cremers, S. Mauw, E. de Vink	*A Syntactic Criterion for Injectivity of Authentication Protocols*
10:45-11:15	A. Gotsman, F. Massacci, M. Pistore	*Towards an Independent Semantics and Verification Technology for the HLPSL Specification Language*
11:55-12:35	K. Imamoto and K. Sakurai	*Design and Analysis of Diffie-Hellman-Based Key Exchange Using One-time ID by SVO Logic*

Afternoon		
14:15-15:05	M. Backes	*Justifying Formal Methods and Cryptography under Active Attacks, and Limitations Thereof* (Invited Talk)
15:05-15:45	C. Caleiro, L. Viganò, D. Basin	*Deconstructing Alice and Bob*
16:15-16:55	C. Rosenkilde Nielsen, E. Heltoft Andersen, H. Riis Nielson	*Static Validation of a Voting Protocol*
16:55-17:35	M. Nesi and G. Rucci	*Formalizing and Analyzing the Needham-Schroeder Symmetric-Key Protocol by Rewriting*
17:35-18:15	D. D'Souza, K.R. Raghavendra, B. Sprick	*An Automata Based Approach for Verifying Information Flow Properties*
18:15-18:45	P. Degano and L. Viganò	*Final discussion*

References

[1] AVISPA. Deliverable 1.3: Periodic Progress Report N°: 3. Available at `http://www.avispa-project.org`, 2005.

[2] AVISPA. Deliverable 1.4: Final Project Report. Available at `http://www.avispa-project.org`, 2005.

A Workshop Proposal

Dear ICALP’05 organizers,

Pierpaolo Degano (University of Pisa, Italy) and I (ETH Zurich, Switzerland) are organizing

ARSPA’05

The Second Workshop on
Automated Reasoning for
Security Protocol Analysis

a one-day workshop (preferably to be held on July 16) that we would like to co-locate with the ICALP’05 conference; see the attached preliminary version of its possible call for papers.

Given this year’s special track on "Security and Cryptography Foundations (C)", we believe that ICALP will provide an excellent environment for our workshop, attracting a large number of participants.

The first edition of the ARSPA workshop was co-located with the Second International Joint Conference on Automated Reasoning, IJCAR 2004, in July 2004.

The workshop was a great success, with a large numbers of attendees (around 40). There were 18 submissions and the program committee selected 9 papers of high quality, which were presented at the workshop together with an invited talk and 3 short presentations of work in progress.

Motivated by this, the members of the program committee of ARSPA’04 are guest-editing a Special Issue of the Journal of Automated Reasoning collecting original papers on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols.

Looking forward to hearing from you soon, we remain

Yours

Pierpaolo Degano and Luca Vigano‘

Prof. Pierpaolo Degano
Dipartimento di Informatica

```
Universita‘ di Pisa
Corso Italia 40
I-56125 Pisa, Italy
Tel.: +39 050 2212 757
Fax: +39 050 2212 726
E_mail: degano -at- di.unipi.it
http://www.di.unipi.it/~degano/degano.html

PD Dr. Luca Vigano‘
Information Security                e-mail: vigano - at- inf.ethz.ch
ETH Zurich                          http://www.inf.ethz.ch/~vigano
ETH Zentrum, IFW C 43.1             Phone:   +41 (0)1 632 72 72
Haldeneggsteig 4                    Fax:     +41 (0)1 632 11 72
CH-8092 Zurich, Switzerland



        ======================================================


                               ARSPA’05

                         The Second Workshop on
                        Automated Reasoning for
                      Security Protocol Analysis

                        co-located with ICALP’05

                            Lisboa, Portugal
                    _ July 2005 (preferably the 16)


                  http://www.avispa-project.org/arspa


                        ***********************
                        *** CALL FOR PAPERS ***
                        ***********************


                  Submission deadline: April 15, 2005
```

BACKGROUND, AIM AND SCOPE
=========================

Experience over the last twenty years has shown that, even assuming perfect cryptography, the design of security protocols (or cryptographic protocols, as they are sometimes called) is highly error-prone and that conventional validation techniques based on informal arguments and/or testing are not up to the task. It is now widely recognized that only formal analysis can provide the level of assurance required by both the developers and the users of the protocols.

Work in this direction initially started in the security community but recently there has been a tremendous progress thanks to contributions from different automated reasoning communities, such as model checking, resolution, planning, rewriting/narrowing, and higher-order theorem proving. There has been another wave of progress due to research in applying non-classical logics, such as epistemic and belief logics, to analyze protocols and their properties. Moreover, a third stream includes static methods, among which those based on abstract interpretation, data and control flow analysis, and type systems proved to be particularly successful. Finally, bisimulations and related techniques have also been applied successfully.

Based on this progress, a large number of formal methods and tools have been developed that have been quite successful in determining strengths and weaknesses of many protocols, i.e. in proving the correctness of the protocols or in identifying attacks on them.

The ARSPA workshop aims to bring together researchers and practitioners from both the security and the formal methods communities, from academia and industry, who are working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols.

Contributions are welcomed on the following topics or related ones:

- Automated analysis and verification of security protocols.
- Languages, logics and calculi for the design and specification of security protocols.
- Verification methods: accuracy, efficiency.
- Decidability and complexity of cryptographic verification problems.
- Synthesis and composition of security protocols.
- Integration of formal security specification, refinement and

validation techniques in development methods and tools.

The workshop will provide a forum for all researchers and practitioners who are interested in this area to share their ideas and report their results. We thus solicit submissions of papers both on mature work and on work in progress.

All submissions will be peer-reviewed. Authors of accepted papers must guarantee that their paper will be presented at the workshop.

DATE
====

The workshop will be a one-day workshop, preferably to be held on July 16 (post-conference).

AUDIENCE
========

The workshop will be open to all interested persons.

INVITED TALKS
=============

The technical program will include presentations of the accepted papers, and one or two invited talks.

PROGRAM COMMITTEE
=================

Preliminary list:

- Alessandro Armando
- David Basin
- Jorge Cuellar
- Pierpaolo Degano (co-chair)
- Roberto Gorrieri
- Michael Rusinowitch
- Luca Vigano‘ (co-chair)

SUBMISSION
==========

Submissions should be at most 15 pages (a4paper, 11pt) and the cover page should include title, names of authors, and the co-ordinates of the corresponding author.

Authors are invited to submit their papers electronically, as portable document format (pdf) or postscript (ps), by sending them to

arspa - at - avispa-project.org

Submissions must be received by the deadline of April 15, 2005.
Notification of acceptance or rejection will be sent to the authors no later than May 14, 2005.
Final versions of accepted papers must be received by June 10, 2005.

PUBLICATION
===========

Accepted contributions will be included in the informal workshop proceedings, which will be available at the workshop. They will also be published on-line on the workshop's web page at

http://www.avispa-project.org/arspa

prior to the workshop.
We are also planning a formal post-workshop publication as a special Journal issue, with an additional reviewing process.

IMPORTANT DATES
===============

- Submission deadline:	April 15, 2005
- Notification of acceptance:	May 15, 2005
- Final versions due:	June 10, 2005
- Workshop:	July 16, 2005

WORKSHOP WEB-SITE
=================

http://www.avispa-project.org/arspa

The workshop is supported by the IST Project AVISPA
(http://www.avispa-project.org)

For further information on the workshop, please send an email to
arspa -at- avispa-project.org

B Call for Papers of the Workshop

ARSPA'05

The Second Workshop on
Automated Reasoning for
Security Protocol Analysis

co-located with ICALP'05
Lisboa, Portugal
July 16, 2005

http://www.avispa-project.org/arspa

****
*** CALL FOR PAPERS ***
****

Submission deadline: April 24, 2005

BACKGROUND, AIM AND SCOPE

Experience over the last twenty years has shown that, even assuming perfect cryptography, the design of security protocols (or cryptographic protocols, as they are sometimes called) is highly error-prone and that conventional validation techniques based on informal arguments and/or testing are not up to the task. It is now widely recognized that only formal analysis can provide the level of assurance required by both the developers and the users of the protocols.

Work in this direction initially started in the security community but recently there has been a tremendous progress thanks to contributions from different automated reasoning communities, such as model checking, resolution, planning, rewriting/narrowing, and higher-order theorem proving. There has been another wave of progress due to research in applying non-classical logics, such as epistemic and belief logics, to analyze protocols and their properties. Moreover, a third stream includes static methods, among which those based on abstract interpretation, data and control flow analysis, and type systems proved to be particularly successful. Finally, bisimulations and related techniques have also been applied successfully.

Based on this progress, a large number of formal methods and tools have been developed that have been quite successful in determining strengths and weaknesses of many protocols, i.e. in proving the correctness of the protocols or in identifying attacks on them.

The ARSPA workshop aims to bring together researchers and practitioners from both the security and the formal methods communities, from academia and industry, who are working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols.

Contributions are welcomed on the following topics or related ones:

- Automated analysis and verification of security protocols.
- Languages, logics and calculi for the design and specification of security protocols.
- Verification methods: accuracy, efficiency.
- Decidability and complexity of cryptographic verification problems.
- Synthesis and composition of security protocols.
- Integration of formal security specification, refinement and validation techniques in development methods and tools.

The workshop will provide a forum for all researchers and practitioners who are interested in this area to share their ideas and report their results. We thus solicit submissions of papers both on mature work and on work in progress.

All submissions will be peer-reviewed. Authors of accepted papers must guarantee that their paper will be presented at the workshop.

AUDIENCE
========

The workshop will be held on Saturday, July 16, 2005, and will be open to all interested persons.

INVITED TALKS
=============

The technical program will include presentations of the accepted papers, and one or two invited talks.

PROGRAM COMMITTEE
=================

- Alessandro Armando (Universita‘ di Genova, Italy)
- David Basin (ETH Zurich, Switzerland)
- Jorge Cuellar (SIEMENS AG, Munich, Germany)
- Pierpaolo Degano (Universita‘ di Pisa, Italy; co-chair)
- Joshua Guttman (The MITRE Corporation, USA)
- Roberto Gorrieri (Universita‘ di Bologna, Italy)
- Sjouke Mauw (University of Eindhoven, The Netherlands)
- Hanne Riis Nielson (Technical University of Denmark)
- Michael Rusinowitch (INRIA-LORRAINE, Nancy, France)
- Luca Vigano‘ (ETH Zurich, Switzerland; co-chair)

SUBMISSION
==========

Submissions should be at most 15 pages (a4paper, 11pt) and the cover page should include title, names of authors, and the co-ordinates of the corresponding author.

Authors are invited to submit their papers electronically, as portable document format (pdf) or postscript (ps), by the deadline of April 24, 2005.

The only mechanism for paper submissions is via the electronic submission web-site, accessible via the workshop web-site.

Notification of acceptance or rejection will be sent to the authors no later than May 18, 2005.

Final versions of accepted papers must be received by June 06, 2005.

PUBLICATION
===========

Accepted contributions will be published in a special volume of the Electonic Notes in Theoretical Computer Science ENTCS.

```
Informal proceedings will be available at the workshop and be
published on-line on the workshop's web page at
                  http://www.avispa-project.org/arspa
We are also planning a formal post-workshop publication as a special
Journal issue, with an additional reviewing process.



IMPORTANT DATES
===============

- Submission deadline:        April 24, 2005
- Notification of acceptance: May   18, 2005
- Final versions due:         June  06, 2005
- Workshop:                   July  16, 2005



WORKSHOP WEB-SITE
=================

http://www.avispa-project.org/arspa

The workshop is supported by the IST Project AVISPA
(http://www.avispa-project.org)


For further information on the workshop, please send an email to
                     arspa -at- avispa-project.org
```