AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D1.3: Periodic Progress Report N°: 3

Covering period 01.01.2005 — 30.06.2005

Abstract

This periodic progress report covers the last 6 months of the AVISPA project. It consists of an executive summary, of an overview of the work progress, of details about the project management, coordination, and cost breakdown, and of a description of information dissemination and exploitation of results.

Deliverable details

Deliverable version: *v1.1*
Date of delivery: *13.10.2005*
Classification: *public*
Person-months required: *1*
Due on: *30.06.2005*
Total pages: *55*

Project details

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

Information Society Technologies

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

[This page has been intentionally left blank.]

Contents

1 Executive Summary

AVISPA is a FET Project with the goal of developing a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. This technology aims at speeding up the development of the next generation of network protocols, improving their security, and therefore increasing the public acceptance of advanced, distributed IT applications based on them.

The partners of the project are:

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

The project scientific objectives and milestones for the reporting period are detailed in the Technical Annex, and can be summarised as follows:

WP4 – Scalability To provide support for compositional reasoning in order to exploit the modular structure of protocols. To improve the automated deduction techniques and tools previously developed by the partners and scale them up to large-scale, state-of-the-art security protocols such as those selected in WP6. To deliver the AVISPA Tool as a web-based version and as a downloadable version (available on the AVISPA Web-Site).

WP5 – Verification To investigate and integrate mechanisms capable of deriving positive statements about protocol security, i.e. verify that the protocols achieve their security objectives, even when considering an unbounded number of sessions.

WP7 – Tool Assessment To evaluate the technical achievements of the project with respect to measurable criteria. Classes of protocols, threat models, and security goals for which each automated deduction technique behaves optimally will be also identified.

WP8 – Dissemination To deliver the AVISPA Tool and disseminate the project results through appropriate channels and in appropriate forums.

All the expected results for the third reporting period have been achieved, all success criteria set out in the Technical Annex have been met, and all the planned deliverables have been produced.

Even though the main bulk of the activities of WP2, WP3, and WP6 has been completed by month 24 (as originally planned in the Technical Annex) we found it appropriate, and in some cases necessary, to continue some of the tasks associated with these workpackages:

WP2 – Protocol Specification Languages We have extended the definition of the High-Level Protocol Specification Language (HLPSL) and of the Intermediate Format (IF) so to allow for *(i)* protocol specifications with improved handling of sets (including the deletion of an element), *(ii)* representation of secrecy properties with respect to a set of agents, and *(iii)* more general security property specifications by means of LTL formulae. We have also carried out improvements to the syntax in order to support a more intuitive representation of assignment and freshness. Finally, we have upgraded the implementation of the translator from HLPSL to IF so to support these changes.

WP3 – Context & Properties Specification We have designed of a specification language based on temporal operators for the specification of complex security properties.

WP6 – Selection & Specification of Protocols We have further extended the AVISPA library with new security problems (i.e. protocols and the security properties they are designed to achieve) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation. In particular, we have been working on modelling five of the seven Main Protocols (see [33]). Note that this activity is considered very valuable by the designers (with whom we are in contact) as these protocols are still in the design (or definition) phase.

The results of the scientific workpackages consist of a series of deliverables, whose purposes and contents are detailed in the next sections. We here summarise the main achievements realised during the reporting period:

WP4&5 During the last six months of the project, we have focused on the completeness of protocol validation procedures and on protocol compositionality, obtaining a number of results on the composition of intruder theories, of different protocols, and of different communication channels. Moreover, we have further worked on infinite-state model-checking, by optimising the verification algorithm for time-sensitive security protocols we introduced in the second project year, and continuing the development and integration of heuristics, optimisations, and reduction and abstraction techniques, both general and specific to the individual back-ends. These techniques are implemented in the four back-ends of the AVISPA Tool:

OFMC, an on-the-fly model-checker developed and maintained by ETHZ,

CL-AtSe, a protocol analyser based on Constraint Logic developed and maintained by INRIA, and

SATMC, a SAT-based model-checker developed and maintained by UNIGE,

TA4SP, a tree automata based protocol analyser developed and maintained by the LIFC group affiliated with INRIA.

The resulting architecture of the AVISPA Tool v.3 is depicted in Figure 1.

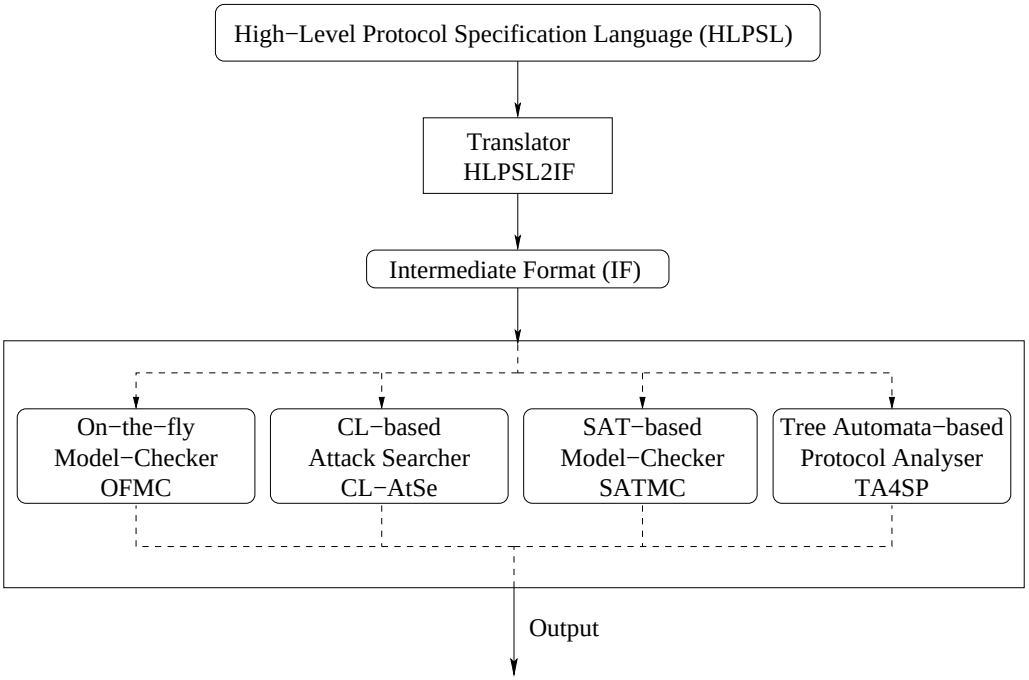

Figure 1: Architecture of the AVISPA Tool v.3

WP6&7 During the first year of the project we have identified and selected a large number of security protocols (along with the associated security properties) to be used as testbed for thoroughly assessing the AVISPA Tool. The resulting collection of candidate protocols and security problems was given in Deliverable 6.1 [33]. During the second year of the project we have formalised in HLPSL a large number of these problems and we have used them to assess the AVISPA Tool, thereby demonstrating proof-of-concept on a large collection of practically relevant, industrial protocols. During the final (half a) year of the project we have handled some further protocols and the problems associated with them, in particular five of the seven Main Protocols.

As described in [33], the following criteria, which refine the ones given in the Technical Annex, are used for the assessment of the AVISPA tool at month 30:

Coverage: at least 80 security problems from 20 groups of the AVISPA library should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 60) of these 80 problems, including at least one problem from each of the first seven groups given in [33], by either verifying that the protocol satisfies the desired security property (mainly for scenarios consisting of a bounded number of protocol sessions) or by finding a counterexample demonstrating that the property is violated.

Table 1: Results of the AVISPA Tool for the reporting period

Success criteria at month 30	**Objectives**	**Results**
Coverage	80 problems from 20 groups	215 problems from 22 groups
Effectiveness	60 problems	215 problems
Performance	$<$ 1 hour per problem	$<$ 24 minutes per problem (all 215 problems in 87 minutes)

Performance: the verification of each problem should be carried out in less than 1 hour of CPU time.

The results demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 215 problems from 22 groups, and the tool successfully analyses 215 problems in less than 24 minutes of CPU time per problem (globally, the entire library of 215 problems requires 87 minutes of CPU time to be analysed). All the above requirements (namely coverage, effectiveness, and performance) are therefore more than fulfilled.

The activities for the Project Management workpackage (WP1) included *(i)* the supervision of the technical activity and of the production of the deliverables, *(ii)* the organisation of project meetings (restricted to the AVISPA personnel), and *(iii)* the writing of the *D1.3 - Periodic Progress Report* (this document) and of the *D1.4 Final Project Report*. All these objectives have been realised successfully: 2 project meetings with a large number of attendees from all project partners have been held. Project work proceeded in compliance with the plan set out in the Technical Annex, meeting all the success criteria.

The activities for the Dissemination workpackage (WP8) included the management of the AVISPA Web-Site (`www.avispa-project.org`), the organisation of the 3rd project workshop and of a tutorial, and the presentation of the project's achievements at conferences and in invited talks, and the preparation of the *D8.7 - Technology and Implementation Plan*. All these objectives have been realised successfully. Dissemination has followed standard scientific channels: 19 papers have been published in international conferences and journals; 2 PhD theses are about to be completed and 4 PhD student have developed a significant part of their thesis in the context of the project; a workshop has been organised, and a number of invited talks, paper presentations, and a tutorial were given in the context of major scientific events. Additionally, we have actively sought for contacts and exchanges of ideas with representatives of research projects on related themes that are currently being carried out at the national, EU, or international level.

We have also continued the dialogue between AVISPA and the Internet Engineering Task Force (IETF). This is particularly important as the large collection of practically relevant, security-sensitive, industrial protocols that AVISPA is studying are mostly being standardised by the IETF. The list of chosen candidate protocols and related problems, as

described in Deliverable 6.1 [33], has been made available to the IETF and discussed with the security area directors. We have also presented the results of the Project during an invited presentation at the Open Security Area Directorate Meeting held in the context of the 62nd Meeting of the IETF.

Summarising, we have met all the objectives that we had set out for the reporting period and satisfied all success criteria. The work we have carried out during this 3rd reporting period has led the foundations of a push-button technology, based on automated deduction, for validating security-sensitive protocols like those used in electronic commerce, telecommunications, multi-media, and other application areas. We believe that this technology will pave the way to the construction of industrial-strength protocol validation tools that will reduce time-to-market and increase trust in the security of applications, thereby improving the competitiveness of European companies working in these application areas.

2 Work Progress Overview

2.1 Specific objectives for the reporting period

The specific objectives of the project for the reporting period are:

1. To extend the specification languages HLPSL and IF so to support the specification of protocols, security goals, and threat models of industrial complexity; to extend the implementation of the HLPSL2IF translator from HLPSL to IF.
2. To build constructs for expressing security goals and assumptions about the environment; to support the specification and the analysis under more sophisticated assumptions such as, e.g., the use of non perfect encryption primitives; to support compositionality of intruder theories, protocols, and communication channels.
3. To advance of state-of-the-art in automated deduction techniques to scale up to this new level of complexity.
4. To investigate classes of protocols for which confidentiality is decidable, even when considering an unbounded number of sessions.
5. To implement the new techniques in the AVISPA Tool.
6. To extend the AVISPA library with new security problems (protocols and security properties) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation.
7. To tune the AVISPA Tool and demonstrate proof-of-concept on the AVISPA Library.
8. To initiate the migration of this technology into standardisation organisations such as the IETF so that both the scientific and the industrial community can benefit from the advances achieved by this project.

2.2 Overview of the progress of the project during the reporting period

The architecture of version 3 of the AVISPA Tool is depicted in Figure 1: specifications of security protocols and properties written in a high-level protocol specification language (the HLPSL specification language) are automatically translated (by the HLPSL2IF translator) into a format amenable to formal analysis (the Intermediate Format IF, which is a low-level specification language); the resulting specifications are then given as input to the different back-ends of the AVISPA Tool: OFMC, CL-AtSe, SATMC, and TA4SP. Upon termination, each back-end reports whether the input problem was solved (positively or negatively) and displays an attack on the protocol whenever one is found.

Considerable progress has been made during the second year on all the objectives and significant results have been achieved on the following areas. We now briefly summarise the achieved results; detailed descriptions are given in the Deliverable Summary Sheets.

2.2.1 Specification languages for Internet security protocols (WP2&3).

A significant amount of work and attention have been devoted to the improvement and the extension of the specification languages HLPSL and IF, as well as to the development of the HLPSL2IF translator. The main extensions and modifications are the following:

HLPSL We have carried out a number of syntactic improvements and extensions to the language:

- We have removed the type `list` (rarely used and not completely handled) and have extended the handling of sets by adding the possibility to delete elements.
- We have introduced an assignment operator (`:=`) for distinguishing it from comparisons.
- We have made the generation of fresh values explicit: `N:=new()`.
- We have modified the `secret` predicate so to allow for the description of secrecy with respect to a set of agents.
- We have simplified the declaration of goal macros.
- We have extended the goal language so to allow for the description of temporal properties.

IF The only change in the IF concerns the description of the goals which now can be either

- a section for positive properties written in a temporal language;
- a section for attack states specified by means of (constrained) Boolean formulae.

HLPSL2IF The HLPSL2IF translator has been updated for taking into account the modifications in the specification languages.

Output Format The Output Format is stable and has almost not been modified.

Additionally, for the release of the first version of the AVISPA Tool, the following documentation has been produced:

- A *user manual*, including the detailed description of all the specification languages (HLPSL, IF, OF).
- A *tutorial*, for helping users to write HLPSL specifications.

The *web interface* has also been improved considerably.

The relevant deliverables produced during the reporting period are:

- D4.6 – AVISPA tool v.3 [4]

2.2.2 Error-detection and verification procedures (WP4&5).

The scaling up of the different state-of-the-art automatic analysis techniques developed by the partners to large-scale security-sensitive protocols is one of the most important technical objectives of the AVISPA project. These techniques are implemented in the back-ends of the AVISPA Tool:

OFMC, an on-the-fly model-checker developed and maintained by ETHZ,

CL-AtSe, a protocol analyser based on Constraint Logic developed and maintained by INRIA, and

SATMC, a SAT-based model-checker developed and maintained by UNIGE.

TA4SP, a tree automata based protocol analyser developed and maintained by the LIFC group affiliated with INRIA.

Moreover, we have devised a number of new heuristics, optimisations, as well as reduction and abstraction techniques, both general and specific to the individual back-ends, both for verification and for error-detection. We have implemented them in the back-ends and carried out experiments to assess their strength. Significant improvements have thus been obtained that enabled the AVISPA Tool to tackle the new, more complex protocols added to the AVISPA Library. We have also proved for some classes of protocols that confidentiality is decidable (they admit an attack searching procedure that is complete and terminate), even when considering an unbounded number of sessions, and we have investigated different forms of compositionality, obtaining a number of results on composition of intruder theories, protocols, and communication channels.

The relevant deliverables produced during the reporting period are:

- D4.1 – Compositionality [3]
- D4.6 – AVISPA Tool v.3 [4]
- D5.3 – Completeness Issue [5]

2.2.3 Analysis of industrial protocols (WP6&7).

During the 3rd reporting period we have formalised in HLPSL further security problems that have been identified as practically relevant in Deliverable 6.1 [33], in particular five of the seven Main Protocols. The resulting collection of specifications (called the AVISPA Library) has then been used to thoroughly assess the AVISPA Tool, thereby demonstrating proof-of-concept on a large collection of practically relevant, industrial protocols.

As described in [33], the following criteria, which refine the ones given in the Technical Annex, are used as for the assessment of the AVISPA tool at month 30:

Coverage: at least 80 security problems from 20 groups of the AVISPA library should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 60) of these 80 problems, including at least one problem from each of the first seven groups given in [33], by either verifying that the protocol satisfies the desired security property (mainly for scenarios consisting of a bounded number of protocol sessions) or by finding a counterexample demonstrating that the property is violated.

Performance: the verification of each problem should be carried out in less than 1 hour of CPU time.

The results demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 215 problems from 22 groups, and the tool successfully analyses 215 problems in less than 24 minutes of CPU time per problem (globally, the entire library of 215 problems requires 87 minutes of CPU time to be analysed). All the above requirements (namely coverage, effectiveness, and performance) are therefore more than fulfilled.

The relevant deliverables produced during the reporting period are:

- D7.4 – Assessment of the AVISPA Tool v. 3 [6]

2.2.4 Deviations from the work-plan.

No deviations from the work-plan have been necessary.

2.3 GANTT Chart — Project Planning and Timetable

A GANTT chart depicting the scheduling of the workpackages and showing the progress made per task is given in Figure 2.3; this chart is the updated version of the chart given in the Technical Annex.

2.4 Deliverables produced during the reporting period

The deliverables due by the second reporting period are listed in Table 2. Brief descriptions of the individual deliverables are given in the Deliverable Summary Sheets in the following pages.

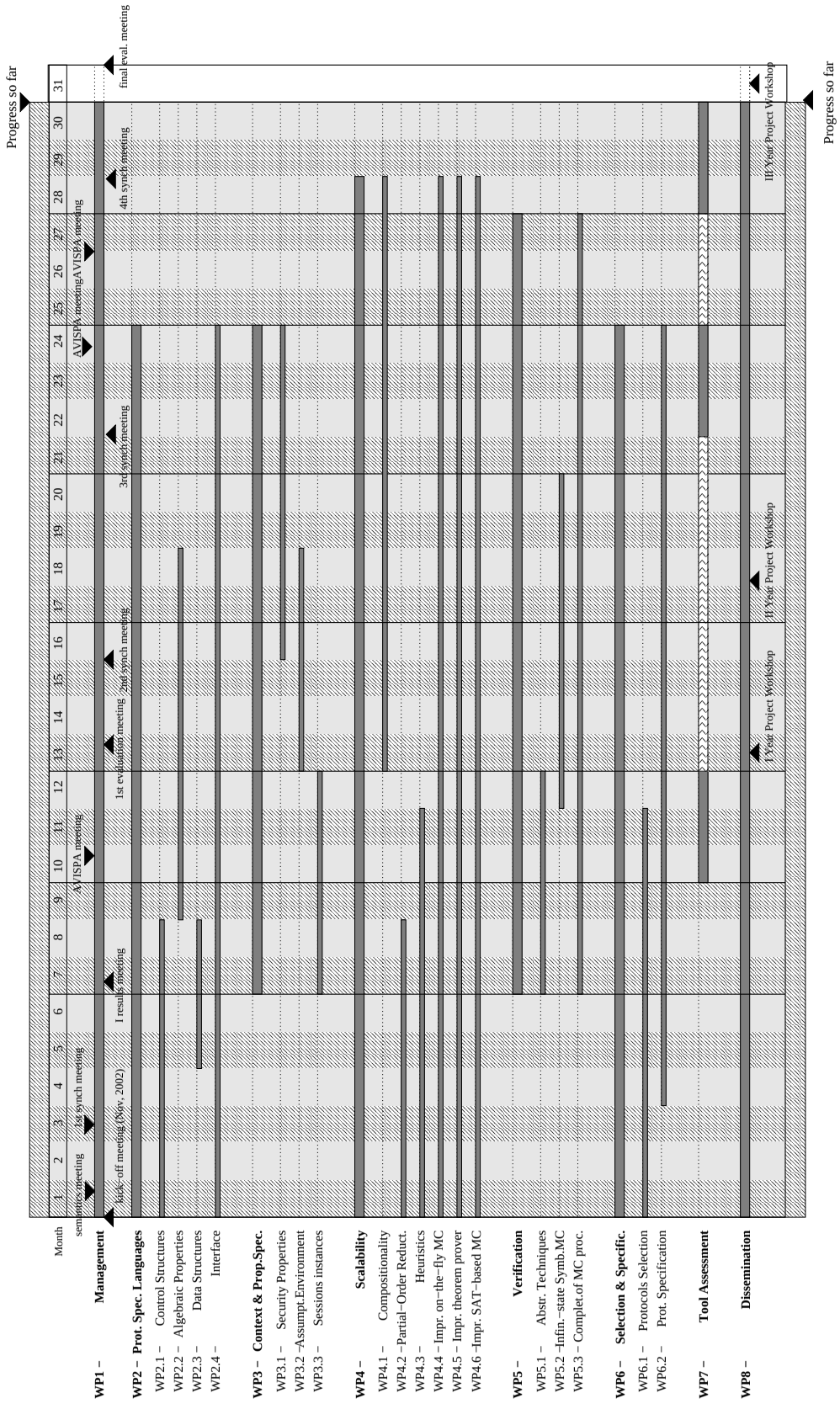

Figure 2: GANTT Chart of the AVISPA Project

Table 2: Deliverables Table

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Del. No.	Revision	Title	Type[1]	Classification[2]	Due Date	Issue Date
1.3	1.0	Periodic Progress Report N°: 3 (Draft)	R	Pub.	30.08.2005	13.07.2005
1.4	1.0	Final Project Report (Draft)	R	Pub.	30.08.2005	13.07.2005
4.1	1.0	Compositionality	R&O	Pub.	30.04.2005	30.06.2005
4.6	1.0	AVISPA Tool v.3	R&S	Pub.	31.03.2005	20.06.2005
5.3	1.0	Completeness Issue	R&O	Pub.	31.03.2005	31.05.2005
7.4	1.0	Assessment of the AVISPA Tool v.3	R	Pub.	30.06.2005	30.06.2005
8.1	1.0	The AVISPA website	S	Pub.	-	-
8.6	1.0	Year 3 Project Workshop	W	Pub.	30.04.2005	30.06.2005
8.7	1.0	Technology and Implementation Plan (Draft)	R	Pub.	30.08.2005	13.07.2005

[1] R: Report; D: Demonstrator; S: Software; W: Workshop; O: Other
[2] Int.: Internal Circulation within the project
Pub.: Public document

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 1.3
Title: **Periodic Progress Report N°: 3** (Draft)
Due date: 30.06.2005
Delivery Date: 30.06.2005

Short Description: This periodic progress report covers the last 6 months of the AVISPA project. It consists of an executive summary, of an overview of the work progress, of details about the project management, coordination, and cost breakdown, and of a description of information dissemination and exploitation of results.

Partners owning: UNIGE
Partners contributed: INRIA, ETHZ, Siemens
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 1.4
Title: **Final Project Report** (Draft)
Due date: 30.06.2005
Delivery Date: 30.06.2005

Short Description: This report provides a comprehensive view of the results obtained, of the methodologies and approaches employed, and of changes in the state-of-the-art since the project was contracted, and elaborates on the degree to which the objectives have been reached.

Partners owning: UNIGE
Partners contributed: INRIA, ETHZ, Siemens
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 4.1
Title: **Compositionality**
Due date: 30.04.2005
Delivery Date: 20.06.2005

Short Description: In this deliverable, we report on three different approaches that we have investigated to tackle different aspects of compositionality: a general method for reasoning about contract-signing protocols using a specialised protocol logic, an algorithm for combining decision procedures for intruder constraints on disjoint signatures, and (Abstract) Secure Communication Channels as a means of modelling larger application protocols which make use of several sub-protocols and where one wishes to specify different intruder models for different parts of a protocol. Our experimental analyses show that these methods are very useful to further scale up the automated deduction techniques and tools that we have been developing in the AVISPA project.

Partners owning: ETHZ
Partners contributed: UNIGE, ETHZ, Siemens
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 4.6
Title: **AVISPA Tool v.3**
Due date: 31.03.2005
Delivery Date: 31.05.2005

Short Description: This deliverable describes version 3 of the AVISPA Tool for security protocol analysis, focussing in particular on the modifications and improvements with respect to version 2 of the tool.

Partners owning: ETHZ
Partners contributed: UNIGE, INRIA
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 5.3
Title: **Completeness Issue**
Due date: 31.03.2005
Delivery Date: 20.06.2005

Short Description: Our back-ends either consider a finite number of protocol sessions or perform abstractions. In the former case, we cannot be sure that there are no attacks at all; in the latter case some false attacks might be reported. In this deliverable we have investigated two classes of protocols for which we can decide the existence of secrecy flaws. For the first class we have encoded the protocol analysis problem as a logical satisfiability problem that we have decided by a resolution strategy. For the second class we have applied tree automata techniques.

Partners owning: INRIA
Partners contributed: UNIGE, ETHZ
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 7.4
Title: **Assessment of the AVISPA Tool v.3**
Due date: 30.06.2005
Delivery Date: 30.06.2005

Short Description: In this document, we report on the assessment of the AVISPA Tool at project month 30. The results of the assessment demonstrate the achievement of the project's objectives for the reporting period. We have been able to formalise in the HLPSL 215 problems from 22 groups (including 38 problems from the seven main groups given in [33]), and the AVISPA Tool v.3 successfully analyses all the 215 problems in less than 24 minutes of CPU time per problem (globally, the whole library of 215 problems requires 87 minutes to be analysed). All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the AVISPA Tool v.3. Moreover, the AVISPA Tool v.3 is able to detect, besides those already discovered by its previous versions, new attacks (i.e. previously unknown in literature) to some of the protocols recently analysed.

Partners owning: UNIGE
Partners contributed: INRIA, ETHZ
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 8.1
Title: **The AVISPA website**
Due date: -
Delivery Date: -

Short Description: In order to provide a comprehensive and timely dissemination of the project's results we have set up at the very beginning of the project and since then maintained a publicly available web-site at the URL `http://www.avispa-project.org`. Currently the website consists of the following sections: *(i)* a general introduction to the project: the objectives, the expected results, the milestones, the detailed description of the consortium and its coordinates within the Fifth Framework Programme; *(ii)* the list of events related to AVISPA: meetings, conferences, workshops, and their availability to the public; *(iii)* the list of present and past collaborators; *(iv)* publications related to AVISPA, both in the scientific community and in the general press; *(v)* a "Software" section which contains the downloading instructions for the AVISPA Tool as well as a link to the AVISPA web-based graphical user interface; *(vi)* three sections especially dedicated to (1) internal communication among AVISPA partners, (2) communication with the European Commission, (3) communication with the IETF; and *(vii)* a number of relevant links: other projects, institutions and companies that are related to AVISPA.

Partners owning: UNIGE
Partners contributed: INRIA
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 8.6
Title: **Year 3 Project Workshop**
Due date: 30.04.2005
Delivery Date: 30.06.2005

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

Partners owning: UNIGE
Partners contributed: ETHZ, INRIA, Siemens
Made available to: public

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252
Project Acronym: AVISPA
Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 8.7
Title: **Technology and Implementation Plan** (Draft)
Due date: 30.06.2005
Delivery Date: 30.06.2005

Short Description: This document describes the participants' actual achievements in dissemination and their plans for the exploitation of the results obtained in the project.

Partners owning: UNIGE
Partners contributed: ETHZ, INRIA, Siemens
Made available to: public

2.5 Comparison of planned activities and actual work accomplished

The activity within the project proceeded as planned in the Technical Annex. A comparison between the estimated and actual effort in person-months is given in Table 3. A detailed description of the activities carried out by the project partners is given in the Progress Overview Sheets in the following pages.

The figures relative to the effort in person months spent by Siemens in the reporting period are now final as opposed to the estimated figures indicated in version 1.0 of this document. The extra person months have been devoted to the writing of a revised version of the AVISPA Library and to the dissemination activities.

Table 3: Effort in person months for reporting period 01.01.2005–30.06.2005

	UNIGE				INRIA				ETHZ				Siemens			
	Period		Total		Period		Total		Period		Total		Period		Total	
WP/Task	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act
WP1	**6,1**	**5,0**	**15**	**14**	**0,3**	**0,2**	**1**	**1**	**0,2**	**0,2**	**1**	**1**	**0,2**	**0,2**	**1**	**1**
Task 1.1	4,5	2,5	10	7,5	0	0	0	0	0	0	0	0	0	0	0	0
Task 1.2	1	1	3	3	0,3	0,2	1	1	0,2	0,2	1	1	0,2	0,2	1	1
Task 1.3	0,6	1,5	2	3,5	0	0	0	0	0	0	0	0	0	0	0	0
WP2	**0**	**2**	**11**	**9,5**	**0**	**6**	**22**	**22**	**2**	**3**	**13**	**14**	**0**	**0**	**2**	**7,2**
WP 2.1	0	2	4	5	0	0	8	8	1	1	3	4	0	0	1	6,2
WP 2.2	0	0	4	3	0	2	5	5	0	1	5	5	0	0	0,5	0,3
WP 2.3	0	0	3	1,5	0	1	3	3	1	1	3	5	0	0	0,5	0,7
WP 2.4	0	0	0	0	0	3	6	6	0	0	2	0	0	0	0	0
WP3	**0**	**3**	**12**	**10**	**0**	**2**	**15**	**15**	**1**	**1**	**15**	**15**	**0**	**0**	**7**	**3**
WP 3.1	0	2	5	5	0	2	8	8	1	1	6	6	0	0	4	1
WP 3.2	0	1	5	3	0	0	7	7	0	0	5	5	0	0	2,5	1,5
WP 3.3	0	0	2	2	0	0	0	0	0	0	4	4	0	0	0,5	0,5
WP4	**7,6**	**5**	**17**	**19**	**3**	**5**	**6**	**8**	**4**	**4**	**17**	**17**	**0**	**0,2**	**0**	**0,7**
WP 4.1	0	3	4	5	0	2	0	2	3	3	4	4	0	0,2	0	0,2
WP 4.2	0	0	0	0	0	0	0	0	0	0	4	4,5	0	0	0	0
WP 4.3	0	0	1	1	0	0	1	1	0	0	4	3	0	0	0	0
WP 4.4	0	0	0	0	0	0	0	0	1	1	5	5,5	0	0	0	0,5
WP 4.5	0	0	0	0	3	3	5	5	0	0	0	0	0	0	0	0
WP 4.6	7,6	2	12	13	0	0	0	0	0	0	0	0	0	0	0	0
WP5	**5**	**4**	**9**	**8**	**1,5**	**2**	**8**	**8**	**2**	**2**	**8**	**8**	**0**	**0**	**3**	**0**
WP 5.1	0	0	3	2	0	0	2	2	0	0	3	3	0	0	1,5	0
WP 5.2	0	0	1	2	0	0	3	3	0	0	3	3	0	0	1,5	0
WP 5.3	5	4	5	4	1,5	2	3	3	2	2	2	2	0	0	0	0
WP6	**3**	**2**	**4**	**6**	**0**	**0**	**2**	**2**	**0**	**1**	**4**	**6**	**0**	**1,8**	**18**	**18**
Task 6.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	4,1
Task 6.2	3	2	4	6	0	0	2	2	0	1	4	6	0	1,8	12	14
WP7	**0,9**	**1**	**2**	**3**	**1,2**	**0,9**	**2**	**2**	**0,7**	**0,7**	**2**	**2**	**1,6**	**1,4**	**2**	**4,6**
Task 7.1	0	0	0,6	0,6	0	0	0	0	0	0	0	0	0	0	0	0
Task 7.2	0,5	0,6	1	2	0,4	0,4	1	1	0,2	0,2	1	1	1,6	1,4	2	4,6
Task 7.3	0,4	0,4	0,4	0,4	0,8	0,5	1	1	0,5	0,5	1	1	0	0	0	0
WP8	**2**	**2,1**	**4**	**6,6**	**2**	**1,2**	**4**	**4**	**1,4**	**2**	**4**	**4,8**	**1,4**	**0,7**	**3**	**3,3**
Task 8.1	0,5	0,5	1	1,5	0	0	0	0	0	0	0	0	0	0	0	0
Task 8.2	0,5	0	0,8	0,8	0,5	0,2	1	1	0,4	1	1	1,8	0,6	0,5	1,5	1,7
Task 8.3	0,2	0,6	0,4	0,8	0	0	0	0	0	0	0	0	0,2	0,2	0,5	0,6
Task 8.4	0,8	1	1,8	3,5	1,5	1	3	3	1	1	3	3	0,6	0	1	1

PROGRESS OVERVIEW SHEET

Organization: UNIGE

	Planned Effort	Planned Date		Actual Date		Resources Employed	Cumulative Resources
WP/Task	**Whole Project**	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP1	**15,0**	**1**	**30**	**24**	**30**	**5,0**	**14,0**
Task 1.1	10,0	1	30	24	30	2,5	7,5
Task 1.2	3,0	1	30	24	30	1,0	3,0
Task 1.3	2,0	1	30	24	30	1,5	3,5
WP2	**11,0**	**1**	**24**	**24**	**24**	**2,0**	**9,5**
WP 2.1	4,0	1	8	24	24	2,0	5,0
WP 2.2	4,0	9	18	24	18	-	3,0
WP 2.3	3,0	5	8	24	18	-	1,5
WP 2.4	-	1	24	24	24	-	-
WP3	**12,0**	**7**	**24**	**24**	**24**	**3,0**	**10,0**
WP 3.1	5,0	16	24	24	30	2,0	5,0
WP 3.2	5,0	13	18	24	18	1,0	3,0
WP 3.3	2,0	7	12	24	12	-	2,0
WP4	**17,0**	**1**	**28**	**24**	**28**	**5,0**	**18,8**
WP 4.1	4,0	13	24	24	28	3,0	5,0
WP 4.2	-	1	8	24	14	-	-
WP 4.3	1,0	1	8	24	14	-	1,0
WP 4.4	-	1	28	24	28	-	-
WP 4.5	-	1	28	24	28	-	-
WP 4.6	12,0	1	28	24	28	2,0	12,8
WP5	**9,0**	**7**	**27**	**24**	**27**	**4,0**	**8,0**
WP 5.1	3,0	7	12	24	18	-	2,0
WP 5.2	1,0	12	20	24	20	-	2,0
WP 5.3	5,0	7	27	24	27	4,0	4,0
WP6	**4,0**	**1**	**24**	**24**	**24**	**2,0**	**6,0**
Task 6.1	-	1	10	24	11	-	-
Task 6.2	4,0	4	24	24	30	2,0	6,0
WP7	**2,0**	**10**	**30**	**24**	**30**	**1,0**	**3,0**
Task 7.1	0,6	10	11	24	11	-	0,6
Task 7.2	1,0	11	30	24	30	0,6	2,0
Task 7.3	0,4	11	30	24	30	0,4	0,4
WP8	**4,0**	**1**	**30**	**24**	**30**	**2,1**	**6,6**
Task 8.1	1,0	1	30	24	30	0,5	1,5
Task 8.2	0,8	6	30	24	30	-	0,8
Task 8.3	0,4	1	30	24	30	0,6	0,8
Task 8.4	1,8	1	30	24	30	1,0	3,5
	74,0					**24,1**	**75,9**
One person-month is 141.3 person-hours							

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	• Detailed planning and scheduling of project activities • Correspondence with Project Officer • Maintenance of concurrent versioning system for distributed management of software and documentation
Task 1.2	• Organisation of the technical program of the AVISPA meeting held at Siemens, München, on 26-27.02.2005 • Organisation of the technical program of the 4th AVISPA Synchronisation Meeting
Task 1.3	• Budgetary overviews • Management of cost statements
WP2	
WP 2.1	• Extensions to the HLPSL
WP 2.2	
WP 2.3	
WP 2.4	
WP3	
WP 3.1	• Design of a language for expressing complex security properties
WP 3.2	• Modelling of non standard intruder models via fairness constraints
WP 3.3	
WP4	
WP 4.1	• Compositionality
WP 4.2	
WP 4.3	
WP 4.4	
WP 4.5	
WP 4.6	• Improvements of SATMC
WP5	
WP 5.1	
WP 5.2	
WP 5.3	• Completeness of the SAT-based approach
WP6	
Task 6.1	
Task 6.2	• Formal specification of selected problems
WP7	
Task 7.1	
Task 7.2	• Assessment of the AVISPA Tool v.3
Task 7.3	• Comparative analysis
WP8	
Task 8.1	• Enhancement of the website
Task 8.2	• Organisation of the 3rd Project Workshop • Organisation of Project Meetings
Task 8.3	• Writing of the Technology and Implementation Plan
Task 8.4	• Writing of scientific publications

Deliverables due this period		
Number	**Title**	**Status**
D1.3	Periodic Progress Report N°: 3	Draft
D1.4	Final Project Report N°: 3	Draft
D7.4	Assessment of AVISPA Tool v.3	Final
D8.1	The AVISPA website	Final
D8.6	Year 3 Project Workshop	Final
D8.7	Technology and Implementation Plan	Draft

Dissemination actions (articles, workshops, conferences, etc.)

1. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In the Proceedings of the 17th International Conference on Computer-Aided Verification (CAV'05), Edinburgh, Scotland, July 6-10, 2005. Available at `www.avispa-project.org`
2. A. Armando, C. Castellini, E. Giunchiglia, M. Maratea. The SAT-based Approach to Separation Logic. Accepted for publication on the Journal of Automated Reasoning.
3. A. Armando and L. Compagna. An Optimized Intruder Model for SAT-based Model-Checking of Security Protocols. In *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004)*, pages 91–108. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct), July 2005.
4. A. Armando and L. Viganò. Preface (editorial). *Electronic Notes in Theoretical Computer Science 125(1):1 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 2005.
5. A. Armando and L. Viganò, editors. *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004)*. Electronic Notes in Theoretical Computer Science 125(1) (Elsevier Science Direct), 2005.
6. Organisation of ARSPA'05: the ICALP'05 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
7. Editing of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`
8. Invited Talk on the AVISPA Project at the "Open Security Area Directorate Meeting" during the 62th IETF meeting in Minneapolis, USA, March 5, 2005.

PROGRESS OVERVIEW SHEET

Organization: INRIA

	Planned Effort	Planned Date		Actual Date		Resources Employed	Cumulative Resources
WP/Task	Whole Project	Start	End	Start	End	This Period	Since start
WP1	**1,0**	**1**	**30**	**24**	**30**	**0,2**	**1,0**
Task 1.1	**-**	1	30	24	30	**-**	-
Task 1.2	**1,0**	1	30	24	30	**0,2**	1,0
Task 1.3	**-**	1	30	24	30	**-**	-
WP2	**22,0**	**1**	**24**	**24**	**24**	**6,0**	**22,0**
WP 2.1	**8,0**	1	8	24	24	**-**	8,0
WP 2.2	**5,0**	9	18	24	18	**2,0**	5,0
WP 2.3	**3,0**	5	8	24	18	**1,0**	3,0
WP 2.4	**6,0**	1	24	24	24	**3,0**	6,0
WP3	**15,0**	**7**	**24**	**24**	**24**	**2,0**	**15,0**
WP 3.1	**8,0**	16	24	24	30	**2,0**	8,0
WP 3.2	**7,0**	13	18	24	18	**-**	7,0
WP 3.3	**-**	7	12	24	12	**-**	-
WP4	**6,0**	**1**	**28**	**24**	**28**	**5,0**	**8,0**
WP 4.1	**-**	13	24	24	28	**2,0**	2,0
WP 4.2	**-**	1	8	24	14	**-**	-
WP 4.3	**1,0**	1	8	24	14	**-**	1,0
WP 4.4	**-**	1	28	24	28	**-**	-
WP 4.5	**5,0**	1	28	24	28	**3,0**	5,0
WP 4.6	**-**	1	28	24	28	**-**	-
WP5	**8,0**	**7**	**27**	**24**	**27**	**2,0**	**8,0**
WP 5.1	**2,0**	7	12	24	18	**-**	2,0
WP 5.2	**3,0**	12	20	24	20	**-**	3,0
WP 5.3	**3,0**	7	27	24	27	**2,0**	3,0
WP6	**2,0**	**1**	**24**	**24**	**24**	**-**	**2,0**
Task 6.1	**-**	1	10	24	11	**-**	-
Task 6.2	**2,0**	4	24	24	30	**-**	2,0
WP7	**2,0**	**10**	**30**	**24**	**30**	**0,9**	**2,0**
Task 7.1	**-**	10	11	24	11	**-**	-
Task 7.2	**1,0**	11	30	24	30	**0,4**	1,0
Task 7.3	**1,0**	11	30	24	30	**0,5**	1,0
WP8	**4,0**	**1**	**30**	**24**	**30**	**1,2**	**4,0**
Task 8.1	**-**	1	30	24	30	**-**	-
Task 8.2	**1,0**	6	30	24	30	**0,2**	1,0
Task 8.3	**-**	1	30	24	30	**-**	-
Task 8.4	**3,0**	1	30	24	30	**1,0**	3,0
	60,0					**17,3**	**62,0**
One person-month is 130.4 person-hours							

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	
Task 1.2	• Participation to the meetings
Task 1.3	
WP2	
WP 2.1	
WP 2.2	• Addition of axioms in the specification languages
WP 2.3	• Improvements of the syntax and semantics of the IF
WP 2.4	• Improvement of the graphical interface runnable on the web
WP3	
WP 3.1	• Addition of temporal security properties in HLPSL
WP 3.2	
WP 3.3	
WP4	
WP 4.1	
WP 4.2	
WP 4.3	
WP 4.4	
WP 4.5	• Improvement of the implementation of CL-AtSe
WP 4.6	
WP5	
WP 5.1	
WP 5.2	
WP 5.3	• Proof of completeness of secrecy for classes of protocols
WP6	
Task 6.1	
Task 6.2	
WP7	
Task 7.1	
Task 7.2	• Preparation of the assessment of AVISPA Tool v.3
Task 7.3	• Comparative analysis
WP8	
Task 8.1	
Task 8.2	• Organisation of the first and second AVISPA workshops
Task 8.3	
Task 8.4	• Writing of scientific publications

Deliverables due this period		
Number	**Title**	**Status**
D5.3	Completeness Issue	Final

Dissemination actions (articles, workshops, conferences, etc.)

1. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In the Proceedings of the 17th International Conference on Computer-Aided Verification (CAV'05), Edinburgh, Scotland, July 6-10, 2005. Available at `www.avispa-project.org`
2. Y. Chevalier, M. Rusinowitch. Combining Intruder Theories. To appear in the *Proceedings of International Colloquium on Automata, Languages and Programming (ICALP)*, 2005. Long version available as INRIA Research Report.
3. V. Cortier, M. Rusinowitch and E. Zalinescu. A resolution Strategy for Verifying Cryptographic Protocols with CBC Encryption and Blind Signatures. To appear in the proceedings of the 7th ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'05), Lisboa, Portugal, July 2005, ACM press.
4. Tomasz Truderung, Regular Protocols and Attacks with Regular Knowledge, to appear in the Proceedings of the International Conference on Automated Deduction (CADE), 2005, LNCS, Springer.
5. Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. Theoretical Computer Science, 338(1-3):247-274, June 2005.
6. Laurent Vigneron, editor. Proceedings of the 19th International Workshop on Unification, Nara, Japan, April 2005. Available as LORIA Research Report A05-R-022, Nancy, France.
7. Y. Chevalier and M. Rusinowitch. Combining Intruder Theories. In L. Vigneron, editor, Proceedings of the 19th International Workshop on Unification, pages 63-76, Nara, Japan, April 2005.
8. L. Vigneron. Tutorial: A Tool helping to Design Cryptographic Protocols. In 4th Conference on Security and Network Architectures (SAR'05), Batz sur Mer, France, June 2005.
9. Organisation of ARSPA'05: the ICALP'05 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
10. Editing of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`
11. M. Backes and A. Datta and A. Derek and J.C. Mitchell and M. Turuani. Compositional Analysis of Contract Signing Protocols. Proceedings of 18th IEEE Computer Security Foundations Workshop. June 2005.

PROGRESS OVERVIEW SHEET

Organization: ETHZ

	Planned Effort	Planned Date		Actual Date		Resources Employed	Cumulative Resources
WP/Task	Whole Project	Start	End	Start	End	This Period	Since start
WP1	**1,0**	**1**	**30**	**24**	**30**	**0,2**	**1,0**
Task 1.1	**-**	1	30	24	30	**-**	-
Task 1.2	**1,0**	1	30	24	30	**0,2**	1,0
Task 1.3	**-**	1	30	24	30	**-**	-
WP2	**13,0**	**1**	**24**	**24**	**24**	**3,0**	**14,0**
WP 2.1	**3,0**	1	8	24	24	**1,0**	4,0
WP 2.2	**5,0**	9	18	24	18	**1,0**	5,0
WP 2.3	**3,0**	5	8	24	18	**1,0**	5,0
WP 2.4	**2,0**	1	24	24	24	**-**	-
WP3	**15,0**	**7**	**24**	**24**	**24**	**1,0**	**15,0**
WP 3.1	**6,0**	16	24	24	30	**1,0**	6,0
WP 3.2	**5,0**	13	18	24	18	**-**	5,0
WP 3.3	**4,0**	7	12	24	12	**-**	4,0
WP4	**17,0**	**1**	**28**	**24**	**28**	**4,0**	**17,0**
WP 4.1	**4,0**	13	24	24	28	**3,0**	4,0
WP 4.2	**4,0**	1	8	24	14	**-**	4,5
WP 4.3	**4,0**	1	8	24	14	**-**	3,0
WP 4.4	**5,0**	1	28	24	28	**1,0**	5,5
WP 4.5	**-**	1	28	24	28	**-**	-
WP 4.6	**-**	1	28	24	28	**-**	-
WP5	**8,0**	**7**	**27**	**24**	**27**	**2,0**	**8,0**
WP 5.1	**3,0**	7	12	24	18	**-**	3,0
WP 5.2	**3,0**	12	20	24	20	**-**	3,0
WP 5.3	**2,0**	7	27	24	27	**2,0**	2,0
WP6	**4,0**	**1**	**24**	**24**	**24**	**1,0**	**6,0**
Task 6.1	**-**	1	10	24	11	**-**	-
Task 6.2	**4,0**	4	24	24	30	**1,0**	6,0
WP7	**2,0**	**10**	**30**	**24**	**30**	**0,7**	**2,0**
Task 7.1	**-**	10	11	24	11	**-**	-
Task 7.2	**1,0**	11	30	24	30	**0,2**	1,0
Task 7.3	**1,0**	11	30	24	30	**0,5**	1,0
WP8	**4,0**	**1**	**30**	**24**	**30**	**2,0**	**4,8**
Task 8.1	**-**	1	30	24	30	**-**	-
Task 8.2	**1,0**	6	30	24	30	**1,0**	1,8
Task 8.3	**-**	1	30	24	30	**-**	-
Task 8.4	**3,0**	1	30	24	30	**1,0**	3,0
	64,0					**13,9**	**67,8**
One person-month is 154 person-hours							

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	
Task 1.2	• Organisation of and participation in the project meetings
WP2	
WP 2.1	• Extensions to the HLPSL
WP 2.2	
WP 2.3	• Extensions to the IF
WP 2.4	• Formal definition of the Output Format
WP3	
WP 3.1	• Design of a language for expressing complex security properties
WP 3.2	• Further investigations of a distributed temporal logic for the specification of object and meta level protocol properties
WP 3.3	
WP4	
WP 4.1	• Investigations on compositionality
WP 4.2	
WP 4.3	
WP 4.4	• Extension and improvement of the OFMC back-end
WP 4.5	
WP 4.6	
WP5	
WP 5.1	• Extension of protocol Verification in OFMC (further implementation of OFMC/FP, the verification module of OFMC for an unbounded number of sessions)
WP 5.2	
WP 5.3	Investigation of the completeness of the OFMC approach
WP6	
Task 6.1	
Task 6.2	• Formal specification of a set of selected problems
WP7	
Task 7.1	
Task 7.2	• Assessment of the AVISPA Tool v.3
Task 7.3	
WP8	
Task 8.1	
Task 8.2	Organisation of the ARSPA'05 workshop Organisation of the JAR special issue on automated reasoning for security protocol analysis
Task 8.3	
Task 8.4	• Writing of scientific publications • Organisation of the tutorial AVASP'05 • A number of invited talks about OFMC and the AVISPA Tool

Deliverables due this period		
Number	**Title**	**Status**
D4.1	Compositionality	Final
D4.6	AVISPA Tool v.3	Final

Dissemination actions (articles, workshops, conferences, etc.)

1. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In the Proceedings of the 17th International Conference on Computer-Aided Verification (CAV'05), Edinburgh, Scotland, July 6-10, 2005. Available at `www.avispa-project.org`
2. D. Basin and Sebastian Mödersheim and Luca Viganò. OFMC: A Symbolic Model Checker for Security Protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. Published online December 2004.
3. A. Armando and L. Viganò. Preface (editorial). *Electronic Notes in Theoretical Computer Science 125(1):1 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 2005.
4. A. Armando and L. Viganò, editors. *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004).* Electronic Notes in Theoretical Computer Science 125(1) (Elsevier Science Direct), 2005.
5. C. Caleiro, L. Viganò, and D. Basin. Metareasoning about security protocols using distributed temporal logic. *Electronic Notes in Theoretical Computer Science 125(1):67–89 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 2005.
6. C. Caleiro, L. Viganò, and D. Basin. Deconstructing Alice and Bob. *Electronic Notes in Theoretical Computer Science 135(1):3–22 (Proceedings of the Second Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005)*, 2005.
7. C. Caleiro, L. Viganò, and D. Basin. Relating strand spaces and distributed temporal logic for security protocol analysis. *Logic Journal of the IGPL*, to appear.
8. P. Degano and L. Viganò. Preface (editorial). *Electronic Notes in Theoretical Computer Science 135(1):1–2 (Proceedings of the Second Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005)*, 2005.
9. P. Degano and L. Viganò, editors. *Proceedings of the Second Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2005).* Electronic Notes in Theoretical Computer Science 135(1), 2005.
10. P. Hankes Drielsma and S. Mödersheim. The ASW Protocol Revisited: A Unified View. In *Electronic Notes in Theoretical Computer Science 125(1):141–156 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 2005.
11. P. Hankes Drielsma, S. Mödersheim, L. Viganò. A formalization of off-line guessing for security protocol analysis. In F. Baader and A. Voronkov, editors, *Proceedings of LPAR'04*, *LNAI 3452*, pages 363–379, Springer-Verlag 2005.
12. Organisation of ARSPA'05: the ICALP'05 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
13. Editing of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`
14. Organisation of AVASP'05: the ETAPS 2005 Tutorial on Automated Validation of Security Protocols. See `www.avispa-project.org/avasp`
15. Invited talk on the OFMC back-end and the AVISPA Project at the Faculty of Computer Science of the University of Pisa, Italy, February 17th, 2005.
16. Invited talk on the OFMC back-end and the AVISPA Project at the Faculty of Computer Science of the University of Verona, Italy, February 22nd, 2005.

Dissemination actions (articles, workshops, conferences, etc.)	
17.	Invited talk on the OFMC back-end and the AVISPA Project at the Faculty of Informatics of the University of Lugano, Switzerland, April 21st, 2005.
18.	Invited talk on the AVISPA Project at the Special Session on Security of the Twenty-First Conference on the Mathematical Foundations of Programming Semantics (MFPS XXI), Birmingham, U.K., May 19th, 2005.
19.	Invited talk on the OFMC back-end and the AVISPA Project at the Faculty of Computer Science of the Imperial College London, U.K, July 6th, 2005.

PROGRESS OVERVIEW SHEET

Organization: Siemens

	Planned Effort	Planned Date		Actual Date		Resources Employed	Cumulative Resources
WP/Task	Whole Project	Start	End	Start	End	This Period	Since start
WP1	**1,0**	**1**	**30**	**24**	**30**	**0,2**	**1,0**
Task 1.1	**-**	1	30	24	30	-	-
Task 1.2	**1,0**	1	30	24	30	0,2	1,0
Task 1.3	**-**	1	30	24	30	-	-
WP2	**2,0**	**1**	**24**	**24**	**24**	**-**	**7,2**
WP 2.1	**1,0**	1	8	24	24	-	6,2
WP 2.2	**0,5**	9	18	24	18	-	0,3
WP 2.3	**0,5**	5	8	24	18	-	0,7
WP 2.4	**-**	1	24	24	24	-	-
WP3	**7,0**	**7**	**24**	**24**	**24**	**-**	**3,0**
WP 3.1	**4,0**	16	24	24	30	-	1,0
WP 3.2	**2,5**	13	18	24	18	-	1,5
WP 3.3	**0,5**	7	12	24	12	-	0,5
WP4	**-**	**1**	**28**	**24**	**28**	**0,2**	**0,7**
WP 4.1	**-**	13	24	24	28	0,2	0,2
WP 4.2	**-**	1	8	24	14	-	-
WP 4.3	**-**	1	8	24	14	-	-
WP 4.4	**-**	1	28	24	28	-	0,5
WP 4.5	**-**	1	28	24	28	-	-
WP 4.6	**-**	1	28	24	28	-	-
WP5	**3,0**	**7**	**27**	**24**	**27**	**-**	**-**
WP 5.1	**1,5**	7	12	24	18	-	-
WP 5.2	**1,5**	12	20	24	20	-	-
WP 5.3	**-**	7	27	24	27	-	-
WP6	**18,0**	**1**	**24**	**24**	**24**	**1,8**	**17,9**
Task 6.1	**6,0**	1	10	24	11	-	4,1
Task 6.2	**12,0**	4	24	24	30	1,8	13,8
WP7	**2,0**	**10**	**30**	**24**	**30**	**1,4**	**4,6**
Task 7.1	**-**	10	11	24	11	-	-
Task 7.2	**2,0**	11	30	24	30	1,4	4,6
Task 7.3	**-**	11	30	24	30	-	-
WP8	**3,0**	**1**	**30**	**24**	**30**	**0,7**	**3,3**
Task 8.1	**-**	1	30	24	30	-	-
Task 8.2	**1,5**	6	30	24	30	0,5	1,7
Task 8.3	**0,5**	1	30	24	30	0,2	0,6
Task 8.4	**1,0**	1	30	24	30	-	1,0
	36,0					**4,3**	**37,7**
One person-month is 133.3 person-hours							

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	
Task 1.2	• Organisation of and participation in project meetings in Munich and Sophia Antipolis
Task 1.3	
WP2	
WP 2.1	• Minor extensions to HLPSL syntax and semantics
WP 2.2	
WP 2.3	
WP 2.4	
WP3	
WP 3.1	
WP 3.2	
WP 3.3	
WP4	
WP 4.1	
WP 4.2	
WP 4.3	
WP 4.4	
WP 4.5	
WP 4.6	
WP5	
WP 5.1	
WP 5.2	
WP 5.3	
WP6	
Task 6.1	
Task 6.2	• Formal specification of further problems, including three Main Protocols
WP7	
Task 7.1	
Task 7.2	• Contributions to assessment of AVISPA Tool v.3
Task 7.3	
WP8	
Task 8.1	
Task 8.2	
Task 8.3	
Task 8.4	• Project presentations, tutorials

Deliverables due this period		
Number	**Title**	**Status**

Dissemination actions (articles, workshops, conferences, etc.)

1. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In the Proceedings of the 17th International Conference on Computer-Aided Verification (CAV'05), Edinburgh, Scotland, July 6-10, 2005. Available at `www.avispa-project.org`.
2. D. von Oheimb. *Introduction to Security Protocols & Formal Methods for Security Protocol Analysis.* Part of the Full day tutorial on Automated Validation of Security Protocols (AVASP'05), Edinburgh, Scotland, April 3rd, 2005.
3. D. von Oheimb. Presentation of the AVISPA Tool at the lecture *Formal Security Modeling*, `http://www.tcs.ifi.lmu.de/~oheimb/SS05_SecMod/` and at *Diesecke & Devrient GmbH* (an SME in the security area, `http://www.gi-de.com/`)
4. Organisation of ARSPA'05: the ICALP'05 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
5. Editing of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`

2.6 State-of-the-art update

There has been considerable activity in the scientific community dedicated to security protocol analysis in 2004, as is testified by the large number of related publications in the proceedings of conferences and workshops, as well as in scientific journals. We address here only the most representative, advanced or concerted, efforts, which are significantly related to the AVISPA project.

For instance, there has been a lot of activity this year on detecting attacks in the context of models that generalise the standard Dolev-Yao intruder model. Verification procedure for handling algebraic properties have been proposed [50, 39, 46]. New security goals related to contract-signing protocols have been investigated too [44, 45]. These extensions are closely related to some AVISPA results and have been and will be taken into consideration in our future plans. There has also been an interesting advance [47, 24] in relating formal models and computational models. We have already started to investigate how to integrate these results in our approach. We also consider to apply our result to the very active area of web services.

2.6.1 The Project PROUVE

The French project PROUVE has started this year and INRIA-Lorraine is a partner of this project (administrative coordinator), together with France Telecom R&D, laboratories LSV (ENS de Cachan, France) and Verimag (Grenoble, France). The objective of PROUVE project is to verify security-sensitive protocols provided by France Telecom R&D. Like for the AVISPA Tool, the PROUVE platform will rely on a high-level specification language close to the language used in textbooks. Three tools will be applied to the case-studies: H1 (LSV), Hermes (Verimag) [38] and CL-AtSe. In contrast to AVISPA, PROUVE is oriented towards the specific applications provided by France Telecom R&D.

H1 and Hermes are designed for verifying secrecy properties for an unbounded number of sessions, in order to *prove* properties on protocols. Hermes can also detect attacks however it is limited to atomic keys. It has been successfully applied to construct secrecy proofs for about 15 protocols of the Clark/Jacob library. But they are not efficient in finding attacks: when a proof attempt fails, this does not automatically mean that there is an attack. In these cases, the tools provide some reasons for the failure but the user has to find a real attack by himself. Note that actually it is not possible to design tools that are able to prove and disprove secrecy properties automatically for an unbounded number of sessions. Thus, these tools implement some abstractions that allow them to prove secrecy properties, but prevent the detection of attacks in some protocols.

Action taken Collaboration between AVISPA and PROUVE is ongoing: although the specification languages, as well as the case-studies, are different, we believe that some back-end technologies can be shared. France Telecom RD has experimented on verifying an electronic purse protocol with CL-AtSe.

We have frequent contacts with LSV Cachan and Verimag with many reciprocal visits.

2.6.2 ECSS Group, Eindhoven

The Eindhoven Computer Science Security Group (led by Prof. Sjouke Mauw) has been working on the formal verification of black box security protocols, which is closely related to our research. Their approach is based on process algebra and on the μCRL language, which allows one to combine data and processes. The approach is quite similar to the model-checking one of CASPER. In general some approximations have to be done and there is no guarantee that an attack was not overlooked [42]. They have not investigated completeness of their approach.

From its publications list it seems that this group has shifted its interest only recently towards security protocols (the related papers dating from the end of 2003 and 2004). It seems that only a few protocols have been analysed by ECSS and whether there is a uniform, fully automatic methodology is not obvious from their work. It is questionable whether a non-specialist of μCRL model-checking would be able to apply the technique easily.

Action taken We have begun communication with the Eindhoven Computer Science Security Group, and Sjouke Mauw has accepted to join the program committee of our third year workshop, namely ARSPA'05, which will be held in Lisbon, Portugal, in co-location with ICALP 2005 (`http://www.avispa-project.org/arspa/`).

2.6.3 Blanchet's Logic Programming Approach

Bruno Blanchet (MPI for computer science, Saarbrücken, Germany, and ENS, France) has developed a tool where protocols and security properties are expressed as Horn clauses and he provides strategies to saturate these sets of clauses [30, 34, 35, 36]. The tool ProVerif allows one to prove security properties for an unbounded number of sessions, in particular strong secrecy (which means that an intruder cannot see any difference when the value of the secret changes). Note, however, that the tool may raise some false attack since nonces are abstracted by constants or function symbols, so that attacks have to be constructed by the user itself. However recently ProVerif has been enhanced to reconstruct automatically the attacks [31]. Note also that at the ARSPA'05 workshop, which we organise, Gotsman, Massacci, and Pistore will present a translation procedure from protocol descriptions in HLPSL to descriptions in the applied pi calculus, which allowed them to apply the ProVerif tool to some of our HLPSL protocol specifications [41]. This will provide the basis for further comparison and cross-fertilisation between AVISPA and ProVerif.

Action taken We have discussed at several conferences with Bruno Blanchet to share experience.

2.6.4 The Project DEGAS

A related European project, DEGAS IST-2001-32072 (`http://www.omnys.it/degas/`), is dedicated to the design of an environment for developing global applications. For instance,

a case study considered in this project is mobile home-banking. The specification language is UML and the abstract language for verification tasks is based on process algebra. The related Italian project Mefisto (`http://mefisto.web.cs.unibo.it`) on formal methods for security ended in November 2003. In particular, this project has attempted to extend protocol verification to more realistic and detailed models including time and probabilistic information flow.

In the context of these projects, a translation has been designed from Alice&Bob protocol notation to a process algebra that is similar to the spi-calculus [37]. This translation allows one to derive a precise description of the protocol behaviour, and is similar to translations previously devised for CAPSL/CIL [40], CASRUL [43], and HLPSL2IF in our projects AVISS and AVISPA. The verification is then performed by a polynomial-time static analysis and related approximation techniques. Some experiments with classical protocols from the Clark/Jacob Library are given, and both real flaws and false ones are detected on these protocols.

Note that, as discussed in [37], the approach does not address asymmetric cryptography, imperfect cryptography, timing issues, type flaw attacks related to bit-string representations. All these topics are currently investigated by the AVISPA project.

Action to be taken We have invited some of the principal investigators of the DEGAS project to our next workshop: Pierpaolo Degano of the University of Pisa will co-chair the ARSPA'05 workshop together with Luca Viganò of ETHZ, and Hanne Riis Nielson of the Technical University of Denmark has joined the program committee of the workshop. Moreover, we have begun a detailed comparison of the approach of the DEGAS project with our abstraction techniques, and in particular with the tree automata techniques discussed in [32]. We believe that it will be possible for them to reuse our technology, which is more efficient according to the experimental results.

2.6.5 The project MYTHS

MyThS, Models and Types for Security in Mobile Distributed Systems, is funded by the Global Computing pro-active initiative (GC) of the Future and Emerging Technologies (FET). (Contract IST-2001-32617). MyThS addresses the foundations of programming languages and paradigms that allow static detection of security violations, and aims at developing type theoretic methods and tools that enable formal analyses of security guarantees appropriate for systems and applications on the global computing platform. As Avispa, MyThS addresses the problems of secure communication in open-ended networks. using cryptographic means. However Myths is more focused on mobility and highly dynamic topologies and expects to derive new mechanisms for decentralised (dynamic) type-checking of distributed computing sites and migrating agents.

Avispa is more focused on providing a fully automated analysis tool although for a less general class of processes than those considered in MyThs. To our knowledge MyThs will not provide an integrated tool.

Action to be taken We plan to discuss with the involved researchers and exchange experience and compare the typed approach with ours.

2.6.6 The CAPSL Environment

In the past four years, Jonathan Millen from SRI International, the main developer of the CAPSL environment, has been regularly collaborating with David Basin's group at ETHZ, closely following our project's results and suggesting a number of possible collaborations. For instance, recent work by Millen [48, 49] is closely related to our current work on exponentiation, XOR encryption, and algebraic properties, and we have begun a fruitful exchange of ideas and results.

Action taken We will continue the regular exchange of ideas and results with Millen and his group at SRI International.

2.7 Assessment of project results and achievements

All the project objectives set for the 3rd reporting period have been successfully achieved.

Specification Languages. We have a formally defined high-level protocol specification language HLPSL and a lower-level IF specification language. HLPSL has been updated for a more intuitive syntax, following users' remarks. Both languages have been extended to support the specification of security properties via temporal operators and the specification of secrecy with respect to a set of agents. In addition, all the verification tools have a common output format that clearly explains the meaning of the results of the analysis carried out by the back-end. All this makes the AVISPA Tool the most user-friendly, but also expressive and powerful tool for the automatic analysis of security protocols.

Problems Specification. We have specified in HLPSL 66 protocols from 27 groups drawn from the list given in [33] thereby obtaining a total 215 security problems. In particular we have specified five of the seven Main Protocols.

The AVISPA Tool v.3. In order to develop version 3 of the AVISPA Tool, we have carried out the following extensions on the tool:

- The HLPSL2IF translator has been updated so to reflect the most recent extensions to the HLPSL and the IF.
- The graphical user interface has been improved.
- XEmacs mode files have been produced to assist the editing of HLPSL specifications.
- OFMC's performance has been improved by removing redundancies in the search procedure. Among other improvements, we have also been able to identity and

correct a number of minor bugs, thanks to the extensive experimentation with the large number of protocols that the AVISPA library now provides.

- CL-AtSe has been improved by integrating new algebraic properties. Among other improvements, we have also carried out a considerable amount of work on the tool kernel to improve the existing algorithms and implement all the changes decided globally by the AVISPA consortium. In particular, the attack detection methods were modified to correspond precisely to the IF semantics.
- SATMC has been improved by extending the interface and the underlying techniques of SATMC. Moreover, thanks to the intensive testing phase performed by us and by external users, we were able to identify some bugs, which we have fixed. This has lead to a new version of SATMC that is simpler to be invoked and more stable than the previous one.
- TA4SP has been updated according to the HLPSL changes about secrecy declarations, in particular to provide better support for the secrecy of data exchanged during protocol executions.

Moreover, in mid-June 2005, we have officially released the AVISPA Tool, which can now be employed by external users thanks to the web-interface accessible from the project web-site, and which is also downloadable as a single "package" to be installed on the users' local machines. Further information is available on the project web-site (`http://www.avispa-project.org`).

Assessment of the AVISPA Tool v.3. All the 215 security problems formalised in HLPSL are successfully analysed by the AVISPA Tool v.3 in less than 24 minutes of CPU time per problem (globally, the entire library of 215 problems requires 87 minutes of CPU time to be analysed). All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the AVISPA Tool v.3. Moreover, the AVISPA Tool v.3 is able to detect, besides those already discovered by its previous versions, new attacks (i.e. previously unknown in literature) to some of the protocols recently analysed.

Dissemination. Dissemination of our progress has followed standard scientific channels:

- 19 articles have been published in international conferences and journals,
- one project workshop and a tutorial have been organised, and
- several invited talks and technical presentation were given in the context of major scientific events.

We have continued the dialogue between AVISPA and the Internet Engineering Task Force (IETF), by officially presenting the AVISPA Project and Tool at the "Open Security Area Directorate Meeting" during the 62th IETF meeting in Minneapolis, USA, March 5, 2005. The presentation was very welcome and the goals of the AVISPA project were seen to be very high and valuable.

The release of the AVISPA Tool and the AVISPA Library to the public is also an effective means to disseminate the project's results. Since mid-June the software package has been downloaded 56 times and 45 people registered to the "AVISPA Users" mailing list.

3 Project Management and Coordination

Project management proved largely unproblematic also during the third reporting period. However, given the complexity of the technical objectives, particular attention has been paid to the coordination of the activities. To this end, we implemented the following project management and coordination measures.

Project Meetings. Project meetings have played a pivotal role in the coordination and synchronisation of activities among the partners:

- **AVISPA meeting**, 26-27.02.2005, Siemens, München, Germany. This meeting was devoted to check the activities carried out by the partners related to the upcoming deliverables, namely D4.1 "Compositionality", D5.3 "Completeness Issue", D4.6 "AVISPA Tool v.3".
- **4th AVISPA Synchronisation Meeting**, 2–4.05.2005, Sophia-Antipolis, France. This meeting was devoted to synchronising the activities among the partners. Special sessions were devoted to discuss open technical issues about the upcoming deliverables, namely D7.4 "Assessment of AVISPA Tool v.3", D8.6 "Year 3 Project Workshop", D8.7 "Technology and Implementation Plan".

Task-forces. The formation of task-forces (comprising experts from all the partners) to tackle well-defined, critical technical issues has been a very effective coordination measure. We formed two task-forces:

- The *translator task-force* has been given the task of updating the syntax and semantics of the specification languages HLPSL and IF, as well as to adapt and improve the translator HLPSL2IF.
- The *modelling task-force* has been given the task of formalising the selected security problems. Both task-forces have been regularly reporting their achievements in special sessions during the project meetings.

Mailing lists. The following mailing lists proved to be a very effective means for exchanging ideas within the project and for coordinating the work:

- `avispa-general@avispa-project.org` is devoted to general announcements such as advertising a project meeting or a new project publication. This mailing list comprises all the people involved in the project both at the technical level and at the management and administrative level.
- `avispa-tech@avispa-project.org` is devoted to the exchange of technical information between the partners. This mailing list comprises all the scientists from the partner groups.

- avispa-admin@avispa-project.org is devoted to the discussion of administrative, financial, and management issues. This mailing list includes all the site leaders plus a restricted number of senior researchers and administration staff.
- avispa-modeling@avispa-project.org is the mailing list used by the modelling task-force.
- avispa-compiler@avispa-project.org is the mailing list used by the translator task-force.

Internal Web-Site. Two password restricted sections of the project web-site (www.avispa-project.org, see Section 5 for more information on the site), set up at the beginning of the project, have been maintained:

- the *Internal Section* (www.avispa-project.org/internal) is used to enable the sharing of reserved documents among the partners;
- the *EC Section* (www.avispa-project.org/internal/EU) contains the deliverables in electronic form as well as the up-to-date list of deliverables.

CVS Server. A CVS Server ("CVS" stands for Concurrent Versioning System), set up at the beginning of the project, has been maintained. CVS allows for the concurrent management of (different versions of) files and it proved very valuable for the project: software and documents (e.g. deliverables) are now routinely and effectively managed via CVS by the AVISPA personnel.

4 Cost Breakdown

The cost breakdown for the reporting period is given in Table 4. Notice that, as for all Swiss partners in FP5 projects, ETHZ's Requested Contribution from the Community is 0%, and ETHZ work was financed by the Swiss Federal Office for Education and Science, which awarded a total contribution of 271,813 Euro (400,000 CHF).

Table 4. Costs in euro for the reporting period: 01.01.2005 --- 30.06.2005

	UNIGE				INRIA				ETHZ				Siemens			
	Period		Total		Period		Total		Period		Total		Period		Total	
Cost Category	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act	Est	Act
Direct Costs																
1. Personnel	129.861	136.584	364.463	394.407	33.003	59.710	213.428	232.821	66.713	88.481	333.565	95.901	54.833	45.509	264.568	324.031
2. Durable Equipment	3.253	3.875	16.264	18.728	-	-	-	-	-	-	-	-	-	-	-	-
3. Subcontracting	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4. Travel and subsistence	4.994	2.876	21.994	17.544	6.000	5.550	26.000	22.580	4.000	12.232	20.000	16.491	-	-	-	-
5. Consumables	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6. Computing	100	-	300	145	-	-	-	-	-	-	-	-	-	-	-	-
7. Protection of Knowledge	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8. Other specific costs	9.000	3.401	11.000	3.551	9.489	-	11.489	6.493	750	-	2.750	-	8.000	1.550	8.000	1.550
Subtotal	**147.208**	**146.735**	**414.021**	**434.375**	**48.492**	**65.260**	**250.917**	**261.894**	**71.463**	**100.713**	**356.315**	**112.392**	**62.833**	**47.059**	**272.568**	**325.581**
Indirect Costs																
9. Overheads	62.159	51.128	175.702	172.604	43.723	87.406	323.621	312.772	3.573	-	17.815	-	49.042	16.107	236.626	211.310
Total	**209.367**	**197.864**	**589.723**	**606.979**	**92.215**	**152.665**	**574.538**	**574.665**	**75.036**	**100.713**	**374.130**	**112.392**	**111.875**	**63.166**	**509.194**	**536.892**

5 Information Dissemination and Exploitation of Results

Communication with the IETF. The dialogue between AVISPA and the IETF is very important as the protocols in the AVISPA library — the large collection of practically relevant, security-sensitive, industrial protocols that AVISPA will study — are mostly being standardised by the IETF. The list of chosen candidate protocols and related problems has been made available to the IETF and discussed with IETF's security area directors, in particular with the purpose of obtaining feedback on the completeness of the list of protocols and the correctness of their security goals (properties). We presented this work in Minneapolis at the IETF Meeting-62 (see below).

Talks. All of the 7 articles that have been published in international conferences (cf. Section 7) have been presented at the respective meetings. We have also organised and/or given talks in the following scientific events. These talks aimed at introducing the high-level project objectives, the protocols and problems that the project is analysing, and the techniques and results achieved:

- Presentation of the AVISPA Project by A. Armando (UNIGE) at the Open Security Area Directorate Meeting (SAAG) held in the context of the 62nd Meeting of the IETF, Minneapolis, 5th March 2005. The slides of the talk are available online in the proceeding of the IETF at `http://www3.ietf.org/proceedings/05mar/saag.html` (Number of attendees: about 200).

- Invited talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Faculty of Computer Science of the University of Pisa, Italy, February 17th, 2005.

- Invited talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Faculty of Computer Science of the University of Verona, Italy, February 22nd, 2005.

- Invited talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Faculty of Informatics of the University of Lugano, Switzerland, April 21st, 2005.

- Invited talk on the AVISPA Project by L. Viganò (ETHZ) at the Special Session on Security of the Twenty-first Conference on the Mathematical Foundations of Programming Semantics (MFPS XXI), Birmingham, U.K, May 19th, 2005.

- Invited talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Faculty of Computer Science of the Imperial College London, U.K, July 6th, 2005.

Project Workshops and Tutorials.

- The Third Project Workshop: Workshop on Automated Reasoning for Security Protocols Analysis (ARSPA'05) co-located with the 32nd International Colloquium on Automata, Languages and Programming (ICALP 2005) in Lisbon, Portugal, July 16th, 2005.
- Tutorial "A Tool helping to Design Cryptographic Protocols" given at the 4th Conference on Security and Network Architectures (SAR), Batz sur Mer, France, June 2005.
- Full day tutorial on Automated Validation of Security Protocols (AVASP'05), in the context of the 8th European Joint Conference on Theory and Practice of Software (ETAPS 2005), Edinburgh, Scotland, April 3rd, 2005.

Editing.

- Proceedings of the 19th International Workshop on Unification. Laurent Vigneron, editor. Available as LORIA research report A05-R-022, Nancy, France, 2005.
- Special issue on First-Order Theorem Proving of the Journal of Automated Reasoning. Deepak Kapur and Laurent Vigneron, editors. Volume 33, Numbers 3-4, Springer Science+Business Media B.V., October 2004.
- Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04). Alessandro Armando and Luca Viganò, editors. Electronic Notes in Computer Science 125, Elsevier Science, 2005.
- Special Issue of the Journal of Automated Reasoning on "Automated Reasoning for Security Protocol Analysis". A large number of papers (21) has been submitted, out of which the program committee (consisting of A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò) selected 5 papers for publication.
- Proceedings of the ICALP 2005 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'05). Electronic Notes in Computer Science, Elsevier Science, in print. Pierpaolo Degano and Luca Viganò, editors. A preprint will be available at `www.avispa-project.org/arspa`.

Publicly available Web-Site. In order to provide a comprehensive and timely dissemination of the project's results we have set up at the very beginning of the project and since then maintained a publicly available web-site at the URL `http://www.avispa-project.org`. Currently the website consists of the following sections:

- A general introduction to the project: the objectives, the expected results, the milestones, the detailed description of the consortium and its coordinates within the Fifth Framework Programme.

- The list of events related to AVISPA: meetings, conferences, workshops, and their availability to the public.
- The list of present and past collaborators.
- Publications related to AVISPA, both in the scientific community and in the general press.
- A "Software" section which contains the downloading istructions for the AVISPA Tool as well as a link to the AVISPA web-based graphical user interface.
- Three sections especially dedicated to (1) internal communication among AVISPA partners, (2) communication with the European Commission, (3) communication with the IETF.
- A number of relevant links: other projects, institutions and companies that are related to AVISPA.

6 AVISPA Deliverables

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

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

[3] AVISPA. Deliverable 4.1: Compositionality. Available at `http://www.avispa-project.org`, 2005.

[4] AVISPA. Deliverable 4.6: AVISPA tool v.3. Available at `http://www.avispa-project.org`, 2005.

[5] AVISPA. Deliverable 5.3: Completeness Issue. Available at `http://www.avispa-project.org`, 2005.

[6] AVISPA. Deliverable 7.4: Assessment of the AVISPA tool v.3. Available at `http://www.avispa-project.org`, 2005.

[7] AVISPA. Deliverable 8.1: AVISPA Website. Available at `http://www.avispa-project.org`, 2005.

[8] AVISPA. Deliverable 8.6: Year 3 Project Workshop. Available at `http://www.avispa-project.org`, 2005.

[9] AVISPA. Deliverable 8.7: Technology and Implementation Plan.

7 AVISPA Publications

[10] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Heám, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05)*. Springer-Verlag, 2005. Available at `www.avispa-project.org`.

[11] A. Armando, C. Castellini, E. Giuchiglia, and M. Maratea. The SAT-based Approach to Separation Logic. Technical report, UNIGE, 2005. To be published in the Journal of Automated Reasoning, 2005.

[12] A. Armando and L. Compagna. An Optimized Intruder Model for SAT-based Model-Checking of Security Protocols. In *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004)*, pages 91–108. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct), July 2005.

[13] A. Armando and L. Viganò. Preface (editorial). *Electronic Notes in Theoretical Computer Science (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 125(1):1, 2005.

[14] A. Armando and L. Viganò, editors. *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004)*, Amsterdam, The Netherlands, 2005. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct).

[15] M. Backes, A. Datta, A. Derek, J.C. Mitchell, and M. Turuani. Compositional Analysis of Contract Signing Protocols. *Proceedings of 18th IEEE Computer Security Foundations Workshop*, 2005.

[16] D. Basin, S. Mödersheim, and L. Viganò. OFMC: A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. Published online December 2004.

[17] C. Caleiro, L. Viganò, and D. Basin. Deconstructing Alice and Bob. *Electronic Notes in Theoretical Computer Science 135(1):3–22 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005)*, 2005.

[18] C. Caleiro, L. Viganò, and D. Basin. Metareasoning about security protocols using distributed temporal logic. *Electronic Notes in Theoretical Computer Science (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004)*, 125(1):67–89, 2005.

[19] C. Caleiro, L. Viganò, and D. Basin. Relating strand spaces and distributed temporal logic for security protocol analysis. *Logic Journal of the IGPL*, to appear.

[20] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. *Theoretical Computer Science*, 338(1-3):247–274, June 2005.

[21] Y. Chevalier and M. Rusinowitch. Combining Intruder Theories. Technical report, INRIA — extended abstract to appear in the proceedings of ICALP'05, 2005. `http://www.inria.fr/rrrt/rr-5495.html`.

[22] Y. Chevalier and M. Rusinowitch. Combining Intruder Theories. In L. Vigneron, editor, *Proceedings of the 19th International Workshop on Unification*, pages 63–76, Nara, Japan, April 2005.

[23] V. Cortier, R. M., and E. Zalinescu. A resolution strategy for verifying cryptographic protocols with cbc encryption and blind signatures. In *Proceedings of the 7th ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'05), Lisboa, Portugal*. ACM press, July 2005.

[24] V. Cortier and B. Warinschi. Computationally Sound, Automated Proofs for Security Protocols. In *Proc. 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *Lecture Notes in Computer Science*, pages 157–171, Edinburgh, U.K, April 2005. Springer.

[25] P. Degano and L. Viganò. Preface (editorial). *Electronic Notes in Theoretical Computer Science 135(1):1–2 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005)*, 2005.

[26] P. Degano and L. Viganò, editors. *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2005)*. Electronic Notes in Theoretical Computer Science (Elsevier Science Direct), to appear.

[27] P. Hankes Drielsma and S. Mödersheim. The ASW Protocol Revisited: A Unified View. In *Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004)*, pages 141–156. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct), July 2005.

[28] P. Hankes Drielsma, S. Mödersheim, and L. Viganò. A formalization of off-line guessing for security protocol analysis. In F. Baader and A. Voronkov, editors, *Proceedings of LPAR'04*, volume 3452 of *LNAI*, pages 363–379. Springer, 2005.

[29] L. Vigneron, editor. *Proceedings of the 19th International Workshop on Unification*, Nara, Japan, April 2005. Available as LORIA Research Report A05-R-022, Nancy, France.

8 References

[30] M. Abadi, B. Blanchet, and C. Fournet. Just Fast Keying in the Pi Calculus. In *Proceedings of the 13th European Symposium on Programming (ESOP'04)*, LNCS 2986, pages 340–354. Springer, 2004.

[31] X. Allamigeon and B. Blanchet. Reconstruction of Attacks against Cryptographic Protocols. In *18th IEEE Computer Security Foundations Workshop (CSFW-18)*, Aix-en-Provence, France, June 2005. IEEE Computer Society. To appear.

[32] AVISPA. Deliverable 5.1: Abstractions. Available at `http://www.avispa-project.org`, 2003.

[33] AVISPA. Deliverable 6.1: List of selected problems. Available at `http://www.avispa-project.org`, 2003.

[34] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proceedings of CSFW'01*, pages 82–96. IEEE Computer Society Press, 2001.

[35] B. Blanchet. Automatic verification of cryptographic protocols: A logic programming approach (invited talk). In *Proceedings of PPDP'03*, pages 1–3. ACM Press, 2003.

[36] B. Blanchet. Automatic Proof of Strong Secrecy for Security Protocols. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 86–100. IEEE Computer Society Press, 2004.

[37] C. Bodei, M. Buchholtz, P. Degano, F. Nielson, and H. Riis Nielson. Automatic validation of protocol narration. In *Proceedings of CSFW'03*, pages 126–140. IEEE Computer Society Press, 2003.

[38] L. Bozga, Y. Lakhnech, and M. Perin. Pattern-based abstraction for verifying secrecy in protocols. In *Proceedings of TACAS 2003*, LNCS 2619. Springer-Verlag, 2003.

[39] H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307, Nara, Japan, Apr. 2005. Springer.

[40] G. Denker, J. Millen, and H. Rueß. The CAPSL Integrated Protocol Environment. Technical Report SRI-CSL-2000-02, SRI International, Menlo Park, CA, October 2000. Available at `http://www.csl.sri.com/~millen/capsl/`.

[41] A. Gotsman, F. Massacci, and M. Pistore. Towards an Independent Semantics and Verification Technology for the HLPSL Specification Language. *Electronic Notes in Theoretical Computer Science 135(1):59–77 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005)*, 2005.

[42] J. Groote, S. Mauw, and A. Serebrenik. Analysing the BKE-security protocol with mCRL. Computer Science Report CSR-04-30, Department of Mathematics and Computer Science, Eindhoven University of Technology, 2004.

[43] F. Jacquemard, M. Rusinowitch, and L. Vigneron. Compiling and Verifying Security Protocols. In M. Parigot and A. Voronkov, editors, *Proceedings of LPAR 2000*, LNCS 1955, pages 131–160. Springer-Verlag, 2000.

[44] D. Kähler and R. Küsters. Constraint Solving for Contract-Signing Protocols. In *Proceedings of the 16th International Conference on Concurrency Theory (CONCUR 2005)*, 2005. To appear.

[45] S. Kremer, A. Mukhamedov, and E. Ritter. Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model. In *Proceedings of the 9th International Conference on Financial Cryptography and Data Security (FC'05)*, Lecture Notes in Computer Science, Roseau, The Commonwealth Of Dominica, Feb.-Mar. 2005. Springer. To appear.

[46] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In J. Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, Apr. 2005. Springer.

[47] D. Micciancio and B. Warinschi. Soundness of formal encryption in the presence of active adversaries. In *Proceedings of the Theory of Cryptography Conference (TCC)*, LNCS 2951, pages 133–151. Springer-Verlag, 2004.

[48] J. K. Millen. On the freedom of decryption. *Information Processing Letters*, 86(6):329–333, 2003.

[49] J. K. Millen and V. Shmatikov. Symbolic protocol analysis with products and diffie-hellman exponentiation. In *Proceedings of the 16th IEEE Computer Security Foundations Workshop (CSFW'03)*, pages 47–61. IEEE Computer Society Press, 2003.

[50] G. Steel. Deduction with xor constraints in security api modelling. In R. Nieuwenhuis, editor, *Proceedings of the 20th Conference on Automated Deduction (CADE 20)*, Tallinn, Estonia, July 2005. To appear.

[51] T. Truderung. Regular protocols and attacks with regular knowledge. In *Proceedings of the International Conference on Automated Deduction (CADE)*, LNCS. Springer, 2005.