Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures

FP7-ICT-2007-1, Project No. 216471

www.avantssar.eu

Deliverable D1.6
Final Dissemination and Use Plan

Abstract

This document describes the final plan for the actions and activities that have been and will be taken to disseminate and use the knowledge and results obtained in the AVANTSSAR project.

Deliverable details

Deliverable version: *v1.0*
Classification: *public*
Date of delivery: *11.02.2011*
Due on: *31.12.2010*
Editors: *all*
Total pages: *73*

Project details

Start date: *January 01, 2008*
Duration: *36 months*
Project Coordinator: *Luca Viganò*
Partners: UNIVR, ETH Zurich, INRIA, UPS-IRIT, UGDIST, IBM, OpenTrust, IEAT, SAP, SIEMENS

Contents

List of Figures

1 Introduction

AVANTSSAR is a 3-year R&D STREP project, started on 01.01.08, funded by the European Commission under the FP7-ICT Theme Work Programme 2007-2008, Challenge 1, Objective 1.4: "Secure, dependable and trusted Infrastructures". This document is the Final Dissemination and Use Plan for AVANTSSAR, which updates and extends the "Basic Dissemination and Use Plan" [D1.2] and is a companion of the "Technology Implementation Plan" [D1.7]. It is structured as follows:

- In section 2, we describe our approach to dissemination and use, along with some market projections.
- In section 3, we describe our dissemination plan, including the project web-site; the conferences, events, and publications by means of which we have been disseminating our results, and the clustering and standardization relevant to AVANTSSAR.
- In section 4, we describe the use plans for each of the main project results.

2 Approach to Dissemination and Use

The AVANTSSAR project has been representing an unprecedented effort to apply automated validation methods to trust and security aspects of service-oriented architectures comprising of composed services, and it has thus generated a large interest in both academia and industry.

We have thus planned from the start of the project appropriate measures to ensure an effective and timely dissemination of the project results to potential users, both at the European level and worldwide, and to stimulate the exploitation of the AVANTSSAR results by industry and standardization bodies.

The main targets of the dissemination activity are industry, research institutions, and standardization bodies working on the design of Web Services and service-oriented architectures, focussing in particular on their trust and security aspects. Moreover, since the European Society as a whole will ultimately benefit from the results of the project (in terms of increased reliability and acceptance of, and confidence in, service-oriented architectures, in particular in e-health, e-government, e-market, etc.), special measures have been planned to reach the public.

Dissemination to industry, research institutions and standardization bodies, as well as to European citizen, has been, and will further be, carried out by a variety of means:

- Talks at relevant international conferences, events and forums (both presenting the technical achievements and introducing at a high level the project's objectives and results).
- Publication of papers in proceedings of international conferences and events, as well as in international scientific journals.
- Organization of conferences and workshops on project-related topics, including "project workshops" where attendance of external experts and professionals is based on invitation.
- Organization of tutorials, educational activities and thematic schools.
- Management of a publicly available web-site that includes descriptions of the main project results and allows the download of the AVANTSSAR Validation Platform and of the library of validated composed services and service architectures.
- Press conferences and press releases describing the advancement and main results of the project, so to reach and make the public aware of both the short-term and long-term impact of the project results.

The new techniques and methodologies, the formal models of the case studies, as well as the AVANTSSAR Validation Platform for the automated validation of trust and security in composed services developed by the project are of interest to researchers and professionals working on the design of new secure services. The public availability of this automatic tool supporting the security validation of services will prove to be the main vehicle for the exploitation of the project results both by the partners involved in the project as well as by industries or standardization bodies. New versions of the AVANTSSAR Validation Platform have been released regularly, along with examples and tutorials, and a mailing list for the users has been set up supported by the consortium.

We do not believe that automatic tools for the security validation of services will be attractive enough for a commercial market for reasons of potential market volume and appropriate pricing. On the other hand, all efforts should be made to increase the chance of AVANTSSAR being accepted as a de facto standard methodology and toolset within standardization bodies, thus opening a market for consulting and services relating to the security validation of services.

The industry migration activity that we carried out provides a means to expedite the transfer of the project results into the development process of the industrial partners of the consortium, and thereby reduce the security-related risk and, thus, contribute to the reduction of the total cost of ownership. Deliverable [D6.2.3] describes the integration of the AVANTSSAR Validation Platform into real industrial environments and its successful application on some industrial scenarios, with a particular focus on the lessons learned and best practices. This shows, proof of concept, that formal validation approaches such as AVANTSSAR can indeed have an impact on the market. Moreover, [D6.3] documents the activities we have carried out to migrate project results to standardization bodies, whereas the Technology Implementation Plan [D1.7] provides a more detailed market analysis.

3 Description of the Dissemination Plan

3.1 Web presence and information exchange

The website of the AVANTSSAR project is

www.avantssar.eu

and includes:

- A general introduction to the project: the objectives, the expected results, the milestones, the detailed description of the consortium and its coordinates within the Seventh Framework Programme.
- The list of events taking place in the context of the project: meetings, conferences, workshops, and their availability to the public.
- Publications originated from the project, both in the scientific community and in the general press.
- A number of relevant links: other projects, institutions and companies that are related to AVANTSSAR.
- An internal protected section, containing contact details, internal mailing lists, details about the meetings (slides, notes and so on) and other temporary technical information needed by the consortium.
- A protected section containing the deliverables and other documents for the European Commission.

Besides for the website, communication and information exchange among the members of the project is enforced via a carefully organized and maintained central repository and a number of dynamically created mailing lists.

3.2 Project workshops, lectures, tutorials, talks and presentations

Three Project Workshops have been organized, in 2008, 2010, and early 2011 (the third workshop will take place in Brussels on February 17, one day before the final review meeting, with participation restricted to project partners). In Deliverable D1.2 "Basic Dissemination and Use Plan", we had envisioned the organization of a final Project Workshop in 2010, open to external participants and possibly co-located with a one-day "Dissemination Workshop", as well as the organization of a "AVANTSSAR Technology Migration Workshop" in the context of the ForTIA industrial interest group on formal methods. However, since ForTIA was closed in the first year of AVANTSSAR and since we had several opportunities for academic and industrial dissemination, we instead carried out a large number of other activities specifically targeted to service designers from industry and standardization bodies. In these 139 activities, which are listed below (as well as in [D1.3, D1.4, D1.5]), we publicly presented methods, techniques, tools, case studies, and success stories developed within the project.

1. *AVANTSSAR: Automated Validation of Trust and Security of Service-oriented Architectures*
   Luca Viganò (UNIVR)
   Invited project presentation at the "Sensoria workshop" (meeting of the Sensoria project), Munich, Germany, March 11–14, 2008.

2. *AVANTSSAR: Automated Validation of Trust and Security of Service-oriented Architectures*
   Luca Viganò (UNIVR)
   Poster presentation at "The Future Of The Internet — Perspectives emerging from R&D in Europe", Bled, Slovenia, March 31 – April 02, 2008.

3. *A Labeled Tableaux System for the Distributed Temporal Logic DTL*
   Luca Viganò (UNIVR)
   15th International Symposium on Temporal Representation and Reasoning, Montreal, Canada, June 16–18, 2008.
   Presentation of [37].

4. *Formal Analysis of a SAML Web Browser Single Sign-On Protocol*
   Luca Viganò (UNIVR)
   5-minute talk about the results of [9] at the "Computer Security Foundations symposium" (CSF 21), Pittsburgh, USA, June 23–25, 2008.

5. *Automated Validation of Trust and Security of Service-oriented Architectures and Formal Analysis of a SAML Web Browser Single Sign-On Protocol*
   Luca Viganò (UNIVR)
   Project presentation, including a presentation of [9], at the Center for Logic and Computation of the Instituto Superior Tecnico, Lisbon, Portugal, July 18, 2008.

6. *Automated Validation of Trust and Security of Service-oriented Architectures and How we found a vulnerability in the SAML-based Single Sign-On Protocol for Google Applications*
   Luca Viganò (UNIVR)
   Project presentation, including a presentation of [9], at the Faculty of Sciences of the University of Verona, Verona, Italy, September 30, 2008.

7. *A Labeled Natural Deduction System for a Fragment of CTL**
   Luca Viganò (UNIVR)
   Symposium on Logical Foundations of Computer Science (LFCS'09), Deerfield Beach, Florida, USA, January 3–6, 2009.
   Presentation of [81].

8. *Secure pseudonymous channels*
   Luca Viganò (UNIVR)
   Presentation of [85] at the Center for Logic and Computation of the Instituto Superior Tecnico, Lisbon, Portugal, January 23, 2009.

9. *La sicurezza informatica: attacchi e soluzioni*
   Luca Viganò (UNIVR)
   Invited talk, including a project presentation, at "Infinita...mente" (a weekend of science and arts, http://www.infinitamente.univr.it/), Verona, Italy, January 31 and February 1, 2009.

10. *Towards SMT Model Checking of Array-based Systems*
    Silvio Ranise (UNIVR)
    6th International Workshop on Satisfiability Modulo Theories (SMT 08). Affiliated with CAV 2008. July 7-8, 2008. Princeton, USA.
    Presentation of [65].

11. *Light-Weight SMT-based Model Checking*
    Silvio Ranise (UNIVR)
    Eighth International Workshop on Automated Verification of Critical Systems. Glasgow, 30 September–1 October 2008.
    Presentation of [66].

12. *Fair exchange is incomparable to consensus*
Mohammad Torabi Dashti (ETH Zurich)
5th International Colloquium on Theoretical Aspects of Computing (ICTAC 08), Istanbul, Turkey, September 1–3, 2008.
Presentation of [89] .

13. *Constraint-based Verification of Cryptographic Protocols*
Michael Rusinowitch (INRIA)
NIAS-Lorentz workshop Logic and information security, September 25, 2008, Leiden, NL.

14. *Protocol and service verification*
Michael Rusinowitch (INRIA)
STIC-Tunisie project workshop, November 1, 2008, Tunis

15. *CL-AtSe, théorie et applications*
Mathieu Turuani (INRIA)
Séminaire Crypto-sécurité, November 27, 2008, IRIT, Toulouse.

16. *AVISPA, un outil d'analyse de protocoles cryptographiques*
Laurent Vigneron (INRIA)
Séminaire Crypto-sécurité, November 27, 2008, IRIT, Toulouse.

17. *On the security of Web services*
Yannick Chevalier (INRIA/UPS-IRIT)
4th Franco-Japanese Workshop on Security, Tokyo, December 5-6, 2008
Partially on a submission with Michaël Rusinowitch to the Information Processing Letters, and partially on the work with Philippe Balbiani and Marwia El Houri.

18. *Composition of Interactive Web Services Based on Controller Synthesis*
Yannick Chevalier (INRIA/UPS-IRIT)
2nd International Workshop on Web Service Composition and Adaptation (WSCA-2008), Hawai'i, July 8 2008
Presentation of the paper of Philippe Balbiani, Guillaume Feuillade, and Fahima Cheikh [25].

19. *Automatic Composition of Services with Security Policies*
Yannick Chevalier (INRIA/UPS-IRIT)
2nd International Workshop on Web Service Composition and Adaptation (WSCA-2008), Hawaii, July 8 2008
Presentation of a paper in collaboration with M. Anis Mekki and Michaël Rusinowitch [56].

20. *Composition of Web services: algorithms and complexity*
Fahima Cheikh (UPS-IRIT)
Presented during the first Interaction and Concurrency Experience Workshop, sponsored by the ESF and co-located with ICALP'08, in Reykjavik, july 2008.

21. *Composition of interactive Web services based on controller synthesis and modal logic*
Philippe balbiani (UPS-IRIT)
An invited presentation at the University of Liverpool, Computer Science Department, february 2008.

22. *A Logical Approach to Dynamic Role-Based Access Control*
Marwa El Houri (UPS-IRIT)
Presented at the AIMSA conference, september 2008.

23. *LTL Model Checking for Security Protocol Analysis*
Alessandro Armando (UGDIST)
Invited talk at the NIAS-Lorentz workshop Logic and Information Security, September 24, 2008, Leiden, NL.

24. *Verifica Automatica della Sicurezza delle Applicazioni Web: come abbiamo scoperto la vulnerabilità al servizio di Single Sign-On di Google*
Alessandro Armando (UGDIST)
Invited talk at the Security seminar after the Silicon Valley Study Tour 2008, Genova, Italy, November 4, 2008.

25. *Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps*
Roberto Carbone (UGDIST)
6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008), Hilton Alexandria Mark Center, Virginia, USA, October 27, 2008.
Presentation of a paper in collaboration with A. Armando, L. Compagna, J. Cuellar, and L. Tobarra [9].

26. *Model Checking of Security-sensitive Service-oriented Business Processes*
Serena Elisa Ponta (UGDIST)
8th International School on Foundations of Security Analysis and Design (FOSAD 2008), Bertinoro University Residential Center, Italy, August 29, 2008.

27. Invited talk titled *"Software Model Checking: new challenges and opportunities for Automated Reasoning"*.
Alessandro Armando (UGDIST)
The 1st Workshop on Practical Aspects of Automated Reasoning (PAAR-2008), Sidney, Australia, August 10, 2008.

28. *Avantssar Industry Migration: can formal methods be beneficial for our development environment?*
Luca Compagna (SAP)
SAP AG, August 5-8, 2008, Walldorf, Germany.

29. *Formal Specification and Verification for Security, and more..*
Volkmar Lotz (SAP)
SAP Research Summit 2008, June 2-6, 2008, Dresden, Germany.

30. *Formal Analysis of Security Protocols and beyond*
Luca Compagna (SAP)
SAP Research Summit 2008, June 2-6, 2008, Dresden, Germany.

31. *Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures*
Luca Compagna (SAP)
Jacques Bus visiting SAP Research S&T at SAP LABS France, November 28, 2008, Sophia Antipolis, France.

32. *Avantssar: when theory discovers real world attacks and has beneficial impact*
Jean-Christophe Pazzaglia (SAP)
Security Week at SAP LABS France, October 27-31, 2008, Sophia Antipolis, France.

33. *Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures*
Luca Compagna (SAP)
European Research towards Trusted Ambient intelligence (EuroTrust), September 17, 2008, Sophia Antipolis, France.

34. *Avantssar: when theory discovers real world attacks and has beneficial impact*
Luca Compagna (SAP)
Members of the European Parliament visiting Research institution at Sophia Antipolis, July 22, 2008, Sophia Antipolis, France.

35. *Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures*
Jean-Christophe Pazzaglia (SAP)
NESSI SECURITY Work group, November 28, 2008, Lyon, France.

36. *Realistic Threats to Self-Enforcing Privacy*
Francesco Librizzi (University of Catania, representing SAP)
4th International Symposium on Information Assurance and Security, September 9, 2008, Naples, Italy.

37. *Verifying the Security of Protocols and Systems*
Jorge Cuellar (SIEMENS)
Invited talk at the Jahrestreffen der Fachgruppe FoMSESS, Gesellschaft für Informatik e.V., March 27, 2008, Technical University of Darmstadt, Germany.

38. *Formal methods for Security Policies*
Jorge Cuellar (SIEMENS)
Class at the University of Los Andes, Bogotá, Colombia, May 2008.

39. *Security, a Sisyphean task? Or: What are our Attacker Models?*
Jorge Cuellar (SIEMENS)
Invited talk at University of Genova, June 18, 2008.

40. *Formal Methods for Web Services*
Jorge Cuellar (SIEMENS)
Class at the University of Washington, Seattle, USA, Jul/Aug 2008.

41. *Formal Methods for Secure Coding*
Jorge Cuellar (SIEMENS)
Class at the University of Los Andes, Bogotá, Colombia, November 2008.

42. *Security, a Sisyphean task?*
Jorge Cuellar, (SIEMENS)
2008 EC-ERCIM Strategic Seminar on ICT Security: Engineering Secure Complex Software Systems and Services
Brussels, Belgium, October 16, 2008.

43. *Secure pseudonymous channels*
Luca Viganò (UNIVR)
Invited talk in the Workshoplet on Formal Methods for Security, Padova, Italy, March 12, 2009.

44. *Secure pseudonymous channels*
Luca Viganò (UNIVR)
Presentation of [85] at the Department of Informatics and Mathematics, Technical University of Denmark, Copenhagen, Denmark, April 2, 2009.

45. *Validation methodologies*
Luca Viganò (UNIVR)
Invited keynote at the FIA Prague Trust and Identity Session "Identity Provisioning in service platforms", Future Internet Conference, Prague, Czech Republic, May 12, 2009.

46. *Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures*
Luca Viganò (UNIVR)
Presentation of [35] at the Center for Logic and Computation of the Instituto Superior Tecnico, Lisbon, Portugal, July 10, 2009.

47. *On-the-Fly Model Checking of Security Protocols and Web Services*
Luca Viganò (UNIVR)
Invited lecture at the 9th International School on Foundations of Security Analysis and Design (FOSAD), Centro Universitario Residenziale di Bertinoro, FC, Italy, August 29 – September 04, 2009.

48. *Verso la validazione automatica della sicurezza delle architetture orientate ai servizi*
Luca Viganò (UNIVR)
Faculty of Sciences of the University of Verona, Verona, Italy, September 23, 2009.

49. *Automated Validation of Trust and Security of Service-oriented Architectures*
Luca Viganò (UNIVR)
Invited talk at the ZISC Colloquium, Zurich Information Security Center (ZISC), Zurich, Switzerland, November 24, 2009.

50. *Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures*
Michele Barletta (UNIVR).
Presentation of [35] at the 9th International School on Foundations of Security Analysis and Design (FOSAD), Centro Universitario Residenziale di Bertinoro, FC, Italy, September 04, 2009.

51. *Towards Verification of Security-Aware Transaction E-services*
Silvio Ranise (UNIVR)
International Workshop on First-Order Theorem Proving, Oslo, Norway, July 6–7 2009.
Presentation of [90].

52. *Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures*
Silvio Ranise (UNIVR)
International Symposium on Secure Computing (SecureCom 2009), Vancouver, Canada, August 29–31.
Presentation of [35].

53. *Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures*
Silvio Ranise (UNIVR)
Microsoft Research, Redmond, WA, USA, September 01.
Invited presentation of [35].

54. *Optimistic fair exchange using trusted devices*
Mohammad Torabi Dashti (ETH Zurich)
11th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2009), Lyon, France, November 3–6, 2009.
Presentation of [93]

55. *From Dolev-Yao to Strong Adaptive Corruption: Analyzing Security in the Presence of Compromising Adversaries*
Cas Cremers (ETH Zurich)
Invited talk at the Security Seminar at VERIMAG, Grenoble, France, February 10, 2009.

56. *From Dolev-Yao to Strong Adaptive Corruption: Analyzing Security in the Presence of Compromising Adversaries*
Cas Cremers (ETH Zurich)
Invited talk in the Workshoplet on Formal Methods for Security, Padova, Italy, March 12, 2009.

57. *Cryptographic protocols as Building Blocks: From the Man-in-the-Middle attack to Compositional Symbolic Analysis*
Cas Cremers (ETH Zurich)
Invited talk at the LSV Seminar, ENS Cachan, Paris, France, March 31, 2009.

58. *Session-state Reveal is stronger than Ephemeral Key Reveal: Attacking the NAXOS Authenticated Key Exchange protocol*
Cas Cremers (ETH Zurich)
ACNS'09, Paris, France, June 2, 2009.

59. *Formalizing and analyzing compromising adversaries*
Cas Cremers (ETH Zurich)
Invited talk at the Information Security seminar at Royal Holloway University of London, November 12, 2009.

60. *Validating Integrity for the Ephemerizer's Protocol with CL-Atse*
Mathieu Turuani (INRIA)
1st Luxembourg Day on Security and Reliability. Luxembourg, February 10, 2009.

61. *Decidable Analysis for a Class of Cryptographic Group Protocols with Unbounded Lists*
Najah Chridi (INRIA)
22nd IEEE Computer Security Foundations Symposium. Port Jefferson. July 8-10. Presentation of [61].

62. *A Flexible Access Control Model for Distributed Collaborative Editors*
Asma Cherif (INRIA)
Secure Data Management, 6th VLDB Workshop, SDM 2009. Lyon, August 28. Presentation of [74].

63. *Orchestration under security constraints.*
Mohamed Anis Mekki (INRIA)
6th International Workshop on Formal Aspects in Security and Trust (FAST2009). Eindhoven, the Netherlands, November 5–6, 2009.
Presentation of [15].

64. *Master Courses on Security of Web Services.*
and *Master Courses on Security of Networks and Services.*
Laurent Vigneron (INRIA, Nancy 2) Fall 2009. University of Nancy, France.

65. *Approche logique pour les contraintes de contrôle d'accès dans les services Web*
Marwa El Houri (UPS-IRIT)
1er atelier sur les droits d'accès à des services et des données définis dans un environnement collaboratif (SDEC 2009). Toulouse, May 2009.
Presentation of [31].

66. *A logical framework for reasoning about policies with trust negotiations and workflows in a distributed environment*
Marwa El Houri (UPS-IRIT)
4th International Conference on Risks and Security of Internet and Systems (CRiSIS 2009). Toulouse, October 2009.
Presentation of [32].

67. *Résultats de complexité pour le problème de la composition d'agents*
Guillaume Feuillade (UPS-IRIT)
5èmes journées francophones sur les modèles formels de l'interaction (MFI 2009). Lannion, June 2009.
Presentation of [27].

68. *Controller/orchestrator synthesis via filtration*
Guillaume Feuillade (UPS-IRIT)
Methods for Modalities (M4M 2009). Copenhagen, November 2009.
Presentation of [28].

69. *Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps*
Alessandro Armando (UGDIST)
Invited Talk at Center for Information Technology - IRST, Fondazione Bruno Kessler, Trento, March 2, 2009.

70. *Formal Specification and Automatic Analysis of Business Processes under Authorization Constraints: an Action-based Approach.*
Serena Elisa Ponta (UGDIST)
6th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'09). Linz, Austria, August 31–September 4, 2009.
Presentation of [14].

71. *Model Checking of Security-sensitive Business Processes.*
Serena Elisa Ponta (UGDIST)
6th International Workshop on Formal Aspects in Security and Trust (FAST2009). Eindhoven, the Netherlands, November 5–6, 2009.
Presentation of [15].

72. *Algebraic Properties in Alice and Bob Notation*
Sebastian Mödersheim (IBM)
4th International Conference on Availability, Reliability and Security (ARES), Fukuoka, Japan, March 16th - 19th, 2009.
Presentation of [84].

73. *Secure Pseudonymous Channels*
Sebastian Mödersheim (IBM)
14th European Symposium on Research in Computer Security (ESORICS), Saint Malo, France, September 21–23, 2009.
Presentation of [85].

74. *Integrating Automated and Interactive Protocol Verification*
Sebastian Mödersheim (IBM) (with Achim Brucker (SAP))
6th International Workshop on Formal Aspects in Security and Trust (FAST), Eindhoven, the Netherlands, November 5–6, 2009.
Presentation of [46].

75. *A calculus to detect guessing attacks*
Marius Minea (IEAT)
12^{th} International Conference on Information Security, Pisa, Italy, September 7–9, 2009.
Presentation of [67].

76. *Validating Security Protocols under the General Attacker*
Xavier Chantry (SAP)
Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS 2009, March 28-29, 2009, York, UK.
Presentation of [18].

77. *Attacking Each Other*
Xavier Chantry (SAP)
17th International Workshop on Security Protocols (IWSP 2009), April 1-3, 2009, Cambridge, UK.
Presentation of [20].

78. *AVANTSSAR Demo on Trust and Security of Internet of Services (IoS)*
Alessandro Sorniotti (SAP)
The Future of the Internet Conference (FIA Prague), May 11-13, 2009, Prague, Czech Republic.
Demo of the discovery of the serious vulnerability to SAML-based SSO for Google Apps.

79. *Avantssar Industry Migration: NW SAML NGSSO - Initial set of results of 2009 collaboration*
Luca Compagna (SAP)
SAP AG - NW SIM, June 16, 2009, Virtual talk.
The initial set of results have been discussed with the SAP Steering

Committee and Experts Group (people selected from SAP NW Security and Identity Management).

80. *Avantssar Industry Migration: NW BPM - security validator plugin - interim result of 2009 collaboration*
Wihem Arsac (SAP)
NetWeaver BPM transfering activity review, September 28, 2009, Walldorf, Germany.
The interim results have been discussed with the SAP NetWeaver BPM transfering committee (people selected from SAP NW Business Process Management).

81. *Model Checking (security-annotated) Business Processes in SAP NetWeaver BPM*
Wihem Arsac (SAP)
Security Week at SAP LABS France, November 23-27, 2009, Sophia Antipolis, France.

82. *Avantssar Industry Migration: NW SAML NGSSO - results of 2009 collaboration and next steps*
Luca Compagna (SAP)
SAP AG - NW SIM, November 26, 2009, Walldorf, Germany.
The final results achieved in 2009 and next steps have been discussed with the SAP Steering Committee and Experts Group (people selected from SAP NW Security and Identity Management).

83. *Avantssar Industry Migration: NW BPM - our security validator plugin*
Luca Compagna (SAP)
SAP AG - NW BPM, November 27, 2009, Walldorf, Germany.
Presentation of the pre-final results achieved to core people of SAP NetWeaver BPM.

84. *Avantssar Industry Migration: NW BPM - our security validator plugin*
Wihem Arsac (SAP)
SAP AG - Sales Montpellier, December 14, 2009, Virtual talk.
Presentation of our security validator plugin to SAP Sales. This work may be showed in the future to events targeting SAP customers.

85. *Avantssar Industry Migration: NW BPM - security validator plugin - result of 2009 collaboration and next steps*
Wihem Arsac (SAP)
NetWeaver BPM transfering activity review, December 15, 2009, Walldorf, Germany.

The final results achieved in 2009 and next steps have been discussed with the SAP NetWeaver BPM transfering committee (people selected from SAP NW Business Process Management).

86. *Security Policy Specification and Validation with the AVANTSSAR Platform*
Luca Viganò (UNIVR)
Invited talk at the International Workshop on Policies for the Future Internet, CRN Pisa, Italy, February 5, 2010.

87. *A History of Until*
Luca Viganò (UNIVR)
Center for Logic and Computation of the Instituto Superior Tecnico, Lisbon, Portugal, February 10, 2010.

88. *Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures*
Luca Viganò (UNIVR)
Presentation of [35, 36] at SOFT Workshop, Pisa, Italy, June 23–24, 2010.

89. *Logica Computazionale*
Luca Viganò (UNIVR)
Lecture at Summer School AILA – Associazione Italiana di Logica e sue Applicazioni, including a presentation of AVANTSSAR, Gargnano, Italy, August 29 – September 4, 2010.

90. *Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA*
Massimo Merro (UNIVR)
Presentation of [44] at eighth IEEE International Conference on Software Engineering and Formal Methods, SEFM 2010, Pisa, Italy, September 13–18, 2010.

91. *Automated Validation of Security-sensitive Web Services specified in BPEL and RBAC*
Luca Viganò (UNIVR)
Presentation of [48] at WoSS 2010 — 1st Workshop on Software Services, Timisoara, Romania, September 25, 2010.

92. *Automated Validation of Internet Security Protocols*
Luca Viganò (UNIVR)
Invited tutorial at SYNASC 2010 — 12th International Symposium on

Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September 25, 2010. Invited paper [34].

93. *Automated Validation of Security-sensitive Web Services specified in BPEL and RBAC*
Luca Viganò (UNIVR)
Presentation of [48] at Center for Logic and Computation of the Instituto Superior Tecnico, Lisbon, Portugal, October 15, 2010.

94. *Policy Monitoring in First-order Temporal Logic*
David Basin (ETH)
Invited talk at Federated Logic Conference FLOC 2010, Edinburgh, Scotland, July 16, 2010.

95. *Degrees of Security: Protocol Guarantees in the Face of Compromising Adversaries*
David Basin (ETH)
Invited talk at 19th EACSL Annual Conference on Computer Science Logic (CSL), Brno, Czech Republic, Aug 26, 2010.

96. *Modeling and Analyzing Security in the Presence of Compromising Adversaries*
Cas Cremers (ETH)
ESORICS'10, Athens, Greece, September 20–22, 2010.

97. *Formal Specification and Verification of Security Services*
Mohammad Torabi Dashti (ETH)
Invited talk at IST Lisbon, June 2010.

98. *Semi-linear Parikh images of regular expressions via reduction*
Mohammad Torabi Dashti (ETH)
MFCS'10, Brno, Czech Republic, August 23–27, 2010.

99. *Formalizing the failure detectors abstraction in set theory*
Mohammad Torabi Dashti (ETH)
Invited talk at *Many Faces of Protocols and Knowledge*, Amsterdam. 21 Sept 2010.

100. *Applications of protocol verification to service security*
Michael Rusinowitch (INRIA)
Invited talk on at SecRet 2010, 5th International Workshop on Security and Rewriting Techniques, Valencia (Spain), June 18, 2010.

101. *Rewrite-based verification of XML updates*
Michael Rusinowitch (INRIA)
PPDP'10 Proceedings of the 12th international ACM SIGPLAN symposium on Principles and practice of declarative programming, Hagenberg, Austria, July 26–28, 2010.

102. *Decidability of Ground Entailment Problems for Saturated Sets of Clauses*
Yannick Chevalier (UPS-IRIT)
Presentation at the International Conference on Logic for Programming Artificial Intelligence and Reasoning of a joint paper with Mounira Kourjieh, April 24 – May 1, 2010, Dakar, Sénégal.

103. *Finitary deduction systems*
Yannick Chevalier (UPS-IRIT)
Presentation of [53] by Yannick Chevalier at SecRet 2010, 5th International Workshop on Security and Rewriting Techniques, Valencia (Spain), June 18, 2010.

104. *An Intruder Model for Trust Negotiation*
Yannick Chevalier (UPS-IRIT)
Presentation of [33] at the 5th International Conference on Risks and Security of Internet and Systems (CRISIS), October 10–13 2010, Montréal, Canada.

105. *Orchestration under Security Constraints*
Yannick Chevalier (UPS-IRIT)
Talk part of the "AVANTSSAR session" at Software Technologies Concertation on Formal Methods for Components and Objects (FMCO 2010), Graz, Austria, November 30, 2010.

106. *Equivalence of Symbolic Derivations*
Yannick Chevalier (UPS-IRIT)
Invited presentation at the AVOTÉ workshop, December 7, Cachan, France.

107. *New decidability result for ground entailment problems and application to security protocols* (UPS-IRIT)
Mounira Kourjieh (UPS-IRIT)
Presentation of [54] at the ESSLLI workshop on Logics in Security, Copenhagen, August 2010.

108. *LTL Model-Checking for Security Protocols*
Roberto Carbone (UGDIST)

Presentation of the PhD Thesis at Security Summit, CLUSIT prize 2010, Milano, Italy, March 18, 2010.

109. *Verifying Security Protocols Using Channels*
Sebastian Mödersheim (IBM)
Introducing AVANTSSAR to the MT-Lab, DTU Copenhagen, May 10, 2010.

110. *Abstraction by Set-Membership*
Sebastian Mödersheim (IBM)
Invited talk at SOFT Workshop, Pisa, Italy, June 23–24, 2010.

111. *Protocol Modelling and Verification*
Sebastian Mödersheim (IBM)
Lecturer at summer School at East China Normal University, Shanghai, PR China, July 18–22, 2010.

112. *A formal model of identity mixer*
Sebastian Mödersheim (IBM)
Presentation of [50] at 15th International Workshop on Formal Methods for Industrial Critical Systems, Antwerp, Belgium, September 19–21, 2010.

113. *Abstraction by Set-Membership—Verifying Security Protocols and Web Services with Databases*
Sebastian Mödersheim (IBM)
Presentation of [88] at 17th ACM Conference on Computer and Communications Security (CCS 2010), Chicago, USA, October 02–10, 2010.

114. *A formal approach for automated reasoning about off-line and non-blockable on-line guessing*
Bogdan Groza (IEAT)
Presentation of [68] at the 14^{th} International Conference on Financial Cryptography and Data Security, Tenerife, Spain, January 25, 2010.

115. *Controlling the unknown*
Casandra Holotescu (IEAT)
Presentation of [71] at the First International Conference on Formal Verification of Object-Oriented Software, Paris, France, June 30, 2010.

116. *Error-avoiding adaptors for black-box software components*
Casandra Holotescu (IEAT)
Presentation of [72] at the 25^{th} IEEE/ACM International Conference on

Automated Software Engineering (Doctoral Symposium), Antwerpen, Belgium, September 21, 2010.

117. *Black-box composition: a dynamic approach*
Casandra Holotescu (IEAT)
Presentation of [73] at the Ninth International Workshop on Specification and Verification of Component-Based Systems, Santa Fe, NM, USA, November 12, 2010.

118. *Customized protocol modeling for detection of guessing and DoS attacks*
Marius Minea (IEAT)
Talk part of the "AVANTSSAR session" at Software Technologies Concertation on Formal Methods for Components and Objects (FMCO 2010), Graz, Austria, November 30, 2010.

119. *Avantssar Industry Migration: security validation for Internet of Services*
Luca Compagna (SAP)
Workshop on Internet of Services at SAP, SAP Research Centers Darmstadt, Germany, February 2–3, 2010.

120. *Avantssar Industry Migration: security validator for NW BPM*
Luca Compagna (SAP)
SAP AG, Walldorf, Germany, February 5, 2010.

121. *Model Checking (security-annotated) Business Processes in SAP NetWeaver BPM*
Wihem Arsac (SAP)
Visit of Gabriel Silbermann (CA Senior Vice President and Director of CA Labs) at SAP Labs France, Sophia Antipolis, France, March 5, 2010.

122. *Security Validation of Business Processes*
Luca Compagna (SAP)
Visit of Gustav Kalbe (Deputy Head of Unit Trust and Security) at SAP Labs France, Sophia Antipolis, France, March 11, 2010.

123. *Model-checking driven security testing of web-based applications*
Giancarlo Pellegrino (SAP)
3rd International Conference on Software Testing, Verification, and Validation Workshops, Paris, France, April 6–10, 2010.

124. *SAP Security Info Session: Formal Analysis of Security Protocols and Services*

Luca Compagna (SAP)
Ongoing series of virtual SAP product security information sessions, Sophia Antipolis, France, April 7, 2010.

125. *Avantssar Industry Migration: applied formal methods for security at SAP*
Luca Compagna (SAP)
Workshop on Applied Formal Methods at SAP, SAP Research Centers Karlsruhe, Germany, May 5, 2010.

126. *Avantssar Industry Migration: security validator for NW BPM*
Luca Compagna (SAP)
SAP AG, Walldorf, Germany, May 6, 2010.

127. *SAP Security Awareness Campaign: Security Validation of on-premise Business Processes*
Giancarlo Pellegrino (SAP)
SAP AG, Walldorf, Germany, June 10, 2010.

128. *SAP Security Awareness Campaign: Security Validation for NW BPM*
Luca Compagna (SAP)
SAP Labs France, Sophia Antipolis, Germany, September 22, 2010.

129. *SAP Demo Jam: Security Validation of Business Process*
Luca Compagna and Samuel Kaluvuri (SAP)
SAP Labs France, Sophia Antipolis, Germany, December 8, 2010.

130. *Formal security analysis and certification in industry, at the example of an AADS*
David von Oheimb (SIEMENS)
Guest lecture in the context of the course "Security Engineering" held by Ricarda Weber at the TU Munich, Germany, summer semester 2010.

131. *AVANTSSAR — an overview with examples*
David von Oheimb (SIEMENS)
Presentation at the GI FoMSESS annual meeting, Berlin, Germany, April 04, 2010.

132. *Model checking SOA Security: a report on work in progress in AVANTSSAR*
David von Oheimb (SIEMENS)
Presentation to the DFKI Research Group "Safe and Secure Systems", Saarbrücken, Germany, July 19, 2010.

133. *Formal security analysis and certification in industry*
David von Oheimb (SIEMENS)
Guest lecture in the context of the course "IT Security" held by Peter Hartmann at the Hochschule Landshut, Germany, winter semester 2010/2011.

134. *SPaCIoS — Secure Provision and Consumption in the Internet of Services and ASLan++ — the AVANTSSAR Specification Language*
David von Oheimb (SIEMENS)
Invited talk at the Kick-Off Meeting of the DIAMONDS project, Berlin, Germany, November 18, 2010.

135. *ASLan++ — the AVANTSSAR Specification Language*
David von Oheimb (SIEMENS)
Talk part of the "AVANTSSAR session" at Software Technologies Concertation on Formal Methods for Components and Objects (FMCO 2010), Graz, Austria, November 30, 2010.

136. *Formal security analysis and early assessment in industry*
Jorge Cuellar (SIEMENS)
Guest lecture in the course "Security Security" of a. Univ.-Prof. Johannes Sametinger at the Institut für Wirtschaftsinformatik, Software Engineering, Johannes Kepler Universität Linz, Winter Semester, January 2010.

137. *Security Assessment of Software in industry*
Jorge Cuellar (SIEMENS)
Guest lecture in the course "Security Security" of Prof. Joachim Posegga, Universität Passau, Sommer Semester 2010.

138. *Formal Methods, with Emphasis on Security*
Jorge Cuellar (SIEMENS)
Summer Course at the Universidad de los Andes, Bogota, June, 2010.

139. *Security Assessment of Software in industry*
Jorge Cuellar (SIEMENS)
Guest lecture in the course "Security Security" of a. Univ.-Prof. Johannes Sametinger at the Institut für Wirtschaftsinformatik, Software Engineering, Johannes Kepler Universität Linz, Winter Semester, January 2011.

3.3 Involvement in scientific events

The members of AVANTSSAR have been playing an active role in the organization of 97 AVANTSSAR-related scientific events:

3.3.1 Scientific events sponsored by AVANTSSAR

1. *ARSPA*
   Workshop series on *Automated Reasoning for Security Protocol Analysis*.
   Several project participants, rotating yearly.

2. *FCS-ARSPA-WITS'08*
   Joint Workshop on "Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security", affiliated with LICS 2008 and CSF 21.
   Pittsburgh, PA, USA, June 21–22, 2008.
   Luca Viganò (UNIVR) co-chair.
   Alessandro Armando (UGDIST), Cas Cremers (ETH Zurich), Sebastian Mödersheim (IBM) PC members.

3. *ARSPA-WITS'09*
   Joint Workshop on "Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security", affiliated with ETAPS 2009.
   York, UK, March 28 and 29, 2009.
   Luca Viganò (UNIVR) co-chair.
   Luca Compagna (SAP) and Sebastian Mödersheim (IBM) PC members.

4. *ARSPA-WITS'10*
   Joint Workshop on "Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security", affiliated with ETAPS 2010.
   Paphos, Cyprus, March 27 and 28, 2010.
   Alessandro Armando (UGDIST) co-chair.
   Luca Viganò (UNIVR), Cas Cremers (ETH Zurich), Michael Rusinowitch (INRIA), Yannick Chevalier (UPS-IRIT), Sebastian Mödersheim (IBM), Luca Compagna (SAP) and Jorge Cuellar (SIEMENS) PC members.

5. *ARSPA-WITS'11/ TOSCA'11*
   ARSPA-WITS'11 (joint Workshop on "Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security") from this year on TOSCA'11 ("Theory of Security and Applications"), affiliated

with ETAPS 2011.
Saarbrücken, Germany, March 31 and April 01, 2011.
Sebastian Mödersheim (IBM) co-chair. Luca Viganò (UNIVR), Cas Cremers (ETH Zurich), Michael Rusinowitch (INRIA), Yannick Chevalier (UPS-IRIT), Alessandro Armando (UGDIST), Luca Compagna (SAP) and Jorge Cuellar (SIEMENS) PC members.

6. *SecTest'11*
The "Second International Workshop on Security Testing", affiliated with "The IEEE International Conference on Software Testing, Verification and Validation" (ICST 2011).
Berlin Germany, March 25, 2011.
Luca Viganò (UNIVR) co-chair.
Alessandro Armando (UGDIST) and Jorge Cuellar (SIEMENS) Steering Committee members. Invited talk by David Basin (ETH Zurich).

3.3.2 Other scientific events

7. *ALICS'08*
Applications of Logic in Computer Security.
Affiliated with LPAR 2008, Doha, Qatar, November 22, 2008.
Luca Viganò (UNIVR), Alessandro Armando (UGDIST), Luca Compagna (SAP) PC members.

8. *APE'08*
Advances in Policy Enforcement.
Affiliated with ARES 2008, Barcelona, Spain, March 4-7, 2008.
Luca Viganò (UNIVR) PC member.

9. *ARES'08*
3rd International Conference on Availability, Reliability and Security.
Barcelona, Spain, March 4-7, 2008.
Luca Viganò (UNIVR) PC member.

10. *CEDAR 2008*
Complexity, Expressibility, and Decidability in Automated Reasoning.
Affiliated with IJCAR 2008, Sydney, Australia, August 10-15, 2008.
Silvio Ranise and Luca Viganò (UNIVR) PC members.

11. *FCS*
Workshop series on the Foundations of Computer Security.
Luca Viganò (UNIVR) chair of the Steering Committee.

12. *FIS 2008*
    Future Internet Symposium.
    Vienna, Austria, September 28-30, 2008.
    Luca Viganò (UNIVR), Alessandro Armando (UGDIST), Luca Compagna (SAP) PC members.

13. *FMWS 2008*
    Formal Methods for Wireless Systems.
    Satellite workshop of CONCUR 2008, Toronto, Canada, August 23, 2008.
    Luca Viganò (UNIVR) PC member.

14. *PAAR-2008*
    Workshop on Practical Aspects of Automated Reasoning (PAAR-2008).
    Affiliated with IJCAR 2008, Sydney, Australia, August 10-15, 2008.
    Silvio Ranise and Luca Viganò (UNIVR) PC members.

15. *Securware 2008*
    The Second International Conference on Emerging Security Information, Systems and Technologies.
    Cap Esterel, France, August 25-31, 2008.
    Luca Viganò (UNIVR) PC member.

16. *SMT 08*
    6th International Workshop on Satisfiability Modulo Theories Affiliated with CAV 2008 July 7-8, 2008 Princeton, USA
    Silvio Ranise (UNIVR) PC member.

17. *Verify 2008*
    5th International Verification Workshop.
    Affiliated with IJCAR 2008, Sydney, Australia, August 10-15, 2008.
    Luca Viganò (UNIVR) PC member.

18. *ASIACCS 2008*
    3rd ASIA Computer and Communication Security Conference.
    Tokyo Japan, March 2008.
    David Basin (ETH Zurich) PC member.

19. *DEON 2008*
    9th International Conference on Deontic Logic in Computer Science.
    Luxembourg, July 2008.
    David Basin (ETH Zurich) PC member.

20. *ESORICS 2008*
    13th European Symposium on Research in Computer Security.
    Malaga, Spain, 2008.
    David Basin (ETH Zurich) PC member.

21. *ICFEM 2008*
    10th International Conference on Formal Engineering Methods.
    Japan 2008.
    David Basin (ETH Zurich) PC member.

22. *ISC 2008*
    11th Information Security Conference.
    Taipei, Taiwan, September 2008.
    David Basin (ETH Zurich) PC member.

23. *ZISC Workshop 2008*
    Advanced Concepts of Access and Usage Control.
    Zurich, Switzerland, September 2008.
    David Basin (ETH Zurich) organizer.

24. *RTA'08*
    19th International Conference on Rewriting Techniques and Applications,
    Hagenberg, Austria, July 15-17, 2008.
    Michael Rusinowitch (INRIA) PC member.

25. *SARSSI 2008*
    3eme Confèrence sur la Sècuritè des Architectures Rèseaux et des Systèmes d'Information.
    Loctudy, France, October 13-17, 2008.
    Michael Rusinowitch (INRIA) PC member.

26. *SecReT'08*
    3rd International Workshop on Security and Rewriting Techniques.
    Affiliated workshop of CSF.
    Pittsburgh, USA, June 22, 2008.
    Michael Rusinowitch (INRIA) PC member.

27. *AISC 2008*
    9th International Conference on Artificial Intelligence and Symbolic Computation.
    Birmingham, UK, 31 July-2 August, 2008.
    Alessandro Armando (UGDIST) PC member.

28. *ASE2008*
    23rd IEEE/ACM International Conference on Automated Software Engineering.
    L'Aquila, Italy, September 15-19 2008.
    Alessandro Armando (UGDIST) PC member.

29. *CISIS'08*
    International Workshop on Computational Intelligence in Security for Information Systems.
    Genova, Italy, October 23-24, 2008.
    Alessandro Armando (UGDIST) PC member.

30. *IJCAR 2008*
    International Joint Conference on Automated Reasoning.
    Sydney, Australia, August 11-16, 2008.
    Alessandro Armando (UGDIST) co-chair.
    Silvio Ranise (UNIVR), Luca Viganò (UNIVR), Michael Rusinowitch (INRIA) PC members.

31. *FACS 2008*
    5^{th} International Workshop on Formal Aspects of Component Software.
    Málaga, Spain, September 10-12, 2008.
    Marius Minea (IEAT) PC member.

32. SAVCBS 2008
    7^{th} International Workshop on Specification and Verification of Component-Based Systems.
    Affiliated workshop of SIGSOFT/FSE.
    Atlanta, Georgia, USA, November 9-10, 2008.
    Marius Minea (IEAT) PC member.

33. *2008 EC-ERCIM Seminar on ICT Security*
    Engineering Secure Complex Software Systems and Services
    Brussels, 16 October 2008.
    Volkmar Lotz (SAP) member of the Organizing Committee.

34. *SAC SEC 2008*
    Security Track at the ACM Symposium on Applied Computing.
    Fortaleza, Ceara, Brazil, March 16-20, 2008.
    Giampaolo Bella (SAP) chair.

35. *SAC SEC 2009*
    Security Track at the ACM Symposium on Applied Computing.

Honolulu (USA) March 8-12, 2009. Giampaolo Bella and Luca Compagna (SAP) co-chairs.

36. *FM'08*
    15th International Symposium on Formal Methods.
    Åbo Akademi University Turku, Finland, May 26-30, 2008.
    Jorge Cuellar (SIEMENS) co-chair.
    David Basin (ETH Zurich), Alessandro Armando (UGDIST), Marius Minea (IEAT) PC members.

37. *ForTIA I-Day'08*
    ForTIA Industry Day at 15th International Symposium on Formal Methods (FM'08),
    Holiday Club Turku, Finland, May 28, 2008.
    Jorge Cuellar (SIEMENS) FM'08 co-chair.
    David von Oheimb (SIEMENS) ForTIA secretary.

38. *FCS'09*
    Workshop on Foundations of Computer Security (Affiliated with LICS'09).
    Los Angeles, California, USA, August 10, 2009.
    Luca Viganò (UNIVR) and Cas Cremers (ETH Zurich) PC members.

39. *ADDCT'09*
    Workshop on Automated Deduction: Decidability, Complexity, Tractability (Affiliated with CADE-22).
    McGill University, Montreal, Canada, August 2–7, 2009.
    Luca Viganò and Silvio Ranise (UNIVR) PC members.

40. *ARES'09*
    International Dependability Conference.
    Fukuoka, Japan, March 16–19 2009.
    Luca Viganò (UNIVR) PC member.

41. *ESORICS'09*
    14th European Symposium on Research in Computer Security.
    Saint Malo France, September 21–25, 2009.
    Luca Viganò (UNIVR) and David Basin (ETH Zurich) PC members.

42. *FIS'09*
    The Second Future Internet Symposium.
    Berlin, Germany, September 1–3, 2009
    Luca Viganò (UNIVR) and Alessandro Armando (UGDIST) PC members.

43. *FMWS'09*
    Second International Workshop on Formal Methods for Wireless Systems (Satellite workshop of CONCUR 2009).
    Bologna, Italy, September 1–4, 2009.
    Luca Viganò (UNIVR) PC member.

44. *SECREYPT'09*
    International Conference on Security and Cryptography.
    Milan, Italy, July 7–10, 2009.
    Luca Viganò (UNIVR) PC member.

45. *SECURWARE'09*
    The Third International Conference on Emerging Security Information, Systems and Technologies.
    Athens/Glyfada, Greece, June 18–23, 2009.
    Luca Viganò (UNIVR) PC member.

46. *STM'09*
    5th International Workshop on Security and Trust Management (In conjunction with ESORICS'09).
    Saint Malo France, September 24–25, 2009.
    Luca Viganò (UNIVR) and Cas Cremers (ETH Zurich) PC members.

47. *AVOCS*
    Workshop on Automated Verification of Critical Systems.
    Swansea University, UK, 23-25 September 2009.
    Silvio Ranise (UNIVR) PC member.

48. *AVOCS*
    Workshop on Automated Verification of Critical Systems.
    University of Düsseldorf, Germany, 20-23 September 2010.
    Silvio Ranise (UNIVR) PC member.

49. *PAAR*
    FLoC/IJCAR'10 Workshop on Practical Aspects of Automated Reasoning.
    Edinburgh, UK, July 2010.
    Silvio Ranise (UNIVR) PC member.

50. *FroCoS*
    International Symposium on Frontiers of Combining Systems.
    Trento, Italy, September 16–18, 2009.
    Silvio Ranise (UNIVR) PC member.

51. *SMT*
International Workshop on Satisfiability Modulo Theories (affiliated with CADE 2009).
McGill University, Montreal, Canada, August 2–3, 2009.
Silvio Ranise (UNIVR) PC member.

52. *FTP*
International Workshop on First-Order Theorem Proving (co-located with TABLEAUX 2009).
University of Oslo, Norway, July 6–7 2009
Silvio Ranise (UNIVR) PC member.
Michael Rusinowitch (INRIA) PC member.

53. *SAC'09*
24th ACM Symposium on Appplied Computing
Honolulu, USA, March 8–12, 2009. David Basin (ETH Zurich) PC member.

54. *ASIACCS'09*
4th ASIA Computer and Communication Security Conference
Sidney, Australia, March 2009.
David Basin (ETH Zurich) PC member.

55. *iNetSec'09*
Workshop on Open Research Problems in Network Security.
Zurich, Switzerland, April 2009.
David Basin (ETH Zurich) PC member.

56. *WiSec'09*
2nd ACM Conference on Wireless Network Security.
Zurich, Switzerland, May 2009.
David Basin (ETH Zurich) Conference Chair.

57. *SecReT'09*
4th International Workshop on Security and Rewriting Techniques.
New York, USA, July 2009.
David Basin (ETH Zurich) PC member.

58. *EUROPKI'09*
The sixth European PKI Workshop.
Pisa, Italy, September 9-11, 2009.
Cas Cremers (ETH Zurich) PC member.

59. *SAC SVT 2010*
    Software Verification and Testing Track at the ACM Symposium on Applied Computing.
    Lausanne, Switzerland, March 22-26, 2010.
    Mohammad Torabi Dashti (ETH Zurich) PC member.

60. *ASIACCS'10*
    ACM Symposium on Information, Computer and Communications Security (ASIACCS).
    Beijing, China, March 2010.
    David Basin (ETH Zurich) Program Chair.
    Michael Rusinowitch (INRIA) PC member.

61. *CADE*
    22nd International Conference on Automated Deduction.
    McGill University, Montreal, Canada, August 2–7, 2009
    Michael Rusinowitch (INRIA) PC member

62. *CRISIS*
    The 4th International Conference on Risks and Security of Internet and Systems 2009 (IEEE technical co-sponsorship in cooperation with ACM SIGSAC Supported by SEE).
    Toulouse, France October 19–22, 2009.
    Michael Rusinowitch (INRIA) PC member

63. *SARSSI'09*
    Conférence sur la sécurité des architectures réseaux et des systèmes d'information.
    Luchon, France, June 22–26, 2009.
    Michael Rusinowitch (INRIA) PC member

64. *1st Luxembourg Day on Security and Reliability.*
    University Campus Kirchberg, Luxembourg city, Luxembourg, February 10, 2009.
    Michael Rusinowitch (INRIA) PC member

65. *ASE2010*
    25th IEEE/ACM International Conference on Automated Software Engineering.
    Antwerp, Belgium, September 20–24, 2010.
    Alessandro Armando (UGDIST), PC member

66. *IJCAR 2010*
    5th International Joint Conference on Automated Reasoning.
    Edinburgh, Scotland, July 16–19, 2010.
    Alessandro Armando (UGDIST), PC member

67. *AISC 2010*
    10th International Conference on Artificial Intelligence and Symbolic Computation.
    Paris, France, July 5–6, 2010.
    Alessandro Armando (UGDIST), PC member

68. *Secret 2010*
    Workshop on Security and Rewriting Techniques.
    Port Jefferson, New York, USA, July 10–11, 2009.
    Yannick Chevalier (UPS-IRIT), PC member

69. *ARES 2010*
    The Fifth International Conference on Availability, Reliability and Security.
    Krakow,Poland, February 15–18, 2010.
    Sebastian Mödersheim (IBM), PC member

70. *FM'09*
    16^{th} International Symposium on Formal Methods.
    Eindhoven, the Netherlands, November 2–6, 2009.
    Jorge Cuellar (SIEMENS), Marius Minea (IEAT) PC members.

71. *SAC SEC 2009*
    Security Track at the ACM Symposium on Applied Computing.
    Honolulu, USA, March 8–12, 2009. Giampaolo Bella and Luca Compagna (SAP) co-chairs.

72. *SAC SEC 2010*
    Security Track at the ACM Symposium on Applied Computing.
    Lausanne, Switzerland, March 22–26, 2010. Luca Compagna and Alessandro Sorniotti (SAP) co-chairs. Cas Cremers (ETH Zurich) PC member.

73. *SecCo 2011*
    The 9th International Workshop on Security Issues in Concurrency.
    Aachen, Germany. September 5 2011.
    Luca Viganò (UNIVR) PC member.

74. *FAST 2011*
    The 7th International Workshop on Formal Aspects of Security &

Trust, co-located with the European Symposium on Research in Computer Security (ESORICS 2011).
Leuven, Belgium. September 15-16, 2011.
Luca Viganò (UNIVR) PC member.

75. *SECURWARE'11*
The Fifth International Conference on Emerging Security Information, Systems and Technologies.
Côte d'Azur, France, August 21–27, 2011.
Luca Viganò (UNIVR) PC member.

76. *FAST 2010*
The 7th International Workshop on Formal Aspects of Security & Trust, co-located with the 8th IEEE International Conference on Software Engineering and Formal Methods (SEFM2010).
CNR, Pisa, Italy, September 16–17, 2010.
Luca Viganò (UNIVR) PC member.

77. *LIS 2010*
Logics in Security Workshop, co-located with ESSLI2010.
Copenhagen, Denkmark, August 9–13, 2010.
Luca Viganò (UNIVR) PC member.

78. *SECURWARE'10*
The Fourth International Conference on Emerging Security Information, Systems and Technologies, Venice, Italy, July 18–25, 2010.
Luca Viganò (UNIVR) PC member.

79. *FCS-PrivMod 2010*
Workshop on Foundations of Security and Privacy, affiliated with FLoC 2010.
Edinburgh, UK, July 14–15, 2010.
Luca Viganò (UNIVR) PC member.

80. *SecArt'10*
Second Workshop on Intelligent Security (Security and Artificial Intelligence).
Atlanta, Georgia, USA, July 11, 2010.
Luca Viganò (UNIVR) PC member.

81. *PSPL 2010*
Proof Systems for Program Logics Workshop, affiliated with FLoC 2010.

Edinburgh, UK, July 14–15, 2010.
Luca Viganò (UNIVR) PC member.

82. MOVEP'10
The 9th School on MOdelling and VErifying parallel Processes.
Aachen, Germany, June 28 – July 2, 2010.
Luca Viganò (UNIVR) PC member.

83. *ASIACCS 2010*
5th ACM Symposium on Information, Computer and Communications Security.
Beijing, China, April 13–16, 2010.
David Basin (ETH) PC chair.
Michael Rusinowitch (INRIA) PC member.

84. *STM'10*
6th International Workshop on Security and Trust Management.
Athens, Greece, September 23–24, 2010.
Jorge Cuellar (Siemens), co-chair, Michael Rusinowitch (INRIA) PC member.

85. *SecCo'10*
8th International Workshop on Security Issues in Concurrency.
Paris, France. August 30 2010.
Michael Rusinowitch (INRIA) PC member.

86. *SecDay2010*
2010 Grande Région Security and Reliability Day.
Saarbrücken, Germany. March 18, 2010.
Michael Rusinowitch (INRIA) PC member.

87. *CRiSIS 2010*
5th International Conference on Risks and Security of Internet and Systems.
Montreal, Canada, Hotel Holiday Inn Midtown, October 11-13, 2010.
Marius Minea (IEAT), PC co-chair
Luca Viganò (UNIVR), Cas Cremers (ETH Zurich), Michael Rusinowitch (INRIA), Philippe Balbiani (IRIT), Bogdan Groza (IEAT) and Jorge Cuellar (Siemens) PC members.

88. *ASE 2010*
25th IEEE/ACM International Conference on Automated Software Engineering (ASE2010).

Antwerp, Belgium, September, 20-24, 2010.
Alessandro Armando (UNIGE), PC Member

89. *IJCAR 2010*
5th International Joint Conference on Automated Reasoning (IJCAR 2010).
Edinburgh, July 16-19, 2010.
Alessandro Armando (UNIGE), PC Member

90. *AISC 2010*
10th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2010).
Paris, France, July 5-6, 2010.
Alessandro Armando (UNIGE), PC Member

91. *SAC SEC 2010*
Security Track at the ACM Symposium on Applied Computing.
Lausanne, Switzerland, March 22-26, 2010.
Luca Compagna and Alessandro Sorniotti (SAP) co-chairs.

92. *PhD defense*
PhD defense: Azzedine Benameur, Web Service Security: From Business Process to Traces
Universite Claude Bernard Lyon 1, Ecole doctorale informatique et mathÃĬmatiques, Lyon, France, Jan 19, 2010.
Luca Compagna (SAP), invited member of the Jury.

93. *STM 2011*
7th International Workshop on Security and Trust Management (STM'11).
Copenhagen, Denmark, June 27-28, 2011.
Alessandro Armando (UNIGE), PC Member

94. *CADE 2011*
23rd International Conference on Automated Deduction (CADE-23).
Wroclaw, Poland, July 31 - August 5, 2011.
Alessandro Armando (UNIGE), PC Member

95. *AsiaCCS 2011*
ACM Symposium on Information, Computer and Communications Security, 2011.
Hong Kong. March 22-24, 2011
David Basin (ETH), PC Member

96. *FM 2011*
Symposium on Formal Methods, 2011.
Lero, Limerick, Ireland. June 20 - 24, 2011
David Basin (ETH), PC Member

97. *FOSSACS 2011*
Conference on Foundations of Software Science and Computation Structures, 2011.
Saarbrucken, Germany, from March 26 to April 3, 2011
David Basin (ETH), PC Member

3.4 AVANTSSAR publications, drafts, PhD theses, deliverables, video

The AVANTSSAR Consortium produced 95 papers published or currently in print about the project's foreground. 7 more papers are currently submitted and further ones are in preparation. 4 PhD theses have been completed in the course of the project and several more are in preparation. We also list the 25 project deliverables, as well as the video "Vulnerability in the SAML-based Single Sign On for Google Apps", which is available on youtube and on the project's website. Figure 1 shows a screenshot of the video.

3.4.1 AVANTSSAR publications

[1] Humberto Abdelnur, Tigran Avanesov, Michaël Rusinowitch, and Radu State. Abusing SIP Authentication. In Massimiliano Rak, Ajith Abraham, and Valentina Casola, editors, *Proceedings of the Fourth International Symposium on Information Assurance and Security (ISIAS'08)*, pages 237–242. IEEE Computer Society Press, 2008.

[2] Humberto Abdelnur, Tigran Avanesov, Michael Rusinowitch, and Radu State. Abusing SIP authentication. *Journal of Information Assurance and Security*, 4(4):311–318, 2009.

[3] Zeeshan Ahmed, Abdessamad Imine, and Michael Rusinowitch. Safe and Efficient Strategies for Updating Firewall Policies. In Sokratis K. Katsikas, Javier Lopez, and Miguel Soriano, editors, *7th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2010)*, volume 6264 of *Lecture Notes of Computer Science*, pages 45–57, Bilbao, Spain, 08 2010. Springer.

[4] Francesco Alberti, Alessandro Armando, and Silvio Ranise. Efficient Symbolic Automated Analysis of Administrative Role Based Access Control Policies. In *Proceedings of the 6th ACM Symposium on Information, Computer, and Communications Security (ASIACCS), Hong Kong, March 22-24, 2011*. ACM SIG, to appear.

[5] Siva Anantharaman, Hai Lin, Christopher Lynch, Paliath Narendran, and Michaël Rusinowitch. Unification modulo homomorphic encryption. In *Frontiers of Combining Systems, 7th International Symposium, FroCoS 2009, Trento, Italy, September 16-18, 2009. Proceedings*, volume 5749 of *Lecture Notes in Computer Science*. Springer, 2009.

[6] Siva Anantharaman, Hai Lin, Christopher Lynch, Paliath Narendran, and Michael Rusinowitch. Cap unification: Application to protocol security modulo homomorphic encryption. In *5th ACM Symposium on Information, Computer and Communications Security - ASIACCS 2010*, Beijing, China, April 2010. ACM.

[7] Siva Anantharaman, Hai Lin, Christopher Lynch, Paliath Narendran, and Michael Rusinowitch. Unification modulo Homomorphic Encryption. *Journal of Automated Reasoning*, to appear.

[8] Alessandro Armando, Roberto Carbone, and Luca Compagna. LTL Model Checking for Security Protocols. *Journal of Applied Non-Classical Logics, special issue on "Logic and Information Security"*, 2009.

[9] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, and Llanos Tobarra Abad. Formal analysis of saml 2.0 web browser single sign-on: Breaking the saml-based single sign-on for google apps. In Vitaly Shmatikov, editor, *Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008)*, pages 1–10. ACM Press, 2008.

[10] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuéllar, Giancarlo Pellegrino, and Alessandro Sorniotti. From Multiple Credentials to Browser-based Single Sign-On: Are We More Secure? In *Proceedings of IFIP SEC 2011*, to appear.

[11] Alessandro Armando, Roberto Carbone, Luca Compagna, Keqin Li, and Giancarlo Pellegrino. Model-Checking Driven Security Testing of Web-Based Applications. In *Proceedings of the 2010 Third International Conference on Software Testing, Verification, and Validation Workshops*, ICSTW'10, pages 361–370. IEEE Computer Society, 2010.

[12] Alessandro Armando, Luca Compagna, Roberto Carbone, and Giancarlo Pellegrino. Automatic Security Analysis of SAML-based Single Sign-On Protocols. In Raj Sharman and Sanjukta Das Smith and Manish Gupta, editor, *Digital Identity and Access Management: Technologies and Frameworks*. IGI Global, 2010.

[13] Alessandro Armando, Enrico Giunchiglia, Marco Maratea, and Serena Elisa Ponta. An action-based approach to the formal specification and automated analysis of business processes under authorization constraints. *Journal of Computer and Systems Sciences: Special issue on Knowledge Representation and Reasoning*, to appear.

[14] Alessandro Armando, Enrico Giunchiglia, and Serena Elisa Ponta. Formal specification and automatic analysis of business processes under authorization constraints: An action-based approach. In Guenther Pernul, Simone Fischer-Huebner, and Costas Lambrinoudakis, editors, *TrustBus'09: Proceedings of the 6th International Conference on Trust, Privacy and Security in Digital Business*, pages 63–72, Berlin, Heidelberg, 2009. Springer-Verlag.

[15] Alessandro Armando and Serena Elisa Ponta. Model checking of security-sensitive business processes. In Pierpaolo Degano and Joshua Guttman, editors, *Formal Aspects in Security and Trust: 6th International Workshop, FAST 2009, Eindhoven, The Netherlands, November 5-6, 2009, Revised Selected Papers*, volume 5983 of *Lecture Notes in Computer Science*, pages 66–80. Springer, 2010.

[16] Alessandro Armando and Silvio Ranise. Automated Symbolic Analysis of ARBAC Policies. In *Proceedings of the 6th International Workshop on Security and Trust Management STM'10 (co-located with EUROPKI'10, CRITIS'10, and ESORICS'10), Athens, September 23–24, 2010*, To appear in Lecture Notes in Computer Science.

[17] Charu Arora and Mathieu Turuani. Validating Integrity for the Ephemerizer's Protocol with CL-Atse. In *Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration*, pages 21–32. Springer, 2009.

[18] Wihem Arsac, Giampaolo Bella, Xavier Chantry, and Luca Compagna. Validating Security Protocols under the General Attacker. In Pierpaolo Degano and Luca Viganò, editors, *Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS 2009)*, ENTCS. Elsevier-Science, 2009.

[19] Wihem Arsac, Giampaolo Bella, Xavier Chantry, and Luca Compagna. Multi-attacker protocol validation. *Journal of Automated Reasoning*, pages 1–36, 2010. 10.1007/s10817-010-9185-y.

[20] Wihem Arsac, Giampaolo Bella, Xavier Chantry, and Luca Compagna. Attacking Each Other. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *17th International Workshop on Security Protocols (IWSP 2009), Cambridge, UK, April 1–3, 2009*, Lecture Notes in Computer Science. Springer, to appear.

[21] Wihem Arsac, Luca Compagna, Giancarlo Pellegrino, and Serena Elisa Ponta. Security Validation of Business Processes via Model-checking. In *International Symposium on Engineering Secure Software and Systems (ESSoS 2011)*. Lecture Notes in Computer Science, Springer-Verlag, to appear.

[22] Tigran Avanesov, Yannick Chevalier, Michael Rusinowitch, and Mathieu Turuani. Satisfiability of general intruder constraints with a set constructor. In José M. Fernandez, editor, *The Fifth International Conference on Risks and Security of Internet and Systems – CRiSIS 2010, Montreal, Canada, October 10–13, 2010*. IEEE XPlore, 2010.

[23] Bahareh Badban and Mohammad Torabi Dashti. Semi-linear Parikh images of regular expressions via reduction. In *Proceedings of the 35th international symposium on Mathematical Foundations of Computer Science (MFCS'10), Brno, Czech Republic, August 2010*, volume 6281 of *Lecture Notes in Computer Science*, pages 653–664. Springer, 2010.

[24] Philippe Balbiani, Fahima Cheikh, and Guillaume Feuillade. Considérations relatives à la décidabilité et à la complexité du problème de la composition de services. In *Proceedings of the Journées Francophones Modèles formels de l'Interaction (MFI 2007)*, pages 261–268, Paris, France, 2007. Annales du LAMSADE.

[25] Philippe Balbiani, Fahima Cheikh, and Guillaume Feuillade. Composition of interactive web services based on controller synthesis. In Jyothishman Pathak, Samik Basu, Marco Pistore, Prashant Doshi, and Rama Akkiraju, editors, *Proceedings of the 2008 IEEE Congress on Services - Part I*, SERVICES'08, pages 521–528, Washington, DC, USA, 2008. IEEE Computer Society.

[26] Philippe Balbiani, Fahima Cheikh, and Guillaume Feuillade. Composition of Web services: algorithms and complexity. Presented at the first Interaction and Concurrency Experience Workshop, sponsored by the ESF and co-located with ICALP'08, 2008.

[27] Philippe Balbiani, Fahima Cheikh, and Guillaume Feuillade. Résultats de complexité pour le problème de la composition d'agents. Cinquièmes Journées Francophones Modèles Formels de l'Interaction (MFI 09), to appear, 2009.

[28] Philippe Balbiani, Fahima Cheikh, and Guillaume Feuillade. Controller/orchestrator synthesis via filtration. *Electronic Notes in Theoretical Computer Science*, 262:33–48, 2010.

[29] Philippe Balbiani, Fahima Cheikh Alili, Pierre-Cyril Héam, and Olga Kouchnarenko. Composition of services with constraints. *Electronic Notes in Theoretical Computer Science*, 263:31–46, June 2010.

[30] Philippe Balbiani, Yannick Chevalier, and Marwa El Houri. A Logical Approach to Dynamic Role-Based Access Control. In *Artificial Intelligence: Methodology, Systems, and Applications, 13th International Conference, AIMSA 2008*, volume 5253 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 2008.

[31] Philippe Balbiani, Yannick Chevalier, and Marwa El Houri. Approche logique pour les contraintes de contrôle d'accès dans les services web. Presented at the Inforsid/SDEC 2009 workshop, 2009.

[32] Philippe Balbiani, Yannick Chevalier, and Marwa El Houri. A logical framework for reasoning about policies with trust negotiations and workflows in a distributed environment. In *The fourth International Conference on Risks and Security of Internet and Systems – CRiSIS 2009, Toulouse, France, October 19-22, 2009*. IEEE XPlore, 2009.

[33] Philippe Balbiani, Yannick Chevalier, and Marwa El Houri. An intruder model for trust negotiation. In José M. Fernandez, editor, *The Fifth International Conference on Risks and Security of Internet and Systems – CRiSIS 2010, Montreal, Canada, October 10–13, 2010*. IEEE XPlore, 2010.

[34] Michele Barletta, Alberto Calvi, Silvio Ranise, Luca Viganò, and Luca Zanetti. WSSMT: towards the automated analysis of Security-Sensitive Services and Applications. In *Proceedings of the SYNASC symposium, Timisoara, Romania, September 23-25, 2010*. IEEE Computer Society Press, to appear.

[35] Michele Barletta, Silvio Ranise, and Luca Viganò. Verifying the Interplay of Authorization Policies and Workflow in Service-Oriented Architectures. In *Proceedings of the 2009 International Symposium on Secure Computing (SecureCom 2009), Volume 3 of 2009 International Conference on Computational Science and Engineering (CSE 2009)*, pages 289–299. IEEE Computer Society Press, 2009. http://doi.ieeecomputersociety.org/10.1109/CSE.2009.172.

[36] Michele Barletta, Silvio Ranise, and Luca Viganò. A Declarative Two-Level Framework to Specify and Verify Workflow and Authorization

Policies in Service-Oriented Architectures. *Service-Oriented Computing and Applications*, 2010, DOI 10.1007/s11761-010-0073-4.

[37] David Basin, Carlos Caleiro, Jaime Ramos, and Luca Viganò. A Labeled Tableaux System for the Distributed Temporal Logic DTL. In Stéphane Demri and Christian S. Jensen, editors, *Proceedings of the 15th International Symposium on Temporal Representation and Reasoning (TIME 2008)*, pages 101–109. IEEE Computer Society Press, Los Alamitos, CA, 2008.

[38] David Basin and Cas Cremers. Degrees of security: Protocol guarantees in the face of compromising adversaries. In A. Dawar and H. Veith, editors, *CSL 2010: Proceedings of the 19th EACSL Annual Conference on Computer Science Logic*, volume 6247 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2010.

[39] David Basin and Cas Cremers. Modeling and analyzing security in the presence of compromising adversaries. In D. Gritzalis, B. Preneel, and M. Theoharidou, editors, *Computer Security - ESORICS 2010*, volume 6345 of *Lecture Notes in Computer Science*, pages 340–356. Springer, 2010.

[40] Giampaolo Bella and Luca Compagna. Special track on computer security 2009: editorial message. In Roger L. Wainwright and Hisham Haddad, editors, *SAC'08: Proceedings of the 2008 ACM Symposium on Applied Computing, Fortaleza, Ceara, Brazil, March 16-20, 2008*. ACM, 2008.

[41] Giampaolo Bella and Luca Compagna. Special track on computer security 2009: editorial message. In *SAC'09: Proceedings of the 2009 ACM symposium on Applied Computing, Honolulu, Hawaii, USA, March 08–12, 2008*. ACM, 2009.

[42] Giampaolo Bella, Francesco Librizzi, and Salvatore Riccobene. A privacy paradigm that tradeoffs anonymity and trust. In *Proceedings of the 2008 International Conference on Software, Telecommunications and Computer Networks - SoftCOM 2008*. IEEE Computer Society, 2008.

[43] Giampaolo Bella, Francesco Librizzi, and Salvatore Riccobene. Realistic threats to self-enforcing privacy. In *Proceedings of the 4th International Symposium on Information Assurance and Security*, pages 155–160. IEEE Computer Society, 2008.

[44] Davide Benetti, Massimo Merro, and Luca Viganò. Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA. In *Proceedings of eighth IEEE International Conference on Software Engineering and Formal Methods, SEFM 2010, Pisa, Italy, September 14–18, 2010*, pages 191–202. IEEE Computer Society Press, 2010.

[45] Daniele Berardi, Fahima Cheikh, Giuseppe DeGiacomo, and Fabio Patrizi. Automatic service composition via simulation. *International Journal of Foundations of Computer Science*, 19(2):429–451, 2008.

[46] Achim D. Brucker and Sebastian A. Mödersheim. Integrating automated and interactive protocol verification. In Pierpaolo Degano and Joshua Guttman, editors, *Formal Aspects in Security and Trust: 6th International Workshop, FAST 2009, Eindhoven, The Netherlands, November 5-6, 2009, Revised Selected Papers*, volume 5983 of *Lecture Notes in Computer Science*, pages 248–262. Springer, 2010.

[47] Elisa Burato, Matteo Cristani, and Luca Viganò. A Deduction System for Meaning Negotiation. In *Postproceedings of the 8th International Workshop on Declarative Agent Languages and Technologies (DALT 2010), held as part of the workshop programme of the 10th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010), Toronto, Canada, May 2010*. Springer, to appear.

[48] Alberto Calvi, Silvio Ranise, and Luca Viganò. Automated Validation of Security-sensitive Web Services specified in BPEL and RBAC. In *Proceedings of WoSS'10, the 1st Workshop on Software Services: Frameworks and Platforms, organized as satellite workshop of SYNASC symposium, Timisoara, Romania, September 23-25, 2010*. IEEE Computer Society Press, to appear.

[49] Jan Camenisch, Sebastian Mödersheim, Gregory Neven, Franz-Stefan Preiss, and Dieter Sommer. A card requirements language enabling privacy-preserving access control. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*. ACM, 2010.

[50] Jan Camenisch, Sebastian Alexander Mödersheim, and Dieter Sommer. A formal model of Identity Mixer. In *Proceedings of the 15th International Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, pages 198–214. Springer, 2010.

[51] Roberto Carbone. LTL Model-Checking for Security Protocols. *AI Commun.*, to appear.

[52] Jan Cederquist and Mohammad Torabi Dashti. Complexity of Fairness Constraints for the Dolev-Yao Attacker Model. *Proceedings of ACM SAC 2011, 26th Symposium On Applied Computing, Taichung, Taiwan, March 21–24, 2011*, to appear.

[53] Yannick Chevalier. Finitary deduction systems. Presented at the 2010 Security and Rewriting (Secret) workshop, 2010.

[54] Yannick Chevalier and Mounira Kourjieh. New decidability result for ground entailment problems and application to security protocols. In Dov M. Gabbay and Leendert van der Torre, editors, *Proceedings of the workshop on Logics in Security, organised as part of the European Summer School on Logic, Language and Information (ESSLLI), Copenhagen, Denmark, August 2010*. 2010.

[55] Yannick Chevalier, Mohamed Anis Mekki, and Michaël Rusinowitch. Orchestration under security constraints. Presented at the *Formal Aspects of Security and Trust*, FAST'09 workshop, 2009.

[56] Yannick Chevalier, Mohammed Anis Mekki, and Michael Rusinowitch. Automatic Composition of Services with Security Policies. In *Web Service Composition and Adaptation Workshop (held in conjunction with SCC/SERVICES-2008)*, pages 529–537. IEEE Computer Society Press, 2008.

[57] Yannick Chevalier and Michael Rusinowitch. Compiling and securing cryptographic protocols. *Information Processing Letters*, 110(3):116–122, 2010.

[58] Yannick Chevalier and Michael Rusinowitch. Decidability of Equivalence of Symbolic Derivations. *Journal of Automated Reasoning*, 2010. 10.1007/s10817-010-9199-5.

[59] Yannick Chevalier and Michael Rusinowitch. Symbolic protocol analysis in the union of disjoint intruder theories: Combining decision procedures. *Theoretical Computer Science*, 411(10):1261–1282, 2010.

[60] Najah Chridi, Mathieu Turuani, and Michael Rusinowitch. Towards a Constrained-based Verification of Parameterized Cryptographic Protocols. In Michael Hanus, editor, *Logic-Based Program Synthesis and Transformation, 18th International Symposium, LOPSTR 2008, Valencia, Spain, July 17-18, 2008, Revised Selected Papers*, volume 5438 of *Lecture Notes in Computer Science*. Springer, 2008.

[61] Najah Chridi, Mathieu Turuani, and Mohammad Rusinowitch. Decidable analysis for a class of cryptographic group protocols with unbounded lists. In *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)*, pages 277–289. IEEE Computer Society, 2009.

[62] Luca Compagna, Ulrich Flegel, and Volkmar Lotz. Towards Validating Security Protocol Deployment in the Wild. In *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International, Seattle, WA, USA, July 20–24, 2009.* IEEE Computer Society Press, 2009.

[63] Matteo Cristani, Erisa Karafili, and Luca Viganò. Blocking underhand attacks by hidden coalitions. In *Proceedings of ICAART 2011: 3rd International Conference on Agents and Artificial Intelligence (ICAART), Rome, Italy, January 28–30, 2011.* SciTePress, to appear.

[64] Wan Fokkink, Mohammad Torabi Dashti, and Anton Wijs. Partial order reduction for branching security protocols. In *Application of Concurrency to System Design (ACSD), 2010 10th International Conference on, Braga, Portugal, June 21–25, 2010*, pages 191–200. IEEE Computer Society, 2010.

[65] Silvio Ghilardi, Enrica Nicolini, Silvio Ranise, and Daniele Zucchelli. Towards smt model checking of array-based systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Proceedings of the 6th International Workshop on Satisfiability Modulo Theories (SMT'08), in Proceedings of the 4th international joint conference on Automated Reasoning*, pages 67–82. Springer, 2008.

[66] Silvio Ghilardi, Silvio Ranise, and Thomas Valsecchi. Light-weight smt-based model checking. *Electronic Notes in Theoretical Computer Science*, 250:85–102, September 2009.

[67] Bogdan Groza and Marius Minea. A calculus to detect guessing attacks. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Ardagna, editors, *Information Security, Proceedings of the* 12^{th} *International Conference on*, volume 5735 of *Lecture Notes in Computer Science*, pages 59–67. Springer, 2009.

[68] Bogdan Groza and Marius Minea. A formal approach for automated reasoning about off-line and undetectable on-line guessing (short paper). In R. Sion, editor, *Financial Cryptography and Data Security, Proceedings*

of the 14^{th} *International Conference on*, volume 6052 of *Lecture Notes in Computer Science*, pages 391–399. Springer, 2010.

[69] Bogdan Groza and Marius Minea. Formal modelling and automatic detection of resource exhaustion attacks. In *Proceedings of the* 6^{th} *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, to appear.

[70] Peter Hartmann, Monika Maidl, David von Oheimb, and Richard Robinson. A case study in decentralized, dynamic, policy-based, authorization and trust management – automated software distribution for airplanes. In Jorge Cuellar and Javier Lopez, editors, *Proceedings of the 6th International Workshop on Security and Trust Management STM'10 (co-located with EUROPKI'10, CRITIS'10, and ESORICS'10), Athens, September 23–24, 2010*. Springer, to appear.

[71] Casandra Holotescu. Controlling the unknown. In *Preproceedings of the First International Conference on Formal Verification of Object-Oriented Software, FoVeOOSS 2010, Paris, France, June 28–30.*, 2010.

[72] Casandra Holotescu. Error-avoiding adaptors for black-box software components. In 25^{th} *IEEE/ACM International Conference on Automated Software Engineering, Doctoral Symposium, Antwerp, Belgium, September 21, 2010*, pages 487–492, 2010.

[73] Casandra Holotescu. Black-box composition: a dynamic approach. In 9^{th} *International Workshop on Specification and Verification of Component-Based Systems SAVCBS'10, Workshop at FSE-18, Santa-Fe, New Mexico, USA, November 12, 2010*, to appear.

[74] Abdessamad Imine, Asma Cherif, and Michael Rusinowitch. A Flexible Access Control Model for Distributed Collaborative Editors. In *Secure Data Management, 6th VLDB Workshop, SDM 2009*, volume 5776 of *Lecture Notes in Computer Science*, pages 89–106, Lyon, France, 2009. Springer.

[75] Florent Jacquemard and Michael Rusinowitch. Closure of Hedge-Automata Languages by Hedge Rewriting. In A. Voronkov, editor, *19th International Conference on Rewriting Techniques and Applications - RTA 2008*, volume 5117 of *Lecture Notes in Computer Science*, pages 157–171. Springer, 2008.

[76] Florent Jacquemard and Michael Rusinowitch. Rewrite-based verification of XML updates. In Temur Kutsia, Wolfgang Schreiner, and

Maribel Fernández, editors, *12th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming - PPDP'10*, pages 119–130, Hagenberg, Austria, July 2010. ACM.

[77] Francis Klay and Laurent Vigneron. Automatic Methods for Analyzing Non-Repudiation Protocols with an Active Intruder. In P. Degano, J. Guttman, and F. Martinelli, editors, *5th International Workshop on Formal Aspects in Security and Trust (FAST)*, volume 5491 of *Lecture Notes in Computer Science*, pages 165–180, Malaga, Spain, 2008. Springer.

[78] Keqin Li. Towards security vulnerability detection by source code model checking. In *ICSTW'10: Software Testing, Verification, and Validation Workshops (ICSTW), 2010 Third International Conference on, Paris, France, April 6–10, 2010*, pages 381–387. IEEE Computer Society, 2010.

[79] Jing Liu and Laurent Vigneron. Design and Verification of a Non-Repudiation Protocol Based on Receiver-Side Smart Card. *IET Information Security*, 4(1):15–29, March 2010.

[80] Monika Maidl, David von Oheimb, Peter Hartmann, and Richard Robinson. Formal security analysis of electronic software distribution systems. In Michael Harrison and Mark-Alexander Sujan, editors, *Proceedings of the 27th International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, volume 5219 of *Lecture Notes in Computer Science*, pages 415–428. Springer, 2008.

[81] Andrea Masini, Luca Viganò, and Marco Volpe. A Labeled Natural Deduction System for a Fragment of CTL^*. In Sergei Artemov and Anil Nerode, editors, *Proceedings of the 2009 International Symposium on Logical Foundations of Computer Science (LFCS'09)*, volume 5407 of *Lecture Notes in Computer Science*, pages 338–353. Springer, Berlin, Heidelberg, 2009.

[82] Andrea Masini, Luca Viganò, and Marco Volpe. Labeled Natural Deduction for a Bundled Branching Temporal Logic. *Journal of Logic and Computation*, 2010, 10.1093/logcom/exq028.

[83] Sjouke Mauw, Sasa Radomirović, and Mohammad Torabi Dashti. Minimal message complexity of asynchronous multi-party contract signing. In *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)*, pages 13–25. IEEE Computer Society, 2009.

[84] Sebastian Mödersheim. Algebraic Properties in Alice and Bob Notation. In *Availability, Reliability and Security, 2009. ARES '09. International Conference on, Fukuoka, Japan, March 16–19, 2009*. IEEE Computer Society Press, 2009.

[85] Sebastian Mödersheim and Luca Viganò. Secure Pseudonymous Channels. In Michael Backes and Peng Ning, editors, *Computer Security âĂŞ ESORICS 2009 (Proceedings)*, volume 5789 of *Lecture Notes in Computer Science*, pages 337–354. Springer, 2009.

[86] Sebastian Mödersheim and Luca Viganò. The Open-Source Fixed-Point Model Checker for Symbolic Analysis of Security Protocols. In Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, editors, *FOSAD 2008/2009*, Lecture Notes in Computer Science 5705, pages 166–194. Springer-Verlag, 2009.

[87] Sebastian Mödersheim, Luca Viganò, and David Basin. Constraint Differentiation: Search-Space Reduction for the Constraint-Based Analysis of Security Protocols. *Journal of Computer Security (JCS)*, 18(4):575–618, 2010.

[88] Sebastian Alexander Mödersheim. Abstraction by Set-Membership : Verifying Security Protocols and Web Services with Databases. In *Proceedings of the 17th ACM conference on Computer and communications security, Chicago, Illinois, USA*, CCS '10, pages 351–360. ACM, 2010.

[89] Simona Orzan and Mohammad Torabi Dashti. Fair exchange is incomparable to consensus. In John S. Fitzgerald, Anne Elisabeth Haxthausen, and Hüsnü Yenigün, editors, *Theoretical Aspects of Computing - ICTAC 2008, Proceedings of the 5th International Colloquium on Theoretical Aspects of Computing*, volume 5160 of *Lecture Notes in Computer Science*, pages 349–363. Springer, 2008.

[90] Silvio Ranise. Towards Verification of Security-Aware E-services. In Nicolas Peltier and Viorica Sofronie-Stokkermans, editors, *First-order Theorem Proving, FTP 2009: International Workshop on First-Order Theorem Proving proceedings*, University Oslo/Departmant of Informatics: Research Report 386. University of Oslo/Department of Informatics, 2009.

[91] Carsten Rudolph, Luca Compagna, Roberto Carbone, Antonio Muñoz, and Juergen Repp. Verification of S&D Solutions for Network Communications and Devices. In George Spanoudakis, Antonio Maña Gomez,

and Spyros Kokolakis, editors, *Security and Dependability for Ambient Intelligence*, volume 45 of *Advances in Information Security*, pages 143–164. Springer, 2009.

[92] Mohammad Torabi Dashti. Efficiency of optimistic fair exchange using trusted devices. *ACM Transactions on Autonomous and Adaptive Systems*, to appear.

[93] Mohammad Torabi Dashti. Optimistic fair exchange using trusted devices. In Guerraoui R. and F. Petit, editors, *Proceedings of the 11th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'09)*, volume 5873 of *Lecture Notes in Computer Science*, pages 711–725. Springer, 2009.

[94] Mohammad Torabi Dashti and Sjouke Mauw. *Handbook of Financial Cryptography and Security (G. Rosenberg, ed.)*, chapter Fair Exchange, pages 109–132. Chapmand and Hall/CRC, 2010.

[95] David von Oheimb, Monika Maidl, and Richard Robinson. Security architecture and formal analysis of an airplane software distribution system. In *26th Congress of the International Council of the Aeronautical Sciences (ICAS)*, pages 1–12. Proceedings on CD-ROM available from secr.exec@icas.org, 2008. http://ddvo.net/papers/ICAS08.html.

3.4.2 AVANTSSAR drafts

[BCRV11] David Basin, Carlos Caleiro, Jaime Ramos, and Luca Viganò. Distributed Temporal Logic for the Analysis of Security Protocol Models, 2010. Submitted.

[BCV11] Elisa Burato, Matteo Cristani, and Luca Viganò. Meaning negotiation as inference, 2011. Available at http://arxiv.org/abs/1101.4356.

[CMMPTV10] Roberto Carbone, Marius Minea, Sebastian Alexander Mödersheim, Serena Elisa Ponta, Mathieu Turuani, and Luca Viganò. Towards Formal Validation of Trust and Security in the Internet of Services, 2010. Submitted.

[FTD10] Simone Frau and Mohammad Torabi Dashti. Integrated specification and verification of security protocols and policies. Technical Report 702, Dept. Computer Science, ETH Zurich, 2010.

[MV11] Sebastian Mödersheim and Luca Viganò. Channels as Assumption, Channels as Goals, 2010. Submitted.

[FPV10] Michele Peroli, M. Camilla Fiazza, and Luca Viganò. Attack Interference in Non-Collaborative Scenarios for Security Protocol Analysis, 2010. Submitted.

[RAN11] Silvio Ranise. On the Verification of Security-Aware Transition-based Services. Submitted, 2001.

3.4.3 AVANTSSAR PhD theses

[Carbone] Roberto Carbone. LTL Model-Checking for Security Protocols. Università degli Studi di Genova, Italy - 2009. http://ai-lab.it/carbone/Phd-thesis/

[Cheikh] Fahima Cheikh. *Composition de services: algorithmes et complexité*. PhD thesis, Université de Toulouse, Toulouse, France, 2009.

[Chridi] Najah Chridi. Contributions à la vérification automatique de protocoles de groupes Université Henri Poincaré - Nancy 1, September 2009. http://tel.archives-ouvertes.fr/tel-00417290/en/

[Kourjieh] Mounira Kourjieh. Logical analysis and verification of cryptographic protocols. PhD thesis, Université de Toulouse, France, 2009.

3.4.4 AVANTSSAR deliverables

[D1.1] AVANTSSAR. Deliverable 1.1: Project Presentation. Available at http://www.avantssar.eu, 2008.

[D1.2] AVANTSSAR. Deliverable 1.2: Basic Dissemination and Use Plan. Available at http://www.avantssar.eu, 2008.

[D1.3] AVANTSSAR. Deliverable 1.3: Progress/Assessment Report for Year 1. Available at http://www.avantssar.eu, 2009.

[D1.4] AVANTSSAR. Deliverable 1.4: Progress/Assessment Report for Year 2. Available at http://www.avantssar.eu, 2010.

[D1.5] AVANTSSAR. Deliverable 1.6: Final Project Report. This report. 2011.

[D1.6] AVANTSSAR. Deliverable 1.6: Final Dissemination and Use Plan. Available at http://www.avantssar.eu, 2010.

[D1.7] AVANTSSAR. Deliverable 1.7: Technology Implementation Plan. Available at http://www.avantssar.eu, 2010.

[D2.1] AVANTSSAR. Deliverable 2.1: Requirements for modelling and ASLan v.1. Available at http://www.avantssar.eu, 2008.

[D2.2] AVANTSSAR. Deliverable 2.2: ASLan v.2 with static service and policy composition. Available at http://www.avantssar.eu, 2009.

[D2.3] AVANTSSAR. Deliverable 2.3: ASLan final version with dynamic service and policy composition. Available at http://www.avantssar.eu, 2010.

[D2.3v2.0] AVANTSSAR. Deliverable 2.3 (v2.0): ASLan++ specification and tutorial. 2011.

[D3.1] AVANTSSAR. Decision Procedures for Service Synthesis and Satisfiability of ASLan Policies. Available at http://www.avantssar.eu, 2010.

[D3.2] AVANTSSAR. Deliverable 3.2: Model-Checking Techniques. Available at http://www.avantssar.eu, 2010.

[D3.3] AVANTSSAR. Deliverable 3.3: Attacker models. Available at http://www.avantssar.eu, 2008.

[D3.4] AVANTSSAR. Deliverable 3.4: Abstraction and Compositional Reasoning Techniques for Service Analysis. Available at http://www.avantssar.eu, 2010.

[D4.1] AVANTSSAR. Deliverable 4.1: AVANTSSAR Validation Platform v.1. Available at http://www.avantssar.eu, 2009.

[D4.2] AVANTSSAR. Deliverable 4.2: AVANTSSAR Validation Platform v.2. Available at http://www.avantssar.eu, 2010.

[D5.1] AVANTSSAR. Deliverable 5.1: Problem cases and their trust and security requirements. Available at http://www.avantssar.eu, 2008.

[D5.2] AVANTSSAR. Deliverable 5.2: Formalized problem cases. Available at http://www.avantssar.eu, 2010.

[D5.3] AVANTSSAR. Deliverable 5.3: AVANTSSAR Library of validated problem cases. Available at http://www.avantssar.eu, 2010.

[D5.4] AVANTSSAR. Deliverable 5.4: Assessment of the AVANTSSAR Validation Platform. Available at http://www.avantssar.eu, 2010.

[D6.1] AVANTSSAR. Deliverable 6.1: AVANTSSAR Website and Package. http://www.avantssar.eu, 2008.

[D6.2.1] AVANTSSAR. Deliverable 6.2.1: State-of-the-art on specification languages for service-oriented architectures. Available at http://www.avantssar.eu, 2008.

[D6.2.2] AVANTSSAR. Deliverable 6.2.2: Industrial language requirements. Available at http://www.avantssar.eu, 2008.

[D6.2.3] AVANTSSAR. Deliverable 6.2.3: Migration to industrial development environments: lessons learned and best practices. Available at http://www.avantssar.eu, 2010.

[D6.3] AVANTSSAR. Deliverable 6.3: Migration to standardisation bodies. Available at http://www.avantssar.eu, 2010.

3.4.5 AVANTSSAR video

[Video] AVANTSSAR. Vulnerability in the SAML-based Single Sign On for Google Apps. http://www.youtube.com/watch?v=O202FBcQNuk.

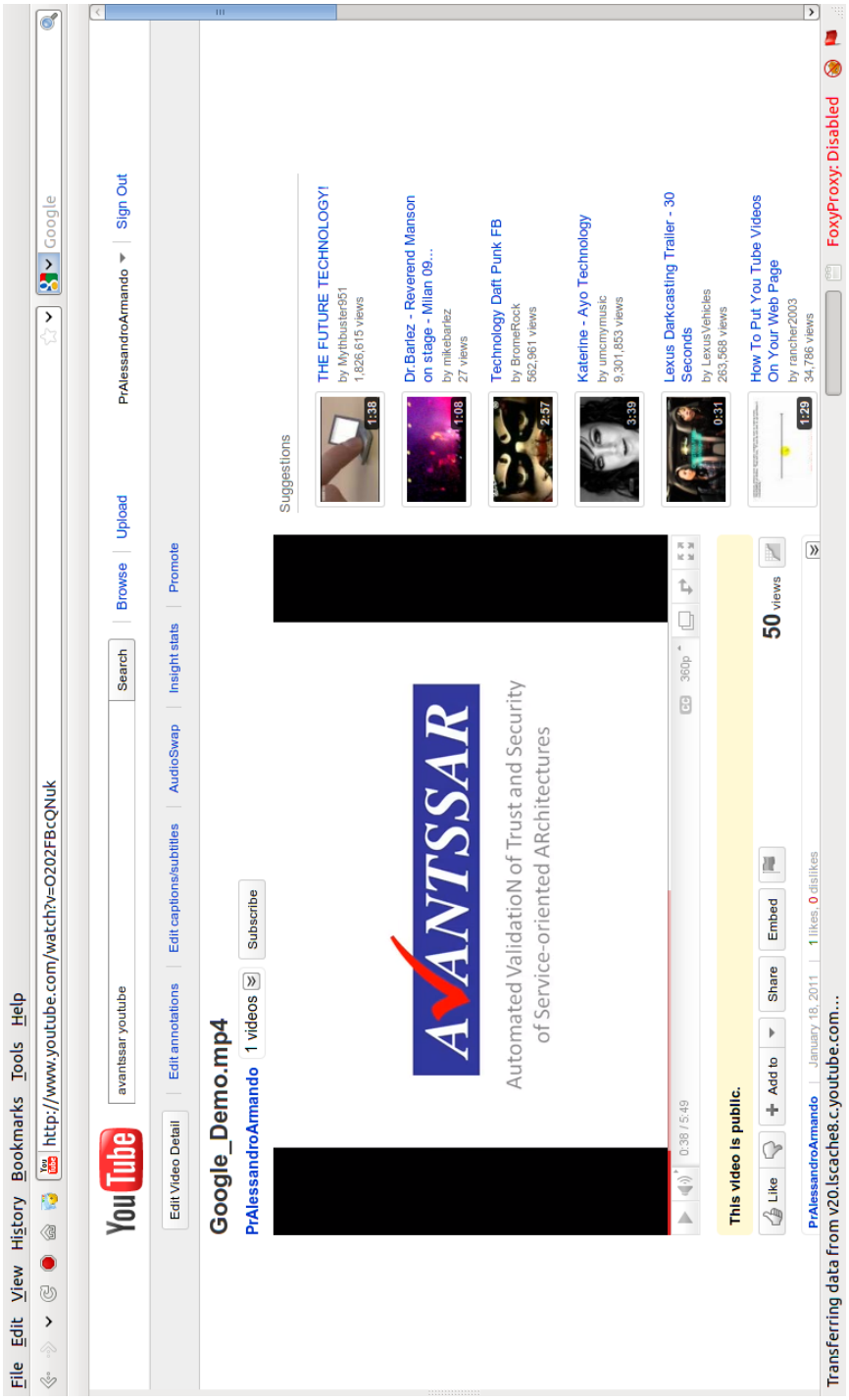

Figure 1: A screenshot of the demo-video about the serious vulnerability of the SAML-based Single Sign-On Service

3.5 Local dissemination by industrial project partners

3.5.1 IBM

We have used the AVANTSSAR Validation Platform for the analysis of the anonymous credential system Identity Mixer developed by IBM, which requires the full range of features that the AVANTSSAR technology has to offer. Related to Identity Mixer, IBM have devised the new specification language CARL for credential-based access control and provided, in relation to AVANTSSAR, a formal semantics for this language that is a pre-requisite for formal verification of CARL-based systems. We have begun designing a mapping from CARL specifications to the Identity Mixer technology; this gives a new form of compositional reasoning, using the Identity Mixer protocols as building blocks of privacy-friendly service-oriented architectures.

3.5.2 OpenTrust

The dissemination of the AVANTSSAR project results at OpenTrust has been carried out in two phases, targeting different audiences. The first phase consisted in internal company dissemination targeting developers and managers, so to inform the OpenTrust team members who did not participate in the project about the results: talks have been given by OpenTrust contributors to present the collection of languages, tools and validations that are output by the project. Feedback from the first phase has been used, in the second phase, to prepare dissemination for external audience: clients and partners. OpenTrust often relies on partners in order to integrate its solutions into client information systems. Consequently, partners, as well as clients, need a deep knowledge of the security aspects of the products. An initiation to AVANTSSAR technologies has been proposed to them as a complement to product training sessions.

3.5.3 SAP

SAP Research has been the main actor in the industry migration activity carried out in WP 6, which has shown how the AVANTSSAR technology can be integrated within industrial BPM systems and indeed used by business analysts via accessible user interfaces and apprehensive feedback. As a proof of concept, we have implemented our approach within an Eclipse plug-in that has been integrated within the SAP NetWeaver Business Process Management system (NW BPM). Moreover, AVANTSSAR results have been migrated within SAP NW SIM with the objective of exploiting the expertise of the SAP Research Security and Trust group to initiate a deep

formal analysis of the NW-NGSSO to formally establish its soundness i.e., to have formal evidence that the employed service providers and identity providers services fulfill the expected security desiderata in the considered SAP relevant scenarios. This has included the evaluation of those configurations of the highly configurable SAML SSO standard that are relevant for SAP as well as design and development decisions SAP could have taken to fulfill internal customer requirements.

3.5.4 SIEMENS

SIEMENS has been using the AVANTSSAR techniques and tools in their security analysis and consulting projects for customers, e.g. at Continental VDO, Boeing Phantom Works, and the Rhön-Klinikum AG. To migrate the project results to the SIEMENS business units, the AVANTSSAR team (all of them members of the central Corporate Technology) had meetings with the developers and application owners within the individual business units and wrote the ASLan++ specifications outside of the existing development process. The advantage of using directly ASLan++ is that it is readily readable by end users and can even be modified or extended by non-specialists. We did not try to embed AVANTSSAR within the industrial development environments, mostly because within SIEMENS there are too many different design frameworks, development programming languages, quality control tools, organizational and procedural constraints, time schedules, etc. Such a migration path to our development environments would have required coordination between the different developer groups, adoption of common design and development programming languages, common design environments, homogeneous quality control tools and procedural constraints, and so on.

3.6 Clustering and standardization

In addition to the external and local dissemination, the whole consortium has been involved in clustering and standardization activities. These activities are described in quite some detail in the deliverables [D1.7, D6.2.3, D6.3], so here we only briefly indicate some relevant projects and organizations (at international or national level) with which information exchange has been and will be beneficial.

3.6.1 European and international projects and working groups

Members of the AVANTSSAR consortium participate in (or are in close contact with the initiators and members of) several related European and international projects and working groups, including:

- SPaCIoS: Secure Provision and Consumption in the Internet of Services, http://www.spacios.eu. SPaCIoS is a 3 year FP7 STREP project that started on October 2010, with the involvement of several partners of AVANTSSAR: UNIVR (again as coordinator), ETH Zurich, UGDIST, SAP, SIEMENS. SPaCIoS will exploit all the results of AVANTSSAR, scaling them up from design time to provision and consumption time. The effort here will be on extending the languages and techniques so as to allow for validation (and in particular, testing) at these later stages of the service development life-cycle, which is a considerably challenging task.

- ANIKETOS: Secure Development of Trustworthy Composable Services, http://www.aniketos.eu/project. ANIKETOS is a 3 year FP7 STREP project that started on July 2010, with the involvement of one partner of AVANTSSAR: SAP. The main objective of ANIKETOS is to provide service developers and providers with a platform for secure and trusted composite services. As the Future Internet will need to be more responsive to threats and changes in services, this platform will help maintain their trust level and secure behaviour in a dynamic environment. The platform will include technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composed services. AVANTSSAR results can be used in the context of ANIKETOS to formally validate security-relevant aspects of composed services.

- Assert4SOA: Advanced Security Service Certificate for SOA, http://www.assert4soa.eu. Assert4SOA is a 3 years FP7 project started

in October 2010 with the involvement of one partner of AVANTSSAR: SAP.

ASSERT4SOA infrastructure will (i) develop enhanced methods for the certification of complex and continuously evolving SOA-based software systems and services and make use of existing certification processes within the SOA context (where possible), (ii) develop mechanisms and tools for the assessment of SOA-based systems' and services' trustworthiness, both at design time and runtime, based on systems and service certification, (iii) integrate the methods, mechanisms and tools of (i) and (ii) into the SOA lifecycle. AVANTSSAR results can be used to validate composed services so to get an Assert4SOA certificate.

- PoSecCo: Policy and Security Configuration Management, FP7 IP project started in October 2010 with the involvement of two partners of AVANTSSAR: SAP and IBM, http://www.posecco.eu.

  PoSecCo aims to establish and maintain a consistent, transparent, sustainable and traceable link between high-level, business-driven security and compliance requirements on one side and low-level technical configuration settings of individual services on the other side. AVANTSSAR results could be used to evaluate policy consistency.

- COST Action IC0901: Rich-Model Toolkit – An Infrastructure for Reliable Computer Systems (Nov. 2009 – Oct. 2013). The action is relevant through its design of language with rich modeling features, and through its work on decision procedures, including SAT checking. From the AVANTSSAR project, Marius Minea and Alessandro Armando are representing Romania and Italy (resp.) in the Management Committee.

- DEPLOY: Industrial deployment of system engineering methods providing high dependability and productivity. FP7 project, Feb 2008 – Jan 2012, http://www.deploy-project.eu/index.html.

  The Deploy project concerns developing critical systems by refinement using the Event-B formalism. The main focus is on embedded systems, but the project will also explore security aspects of such systems. ETH Zurich is the focal point for the security activities and can serve as a hub for collaboration here. Point of contact for Deploy: David Basin.

- IFIP WG 1.7 *Theoretical Foundations of Security Analysis and Design*, http://www.dsi.unive.it/IFIPWG1_7/. Luca Viganò of UNIVR is a member of the working group.

- MASTER: Managing Assurance, Security and Trust for sERvices. FP7 project, Feb 2008 – Jan 2011, http://www.master-fp7.eu/index.php. ETH Zurich and SAP are collaborating in this project, which is about the management of security and trust for services. Since MASTER focuses on the runtime monitoring of services with respect to given policies, and also takes into account web services and applications, the work carried out in AVANTSSAR nicely complements these activities.

- PrimeLife: Bringing sustainable privacy and identity management to future networks and services. FP7 project, Mar 2008 – Feb 2011, http://www.primelife.eu.

  The PrimeLife project is related in several regards. First of all, Prime Life is concerned with improving privacy-friendly technologies such as IBM's Identity Mixer, which is one of the major case studies in AVANTSSAR. We already have a close collaboration between these two projects at the IBM site. In particular, we have been discussing our formalization of the Identity Mixer directly with its developers. Moreover, PrimeLife is also related to questions of access control policies and their composition. The privacy-friendly credential-based access control language CARL has been developed in collaboration of AVANTSSAR and PrimeLife at IBM.

- SPOCS: Simple Procedures Online for Crossborder Services. Siemens participates in the FP7 e-government project SPOCS, CIP-ICT PSP-2008-2 no238935, http://www.eu-spocs.eu/, started in June 2009. Among others, SPOCS specifies the security architecture for prototypical service portal implementations related to the EU Services Directive. SIEMENS is going to formalize and verify the security architecture using the AVANTSSAR toolset, whereby valuable feedback is anticipated in both directions between the projects.

- mOSAIC: Open-Source API and Platform for Multiple Clouds is an FP7 project (Sept. 2010 - Feb. 2013) scientifically coordinated by IEAT. The project will create, promote and exploit an open Cloud application programming interface and an open-source development platform. mOSAIC services could be validated using techniques derived from the AVANTSSAR project; this is part of a submitted proposal to associate IeAT with the ongoing FP7 SPaCIoS project.

- SPRERS (http://www.sprers.eu), an FP7 support action (Jan. 2010 - Dec. 2011) to strengthen the participation of research teams from new member states in European R&D on software services, including

the IEAT team as participant. The AVANTSSAR project meeting in Timişoara was co-located with a SPRERS workshop, including the presentation of an AVANTSSAR tutorial and a research paper.

- NESSOS is a network of excellence that began in October 2010. It includes three partners of AVANTSSAR and focuses on a set of methodologies, processes and tools for engineering secure Future Internet software services. AVANTSSAR is mentioned in Workpackage "Security assurance for services" (lead by ETH Zurich) as a key enabling technology to be exploited within NESSOS. As a result, NESSOS can also be considered as part of the general exploitation of AVANTSSAR.

Some of the members of the AVANTSSAR team, including ETH Zurich, INRIA, SAP, SIEMENS, and UNIVR also participate, at different levels, in the activities of the European Research Consortium in Informatics and Mathematics (ERCIM), in particular, ERCIM's Working Group on Security and Trust Management, which aims at steering the research of ERCIM institutions on a series of activities (e.g., research projects, workshops, dissemination of knowledge) for fostering the European research and development on security, trust and privacy in ICT. These are among the main issues of current and future research efforts for "security in Europe" (cf., for example, http://www.cordis.lu/security). We thus expect that the results of AVANTSSAR will be beneficial for this ERCIM WG, which will in turn provide a major forum for the peer-evaluation and dissemination of our results.

France

- SAP: CESSA (Compositional Evolution of Secure Services using Aspects) is a ANR project (09-SEGI-002-01) that started in 2010 between École des Mines de Nantes, Eurecom, IS2T and SAP. CESSA will provide solutions for the evolution of secure SOAs by providing an aspect-oriented structuring and programming model that allows security functionalities to be modularized that cross administrative and technological domains. By means of security aspects and a new notion of aspect-aware service interfaces, CESSA will enable the synthesis of SOA-based applications that are correct by construction and will allow the formal analysis of security properties of SOAs.

- SAP: RescueIT project, http://soknos.domainfactory-kunde.de/index.php?id=480. SAP Research coordinates a joint German/French proposal in the context of the BMBF/ANR call Securing the Supply Chains / Concepts Systems and Tools for Global Security.

- INRIA: ACCESS is an INRIA ARC project that has started in 2010 between Lille, Saclay and Nancy. ACCESS is concerned with the security and access control for Web data exchange. It aims at defining automatic verification methods for checking properties of access control policies (ACP) for XML, like consistency and for the comparison of ACPs. Formal tools from tree automata theory will be applied for this purpose.

- UPS-IRIT: Philippe Balbiani is the leader of ARA SSIA COPS. Lilac is also part of the ROSACE (Robots et systèmes, auto-adaptatifs, communicants et embarqués) project, which aims at studying and developing means to design, specify, implement and deploy a set of mobile autonomous communicating and cooperating robots with well-established properties particularly in terms of safety, self-healability, ability to achieve a set of missions and self-adaptation in a dynamic environment. The project is focused on the associated software (models, algorithms and systems). We propose to address in a systematic and convergent approach the robotics software levels and the specific constraints imposed to the middleware level corresponding to the real-time embedded systems as well as network and inter-communication level management. ROSACE will bring together a strong research consortium composed of research teams from three laboratories (CERT-ONERA, IRIT and LAAS-CNRS) for making real progress in this area: an active and central object - namely a fleet of cooperative robots - is critical for keeping the difficult and ambitious scientific and technical work well grounded in relevant realities and well focused on actual needs.

Germany SIEMENS participates to:

- BITKOM AK (working group) SOA Technologies, http://www.bitkom.org/de/themen_gremien/18151.aspx

- CAST workshops on SOA Security, http://www.cast-forum.de/workshops/infos/103

- TeleTrusT project group SOA Security, http://teletrust.de

- RescueIT project, http://soknos.domainfactory-kunde.de/index.php?id=480: SAP Research coordinates a joint German/French proposal in the context of the BMBF/ANR call Securing the Supply Chains / Concepts Systems and Tools for Global Security.

Italy

- UNIVR participated to the PRIN'07 project "SOFT — Tecniche formali orientate alla sicurezza", Sep 2008 – Aug 2010.
- UGDIST coordinated the PRIN'07 project "Integrating automated reasoning in model checking: towards push-button formal verification of large-scale and infinite-state systems", Sep 2008 – Aug 2010.
- In April 2010, Alessandro Armando has created and is currently leading the Security & Trust Research Unit at the Center for Information Technologies (Fondazione Bruno Kessler), Trento, Italy.

Romania

- CONQUERS: Continuous Quality Evaluation and Restructuring of Software. Romanian national research grant, Oct 2007 – Sep 2010, http://loose.upt.ro/conquers. Relevant to AVANTSSAR is a task on extraction and composition of component and service interfaces.
- IEAT won a 20-month Romanian national grant (2009–2010) supplementing FP7 participation in AVANTSSAR. This grant allowed IEAT to provide additional person-months to the project and to finance part of the participation in AVANTSSAR project meetings and conferences.

Switzerland

- ETH Zurich has been involved in the project ComposeSec (funded by the Hasler Foundation). This 3-year project, which started in September 2007, aimed at analyzing complex protocol suites or services built by combining networked components. The goal of this project was to develop effective compositional methods, with accompanying tool support, to tackle this problem. This includes foundational work on bridging the gap between currently used security protocol models and high-level analysis models of composed services.

4 Description of the Use Plan (by result)

As the project reaches completion, all partners are confident in the results that they have produced and are therefore beginning to exploit the extensive potential value of these results. This section describes the project results that have potential for exploitation, including those beyond the use of AVANTSSAR as a whole as described above. Additional details about exploitation are given in [D1.7].

We do not believe that automatic tools for the security and trust validation of services will be attractive enough for a commercial market, for reasons of potential market volume and appropriate pricing. In order to best exploit the value of the research that has been produced, the results have been (see [D6.3]) and will be further submitted to industry standardisation bodies in an effort to establish AVANTSSAR as an industry standard for security and trust validation in SOA systems. Success in achieving status as de facto standard methodology and toolset could open up a market for the project partners to offer consulting services around this technology, making use of the unique expertise developed during the project.

The technology developed in this project will also be used as a basis for the FP7 project SPaCIoS (Secure Provision and Consumption in the Internet of Services, www.spacios.eu). The technology will also provide value in two other EU-funded research projects that started recently, DIAMONDS (www.fokus.fraunhofer.de/en/motion/projekte/laufende_projekte/DIAMONDS) and NESSOS.[1] As much of the AVANTSSAR results will be used as a basis for these new projects, they can be considered as part of our exploitation strategy. Such further commitment to research on this subject by many of the AVANTSSAR partners shows a strong confidence in the value of the work that has been carried out and the potential to deliver further valuable research in the future.

4.1 Exploitation approach

In order to exploit the results of the project, the primary approach is public dissemination of the research, targeting industry, academic institutions and

[1] NESSOS is a network of excellence that began in late 2010 (Network of Excellence on Engineering Secure Future Internet Software Services and Systems, www.nessos-project.eu). It includes three partners of AVANTSSAR and focuses on a set of methodologies, processes and tools for engineering secure Future Internet software services. AVANTSSAR is mentioned in Workpackage "Security assurance for services" (lead by ETH Zurich) as a key enabling technology to be exploited within NESSOS. As a result, NESSOS can also be considered as part of the general exploitation of AVANTSSAR.

standardisation bodies. As described above, to achieve this effectively a number of activities have been and will be carried out to generate awareness about the project within the target market. Delivering a strong and clear message to a wide audience with a clearly communicated value proposition is intended to help stimulate market adoption of the technology. This in turn could improve chances for moving towards adoption of a de facto industry standard for this technology in the future.

Effective communication regarding the technology is also intended to generate interest within industry and organizations, so that eventually they may employ the technology within their own SOA projects. If this occurs, there may be an opportunity for project partners to engage by providing a consulting service employing the AVANTSSAR Platform. This may occur as a research based activity, to further develop the principles of the technology through feedback from real world implementation, with no consultation fee arrangement, or as a formal consultation service with partners charging organizations for their time.

4.2 Expected Impact

The primary impact targets are industry, research institutions, and standardization bodies worldwide, working on the design of web services and SOAs, and focusing in particular on their trust and security aspects. Successful establishment of AVANTSSAR as an industry standard is likely to result in greater industry uptake, helping organizations to deliver more secure SOA solutions within and even across industry domains. It is expected that, through use of this technology, society as a whole will ultimately benefit from the results of the project in terms of increased reliability and acceptance of, and confidence in, SOAs across all industry domains.

4.3 The AVANTSSAR Platform

The main result of the project is the AVANTSSAR Validation Platform, shown in Figure 2. The platform takes as input a policy stating the functional and security requirements of a goal service and a description of the available services (including a specification of their security-relevant behavior, possibly also including the local policies they satisfy) and aims at proving that the service (possibly orchestrated from the available services) meets the security requirements stated in the policy.

The main components of the platform are the TS Orchestrator and the TS Validator (Orchestrator and Validator, for short):

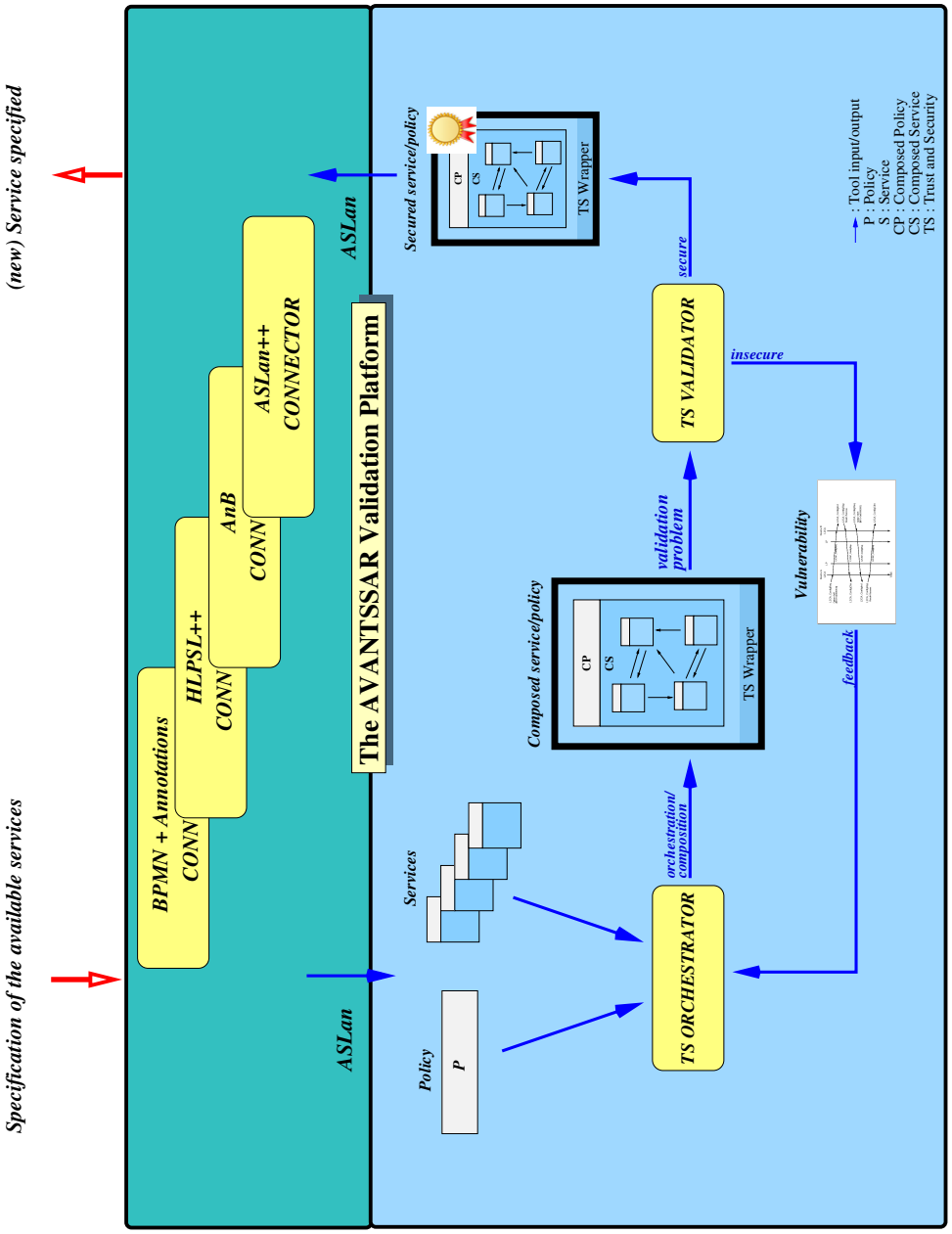

Figure 2: The AVANTSSAR Validation Platform

- The *Orchestrator* builds an orchestration (if any), i.e. a composition, of the available services in a way that is expected (but not yet guaranteed) to satisfy the input policy. In the case of dynamic composition of services, this orchestration is synthesized using *TS Wrappers* that add security functionality not provided by the initial set of services.

- The *Validator* automatically analyzes the validation problem resulting from the Orchestrator output. Failed validation means the existence of vulnerabilities that need to be fixed; otherwise, the composition of the services is guaranteed to be secure, i.e. to meet the input policy.

Whenever the Validator detects a vulnerability on the composed service, a feedback loop to the Orchestrator is initiated. When an orchestration of the available services is given in the problem specification, the AVANTSSAR Platform directly invokes the Validator.

The platform includes a *connectors layer*, i.e. a layer of software modules that carry out the translation from application-level specification languages (e.g. BPMN) into the ASLan language (and vice versa). ASLan, which was defined in Deliverable D2.1 ("Requirements for modelling and ASLan v.1" [D2.1]) and the updated Deliverable D2.3 ("ASLan final version with dynamic service and policy composition", updated [D2.3v2.0]), is the input and output format of the logical level of the platform.

An input specification consists of: the *available web services* (i.e. services that the orchestrator can compose to reach its goal), and the *policy* stating both the functional and the security goals of the desired service. The functional goals express functionalities that must be synthesized by composing the available services, while the security goals express the trust and security properties that must be satisfied by the synthesized service.

The output is a validated orchestration, i.e. a composed service that employs the available services and achieves both the functional and the security goals. In more detail:

- The Orchestrator looks for a combination of the available services meeting the functional goals. It may additionally receive as input a counterexample found by the validator, if any. The output of the Orchestrator is an ASLan specification of the goal service that is guaranteed to satisfy the functional goals.

- The Validator checks the security of the orchestration (i.e. the output of the Orchestrator) by checking if it satisfies the security goals. If a counterexample is found, it is returned to the Orchestrator; otherwise the orchestration produced by the Orchestrator is returned as output.

ASLan specifications are amenable to formal analysis, but high-level languages are better suited for developers. The specifications provided to the logical level of the platform (and resulting from the validation and synthesis activities) need to be translated from (and to) the modelling artifacts and languages used at the application level. The languages we consider are indicated in Figure 2: ASLan++ [D2.2], BPMN, possibly annotated, HLPSL++, and the novel language AnB, based on an extended Alice-and-Bob notation [84].

These transformations implemented in the connectors layer play a primary role in the Industry Migration workpackage WP 6. In particular, a security-annotated BPMN is used in the migration to the industrial development environments of SAP and OpenTrust for the specification of the Industrially-Suited Specification Language (ISSL) as described in Deliverable D6.2.2 ("Industrial language requirements" [D6.2.2]). Moreover, the ASLan specification can be obtained by translating a specification in ASLan++, as described in Deliverable 2.2 ("ASLan v.2 with static service and policy composition" [D2.2]). An automatic translator from ASLan++ to ASLan has been developed. Notice that other languages can be used in the AVANTSSAR Platform by defining their connectors to ASLan. In order to simplify the integration of new connectors with the AVANTSSAR Platform, we also provide two converters that generate the XML representation of ASLan and of the common output format of the validator back-ends.

The AVANTSSAR Validation Platform thus provides SOA designers with expressive formal languages for expressing their products and with powerful tools to verify them. Moreover, the AVANTSSAR library provides them with a good basis for developing new services by describing many examples and allowing the reuse of well-tested modules. This will pave the way to the migration of our technology into standardization organizations so that both the scientific and the industrial communities will readily benefit from the advances achieved by the project.

4.4 Specification Languages

In order to facilitate the penetration of formal validation techniques in the SOA industry, we have been promoting and will promote ASLan, ASLan++ and the other industrially suited specification languages of the platform as candidates for standardized formal notation for SOAs. Such precise notations allow for easy validation and reuse of modules and services by industry. This promotion has been and will be supported by tutorials given at conferences, industrial meetings, thematic schools, and presentations and courses at engineering schools.

4.5 Automated reasoning techniques

We have developed automated reasoning techniques supporting the automatic verification of ASLan specifications of SOAs. By automating the reasoning about security-relevant aspects of services and associated policies, these techniques serve as the basis for the automated validation technologies developed by the project. Moreover, several of the techniques are general enough to be applied also in other validation environments.

4.6 The AVANTSSAR Library of validated SOA problem cases

We have followed a proof of concept approach by providing a test suite of relevant SOA problem cases to evaluate the concepts, methodologies, techniques, and tools developed by the project. The formal modeling of the problem cases in the AVANTSSAR Library has allowed us to improve the specification languages and the AVANTSSAR Platform, in particular in terms of the efficiency needed for the validation of significantly complex models. We have applied the platform on the library. We have been able to formalize (in ASLan++, HLPSL++, annotated BPMN, and ASLan) 94 problem cases from 9 application scenarios, and the platform successfully analyses 74 problem cases. All of the success criteria set out in the Description of Work are thus fulfilled by the platform, exceeding by several times the required number of formalized and validated problem cases, which suggests that it will be possible to apply the platform also to other, more complex problem cases, possibly from industries other than those in the consortium. The library will be proposed to the scientific community as a suite of benchmark problems for automated analysis of trust and security aspects of SOAs that can be readily used to assess and compare the performance of rival validation approaches.

4.7 Dissemination and industry migration

Dissemination and migration of the project results into the scientific community, standardization organizations and industry have been carried out successfully. In addition to migration activities towards standardization organizations, we have succeeded in integrating the AVANTSSAR Validation Platform into real industrial environments (those of SAP, SIEMENS, IBM and OpenTrust) and successfully applied it on some industrial scenarios, so that we have been able also to collect the lessons learned and best practices.