AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D8.5: Year 2 Project Workshop

Abstract

We report on the Year 2 Project Workshop of the AVISPA Project. The workshop, titled “Automated Reasoning for Security Protocol Analysis” (ARSPA), was held at the University College, Cork (Ireland), on July 4, 2004 in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR’04). The workshop brought 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 results of the workshop have been significant in terms of dissemination and cross-fertilisation of ideas. The workshop proceedings will be published as a special issue of the Electronic Notes in Theoretical Computer Science. Moreover, the members of the program committee of ARSPA will guest-edit a Special Issue of the Journal of Automated Reasoning collecting original papers on automated reasoning techniques and tools for the formal specification and analysis of security protocols.

Deliverable details

Deliverable version: *v1.0*	Person-months required: *0.3*
Date of delivery: *20.08.2004*	Due on: *31.07.2004*
Classification: *public*	Total pages: *17*

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)

Contents

1 Introduction 2

2 Description of the event 2

3 Dissemination 4

A Workshop Proposal 5

B Call for Papers of the Workshop 11

C Call for Papers of the Special Issue of the Journal of Automated Reasoning 15

1 Introduction

The Year 2 Project Workshop, titled "Automated Reasoning for Security Protocol Analysis" (ARSPA), was held at the University College, Cork (Ireland), on July 4, 2004 in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR'04). The workshop was devoted to recent advances on the specification of security protocols and their properties and 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 Organising Committee, consisting of Alessandro Armando (UNIGE), David Basin (ETHZ), Jorge Cuellar (SIEMENS), Michaël Rusinowitch (INRIA), and Luca Viganò (ETHZ) was set well in advance in order to plan and undertake the necessary organisational measures. Alessandro Armando and Luca Viganò were appointed program chairs of the workshop.

Following the call published by the IJCAR Workshop Chair, a workshop proposal (see Annex A) was prepared by the Organising Committee. Upon acceptance of the proposal (as IJCAR workshop W6, see `http://www.mpi-sb.mpg.de/~baumgart/ijcar-workshops/`), 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).

By the deadline, 18 papers were submitted from a wide variety of countries: France, Ireland, Italy, Malaysia, Mexico, The Netherlands, Portugal, Switzerland, UK, and USA. The reviewing process was carried out by the Organising Committee with the collaboration of 16 additional referees. Each paper was reviewed by at least 2 independent referees. As a result of the reviewing process, 9 regular papers were accepted for presentation at the workshop. Two additional papers presenting interesting, even though not completely mature work were accepted for short presentations at the workshop.

2 Description of the event

The program of the workshop (see Table 1) consisted of the presentation of the 9 regular papers, the presentation of the two short papers, and by an invited talk given by an internationally renown researcher, namely

- Prof. Simon Foley from the University College, Cork, Ireland.

Prof. Foley's talk about the problems associated with the modelling and formalisation of the notion of the integrity raised several interesting issues, which the audience discussed in detail

Participation in the workshop was open to the public, and ARSPA was one of the most successful of the IJCAR'04 workshops, with approximately 50 participants.[1]

Table 1: Program of the workshop

Morning

9:00-9:10	A. Armando, L. Viganò	*Opening*
9:10-10:00	S. Foley	*Believing the Integrity of a System* (Invited Talk)
10:00-10:30	M. Bond, J. Clulow	*Extending Security Protocol Analysis: New Challenges*
11:00-11:30	H. Chen, J.A. Clark, J.L. Jacob	*Synthesizing Efficient and Effective Security Protocols*
11:30-12:00	C. Lynch, C. Meadows	*On the Relative Soundness of the Free Algebra Model for Public Key Encryption*
12:00-12:30	Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani	*Deciding the Security of Protocols with Commuting Public Key Encryption*

Afternoon

14:00-14:40	C. Caleiro, L. Viganò, D. Basin	*Metareasoning about Security Protocols using Distributed Temporal Logic*
14:30-15:00	A. Armando, L. Compagna	*An Optimized Intruder Model for SAT-based Model-Checking of Security Protocols*
15:00-15:30	L. Mazaré	*Satisfiability of Dolev-Yao Constraints*
16:00-16:30	G. Steel, A. Bundy	*Attacking a Group Multicast Protocol using CORAL*
16:30-17:00	P. Hankes Drielsma, S. Mödersheim	*The ASW Protocol Revisited: A Unified View*
17:00-17:15	E. Kleiner, B. Roscoe	*Web Services Security: a preliminary study using Casper and FDR* (short paper)
17:15-17:30	F. Sadri, F. Toni	*A logic-based approach to reasoning with beliefs about trust* (short paper)

[1] Note also that related talks on protocol analysis were given also as part of the main technical program of the IJCAR conference (2 talks), as well as in two other associated workshops (3 talks at the "UNIF" workshop and 1 at the "Disproving" workshop), which further shows that protocol analysis is currently one of the most important and research topics in computer science; see `http://www.4c.ucc.ie/ijcar/` for more details on these talks.

3 Dissemination

The workshop proved to be a stimulating forum for the exchange of ideas on state-of-the-art techniques for the modelling, formalisation, and automatic analysis of security protocols. Special measures were planned and undertaken by the Organising Committee in order to ensure a timely and widespread dissemination of the works presented at the workshop.

Workshop Proceedings. In order to provide a timely dissemination of ideas, workshop proceedings were made available in electronic format on the workshop web-site before the workshop took place. Furthermore, hard copies of the workshop proceedings have been distributed to the participants. Finally, in order to ensure a wide dissemination of the results, workshop proceedings have been collected and will soon be published by Elsevier as a special issue of the Electronic Notes in Theoretical Computer Science (ENTCS, URL: `http://www.sciencedirect.com/science/journal/15710661`).

Special Issue of the Journal of Automated Reasoning. Following contacts with the Editor in Chief of the Journal of Automated Reasoning, the Organising Committee of ARSPA is working at the organisation of a special issue of the Journal of Automated Reasoning devoted "Automated Reasoning for Security Protocol Analysis". Authors of the papers presented at the ARSPA workshop will be invited to submit extended version of their papers, but submission will be open to other researchers as well. In any case submitted papers will be subject to the standard journal refereeing process. Papers submitted to the special issue must be original and not submitted for publication elsewhere. The call for papers of the Special Issue will be published in August 2004 (see Annex C).

A Workshop Proposal

Workshop Proposal

Workshop on
Automated Reasoning for
Security Protocols Analysis (ARSPA)

July 04, 2004, Cork, Ireland

co-located with the Second International Joint Conference on Automated Reasoning, IJCAR 2004

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. Moreover, 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.

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. Thus, this progress can be seen as one of the recent success stories of the automated reasoning community.

The workshop aims to 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.

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 be held on Sunday, July 04, 2004, and will be open to all interested persons.

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

Besides for presentations of accepted papers, we will schedule a couple of invited talks and a panel discussion "Bridging the analysis gap: from the Clark/Jacob library to Internet protocols".

ORGANIZATION/PROGRAM COMMITTEE
==============================

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

Alessandro Armando
Universita‘ di Genova, Italy
Email: armando@dist.unige.it
URL: http://www.mrg.dist.unige.it/~armando

Alessandro Armando has been assistant professor at the University of Genova since 1995. He received his master degree in Electronic Engineering in 1988 and his Ph.D. in 1994 from the University of

Genova. In February 2001 he got the qualification of associate professor in Computer Engineering. His appointments include a research position at the University of Edinburgh (1994-1995) and one at INRIA-Lorraine, Nancy (1998-1999). His research focuses on the integration of automated reasoning techniques and their application to verification problems including the automatic analysis of security protocols. He is coordinator an EU-funded project titled "Automated Validation of Internet Security-sensitive Protocols and Applications" (AVISPA) and is scientific representative for the University of Genova of the Research Training Network CALCULEMUS. He is member of the Steering Committees of the ‘‘First Order Theorem Proving’’ and of the ‘‘Frontiers of Combining Systems’’ Workshop Series as well as of the International Joint Conference on Automated Reasoning (IJCAR). He has been program committee member of a number of international workshops and conferences and program chair of the 4th International Workshop on Frontiers of Combining Systems (FroCoS 2002).

David Basin
ETH Zurich, Switzerland
Email: basin@inf.ethz.ch
URL: http://www.infsec.ethz.ch/~basin

David Basin has been a professor of Computer Science at ETH Zurich since January 2003. He received his bachelor’s degree in mathematics from Reed College in 1984, his Ph.D. in Computer Science from Cornell University in 1989, and his Habilitation in computer science from the University of Saarbruecken in 1996. His appointments include a postdoctoral research position at the University of Edinburgh (1990-1991), and afterwards he led a subgroup, within the programming logics research group, at the Max-Planck-Institut fuer Informatik (1992-1997). From 1997 to 2002 he was a full professor of Software Engineering at the University of Freiburg in Germany. His research area is Information Security, in particular methods and tools for building secure and reliable systems. He currently leads the Zurich Information Security Center (ZISC). He also serves on the editorial boards of Acta Informatica, Information Processing Letters, and Higher-Order and Symbolic Computation. Among others, he has chaired the Workshop on Formal Methods in Security Engineering (FMSE, co-located with CCS’03) and co-chairs IJCAR’04.

Jorge Cuellar
Siemens AG, Munich, Germany
Email: Jorge.Cuellar@siemens.com

Jorge R. Cuellar studied mathematics (BA. and MA.) at the Universidad de los Andes, Bogota, and obtained a Ph.D. from the University of Mainz. He was faculty member of the Ohio State University and Universidad de los Andes. Since 1987 he has been with Siemens, where he is Principal Research Scientist and has held visiting teaching positions at Technical University of Chemnitz, Technical University of Munich, University of Dortmund, University of Freiburg, and the University of Canterbury (Christchurch, New Zealand). He has worked in operating systems, formal methods, neural networks, performance, network and mobile security and Internet protocols. He has been in the editorial board of Science of Computer Programming (Elsevier). He has given a number of invited talks and held two tutorials on security protocols (‘‘Internet Security Protocols: Specification and Modeling", at SEFM03, and ‘‘IETF-Standardisierung von Sicherheit", at VIS 2001).

Michael Rusinowitch
INRIA, Nancy, France
Email: Michael.Rusinowitch@loria.fr
URL: http://www.loria.fr/˜rusi

Michael Rusinowitch received a These d'Etat in Computer Science in 1987 at the University Henri Poincare in Nancy. Since 1994 he is Directeur de Recherche at INRIA. His research is mainly concerned with theorem-proving, term-rewriting, and their application to software verification. He contributed to the development of automated deduction with constraints, to new proof methods based on induction and rewriting and to the verification of security protocols. Dr. Rusinowitch has been responsible in 1998/99 for an INRIA Cooperative Research Action on the Validation of Infinite State Systems. He is currently leader of the Cassis group at INRIA Lorraine. He has published his works in 30 international conferences and 20 journal papers, and is the author of a book on automated deduction. He has been a member of program committees for several international conferences and co-chairman of the conference on Rewriting Techniques and Applications, was invited speaker at LPAR'00 and RTA'01. Among others, he has chaired the Workshop on Security Protocols Verification (SPV, co-located with CONCUR'03) and co-chairs IJCAR'04.

Luca Vigano‘
ETH Zurich, Switzerland
Email: vigano@inf.ethz.ch
URL: http://www.infsec.ethz.ch/˜vigano

Luca Vigano‘ received his Masters in Electronic Engineering from the University of Genova in 1994, his Ph.D. in Computer Science from the University of Saarbruecken in 1997, and his Habilitation in Computer Science from the University of Freiburg in 2003. His appointments include a research position at the Max-Planck-Institut fuer Informatik in Saarbruecken (1994-1997), an assistant professor position at the Institute for Software Engineering at the University of Freiburg (1997-2002), and a senior research scientist position at ETH Zurich (since 2003). His research focuses on methods for the specification, verification, and construction of secure systems. His work includes foundational work on the theory and applications of non-classical and security logics, of proof development systems, and of logical frameworks. On these topics he has co-organized several classes and seminars, and has published a book and more than 20 papers in international journals and conferences. He is member of the steering committee of the ‘‘First Order Theorem Proving’’ workshop series.

SUBMISSION
==========

Submissions should be at most 10 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). A detailed description of the electronic submission procedure will be given at ARSPA web-page.

Submissions must be received by the deadline of April 15, 2004. Notification of acceptance or rejection will be sent to the authors no later than May 10, 2004. Final versions of accepted papers must be received by June 01, 2004.

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

Accepted contributions will be included in the informal workshop proceedings, which will be available at the workshop. As written in the "Call for Workshop Proposals", a volume of ENTCS devoted to proceedings of selected workshops is also anticipated.

Moreover, workshop participants will be invited to submit full versions of their papers to a special issue of the Journal of Automated Reasoning.

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

Submission deadline: April 15, 2004
Notification of acceptance: May 10, 2004
Deadline for camera-ready copy of workshop notes: June 01, 2004
Workshop Date: July 04, 2004

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

http://www.infsec.ethz.ch/~vigano/arspa

RELATED LINKS
=============

Supported by the IST Project AVISPA (http://www.avispa-project.org)

B Call for Papers of the Workshop

IJCAR 2004 Workshop W6

ARSPA

Automated Reasoning for
Security Protocol Analysis

University College Cork
Cork, Ireland
Sunday, July 04, 2004

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

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

Submission deadline: April 15, 2004

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. Moreover, 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.

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. Thus, this progress can be seen as one of the recent success stories of the automated reasoning community.

The workshop aims to 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.

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.

AUDIENCE
========

The workshop will be held on Sunday, July 04, 2004, and will be open to all interested persons.

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

The technical program will include
- presentations of the accepted papers,
- one or two invited talks,
- a panel discussion "Bridging the analysis gap: from the Clark/Jacob library to Internet protocols".

ORGANIZATION AND PROGRAM COMMITTEE
==================================

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

SUBMISSION
==========

Submissions should be at most 10 pages (a4paper, 11pt) and the cover page should include title, names of authors, and the co-ordinates of the corresponding author.

Please use LaTeX, with the following header:

```
    \documentclass[a4paper,11pt]{article}
    \textwidth  14.63cm
    \textheight 22cm
    \oddsidemargin  0.65cm
    \evensidemargin 0.65cm
    \topmargin  0.55cm
    \headheight 0.0pt
    \headsep    0.0pt
```

Authors are invited to submit their papers electronically, as portable document format (pdf) or postscript (ps), by sending them to arspa@avispa-project.org

Submissions must be received by the deadline of April 15, 2004. Notification of acceptance or rejection will be sent to the authors no later than May 10, 2004. Final versions of accepted papers must be received by June 01, 2004.

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

```
Accepted contributions will be included in the informal workshop
proceedings, which will be available at the workshop. As written in the
"Call for Workshop Proposals", a volume of ENTCS devoted to proceedings
of selected workshops is also anticipated.

Moreover, workshop participants will be invited to submit full
versions of their papers to a special issue of the Journal of
Automated Reasoning, which will be open also to non-participants, in
all cases with fresh reviewing.



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

- Submission deadline:        April 15, 2004
- Notification of acceptance: May 10, 2004
- Final versions due:         June 01, 2004
- Workshop:                   July 04, 2004



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

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


For further information on the workshop, please send an email to
arspa@avispa-project.org
From lvigano Thu Feb  5 15:52:55 2004
To: armando@dist.unige.it
Subject: CFP: Automated Reasoning for Security Protocols Analysis (ARSPA)
```

C Call for Papers of the Special Issue of the Journal of Automated Reasoning

```
                          Special Issue
                               of
                The Journal of Automated Reasoning
                               on
                     Automated Reasoning for
                    Security Protocol Analysis


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


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



BACKGROUND 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
automated deduction, model checking, and artificial intelligence.
Moreover, 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.
  Based on this progress, a large number of formal methods and tools
have been developed that have been quite successful in analyzing many
protocols, i.e. in proving the correctness of the protocols or in
identifying attacks on them. Thus, this progress can be seen as one of
the recent success stories of the automated reasoning community.

In July 2004, the first
```

Workshop on Automated Reasoning for
Security Protocol Analysis (ARSPA)

took place as part of IJCAR 2004. Motivated by the success of the workshop, the members of the program committee of ARSPA will guest-edit 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.

Contributions are welcomed on the following topics and 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.

EDITORS
=======

Alessandro Armando	(Universita‘ di Genova, Italy)
David Basin	(ETH Zurich, Switzerland)
Jorge Cuellar	(Siemens AG, Munich, Germany)
Michael Rusinowitch	(LORIA-INRIA-Lorraine, France)
Luca Vigano‘	(ETH Zurich, Switzerland)

SUBMISSION
==========

Authors should submit their papers electronically, in portable document format (pdf) or postscript (ps), by sending an email with subject "JAR submission" to the address

arspa@avispa-project.org

with the file of the paper as an attachment, and the following information in the body of the email, in plain text:

- paper title
- author names
- coordinates of the corresponding author
- abstract of the paper

The cover page of the submission should also include this information.

Authors are strongly encouraged to use Kluwer's LaTeX stylefiles for journal submissions available at

http://www.wkap.nl/authors/jrnlstylefiles/

Submitted papers must be original and not submitted for publication elsewhere. The submitted papers will be subject to the standard journal refereeing process.

DEADLINE FOR SUBMISSION
=======================

NOVEMBER 26, 2004

WEB-SITE
========

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