AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D1.1: Periodic Progress Report N°: 1

Covering period 01.01.2003 — 31.12.2003

Abstract

This periodic progress report covers the first year 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: *v3.0*
Date of delivery: *18.02.2005*
Classification: *public*
Person-months required: *0.5*
Due on: *31.01.2004*
Total pages: *56*

Project details

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

Information Society Technologies

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

Contents

1 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.

AVISPA is the follow-up of the 1-year FET assessment project called AVISS (Automated Verification of Infinite State Systems), which has laid the foundations for the present project and allowed the project partners to come up with the ambitious, yet clearly defined, work-plan described in the Technical Annex. The joint experience gained during the AVISS project proved to be extremely valuable as it allowed the partners to work very effectively on precisely defined tasks from the start of the project.

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

WP2 – Protocol Specification Languages To define a high-level protocol specification language capable of supporting the specification of security-sensitive, state-of-the-art Internet protocols. To design and develop a translator from the high-level language to a rewrite-based declarative intermediate format amenable to formal analysis.

WP3 – Context & Properties Specification To build constructs for expressing security goals and assumptions about the environment into both the high-level and the intermediate specification languages.

WP4 – Scalability 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.

WP5 – Verification To investigate and integrate mechanisms to derive positive statements about protocol security, i.e. verify that they achieve their security objectives.

WP6 – Selection & Specification of Protocols To define the AVISPA library, a set of formalised security problems (protocols and security properties) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation.

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 disseminate the project results through appropriate channels and in appropriate forums.

All the expected results for the first reporting period have been achieved, all success criteria set out in the Technical Annex have been met, and all (13) planned deliverables have been produced on time.

The results of the scientific workpackages (WP2—WP7) 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:

WP2&3 We have formalised the High-Level Protocol Specification Language HLPSL and the Intermediate Format IF, and have implemented the automated translator HLPSL2IF from HLPSL to IF. Both the HLPSL and the IF are more expressive than other specification languages used for the same purpose. The HLPSL is a very expressive language supporting the specification of security-sensitive protocols with a formal semantics based on an expressive first-order temporal logic. The IF is a tool-independent, low-level protocol specification language that supports the specification of sophisticated typed protocol models and that is suitable for automated deduction. Specifications of security protocols and properties written in HLPSL are automatically translated into IF specifications, which are then given as input to the different back-ends that constitute the AVISPA Tool.

When solving a problem, it is often the case that multiple protocol sessions must be considered in parallel in order to discover an attack. We have devised a number of techniques to specify parallel protocol sessions in a security problem, and thereby enlarge the class of attacks that can be considered by our tool and speed up their detection. We have implemented a HLPSL pre-processor called ASG (Automatic Session Generator), which is based on techniques for automatically assigning concrete values to the protocol variables to generate ground session instances, based on a protocol specification and a desired number of sessions to be run in parallel. Moreover, ASG identifies and filters out redundant and uninteresting sessions. We have also formalised symbolic sessions in which protocol parameters are left as uninstantiated variables (this is in contrast to ground sessions, in which all protocol variables are instantiated with concrete values). This technique exploits our symbolic representation of the intruder (the lazy intruder) to search for satisfying assignments of protocol variables that will lead to attacks.

WP4&5 We have devised a number of new heuristics, optimisations, and reduction and abstraction techniques, both general and specific to the individual back-ends. We

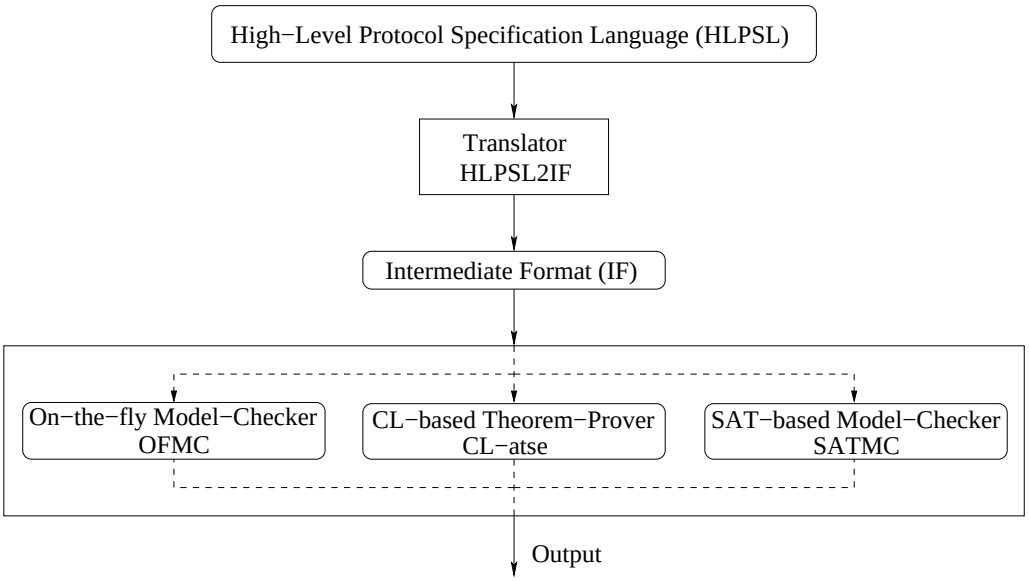

Figure 1: Architecture of the AVISPA Tool

have integrated them in the three state-of-the-art automatic analysis techniques developed by the partners in order to scale their applicability to large-scale security-sensitive protocols. We have implemented these techniques in the three 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.

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

WP6&7 In order to assess the strength of the back-ends of the AVISPA Tool, and to demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols, we have selected a set of candidate protocols currently being drafted by the IETF, along with the security properties these protocols are expected to enjoy. We have thus identified a set of security problems, where a problem is given by both a protocol and a security property the protocol should satisfy. This set, which we call the AVISPA library, contains a total of 384 security problems and 79 protocols, mostly from the IETF, divided into 33 groups.

We use the AVISPA library as the basis for the success criteria for the project. As described in Deliverable 6.1 [8], the following criteria, which refine the ones given in the Technical Annex, are used for the assessment of the AVISPA tool:

Coverage: at least 20 security problems from 5 groups should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 15) of these 20 problems by either verifying that the protocol satisfies the desired security property (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 of the assessment of the AVISPA Tool at month 12 demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 54 problems from 8 groups, and the AVISPA Tool successfully analyses all the 54 problems in a few minutes. All the above requirements (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the tool. Moreover, the tool has been able to detect new (i.e. previously unknown) attacks to some of the protocols analysed. These results give evidence that the project is swiftly advancing the specification and deduction technologies towards the point where industrial-scale, security-sensitive protocols can be specified and automatically analysed.

The activities for the Project Management workpackage (WP1) included the production of a *Project Presentation*, of a *Dissemination and Use Plan*, of the *Consortium Agreement*, and of this *Periodic Progress Report*, as well as the organisation of the *First Evaluation Meeting* and of various internal meetings. All these objectives have been realised successfully: the above documents have all been produced, and we held 5 project meetings with a large number of attendees from all the partners. Moreover, a number of exchange visits took place to address technical issues. 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 creation of the AVISPA Web-Site and the organisation of a project workshop. All these objectives have been realised successfully. Dissemination has followed standard scientific channels: 13 papers have been published in international conferences and journals, 2 PhD theses have been completed, two workshops have been organised, and an invited talk, a scientific talk, and a tutorial were given in the context of major scientific events. In the second year, we plan to continue the dissemination of our results by presenting the AVISPA protocols and problems at the Open Security Area Directorate Meeting (SAAG), by organising a workshop and a tutorial at the Joint International Conference on Automated Reasoning (IJCAR'04), and by continuing to publish our results in international conferences and journals.

We have also initiated dialogue between AVISPA and the Internet Engineering Task Force (IETF). This is particularly important as the large collection of practically relevant,

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

Success criteria at month 12	**Objectives**	**Results**
Coverage	20 problems from 5 groups	54 problems from 8 groups
Effectiveness	15 problems	54 problems
Performance	$<$ 1 hour per problem	all 54 problems in $<$ 8 minutes

security-sensitive, industrial protocols that AVISPA is studying and 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 the security area directors, in particular with the aim of obtaining feedback on the completeness of the list of protocols and the correctness of their security goals (properties).

It is also important to note that the ETHZ and Siemens partners have applied the OFMC back-end to analyse the H.530 protocol of the ITU [42], a protocol developed by Siemens to provide mutual authentication and key agreement in mobile roaming scenarios in multimedia communication. As discussed in detail in [14], OFMC takes only 1.6 seconds to detect a previously unknown attack to H.530. The weakness is serious enough that Siemens has changed the protocol accordingly, and Sebastian Mödersheim of ETHZ participated in the new patent that was recently submitted.

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 first project year has set the basis for the design 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 are:

1. to develop a rich specification language for formalising protocols, security goals, and threat models of industrial complexity;
2. to advance of state-of-the-art in automated deduction techniques to scale up to this complexity;
3. to design and develop a tool, the AVISPA Tool, based on these techniques, which will allow industry and standardisation organisations to automatically validate or detect errors in their products;
4. to tune the AVISPA Tool and demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols;
5. 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 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, and SATMC. Upon termination, each back-end reports whether the input problem was solved (positively or negatively) and displays an attack to the protocol whenever one is found.

Considerable progress has been made during the first year on all these objectives and significant results have been achieved on the following topics. 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 definition of the specification languages HLPSL and IF, as well as to the design and development of the HLPSL2IF translator. This endeavour led us to the following important results:

HLPSL The need to support the specification of practically relevant, industrial protocols led us to a complete redesign of the high-level protocol specification language used in the AVISS project. The HLPSL is now a very expressive language supporting the specification of security-sensitive protocols with a formal semantics based on an expressive first-order temporal logic. The HLPSL is more expressive than other specification languages used for the same purpose such as, e.g., CAPSL [35] and CASPER [46].

IF The IF specification language used in the AVISS project has been extended with a rich type system that supports the specification of sophisticated typed protocol models. Similarly to the HLPSL, the IF is more expressive than alternative specification languages, such as, e.g., CIL [38].

HLPSL2IF A prototype implementation of the HLPSL2IF translator is now available and has been used to carry out the assessment of the AVISPA Tool.

The definition of these specification languages is particularly critical for the project since several, partly conflicting, requirements must be fulfilled:

1. The HLPSL must be expressive enough to support the formal specification of complex, state-of-the-art, security-sensitive Internet protocols, yet it must be simple enough to be used by protocol designers; moreover it must be also automatically translatable into the IF.

2. Protocol specifications in the IF must be automatically analysed by all three back-ends, and thus the IF specification language must be technology-neutral (which also allows for the possible integration of other back-ends in the future).

Considerable effort (both at the technical and at the coordination level) has been spent to address the above issues:

- we anticipated the project kick-off meeting by 2 months in order to identify the difficulties at an early stage and to carefully plan subsequent activities,

- we have formed two task-forces comprising experts from the partners to tackle specific problems: the *translator task-force* and the *modelling task-force*,

- we have scheduled special sessions devoted to the specification languages and the translator in all project meetings, and

- we have conducted numerous discussions by email and by phone.

For WP3, we investigated how to restrict the search space for a problem by introducing assumptions about the possible protocol execution scenarios considered by the analysis tools. When solving a problem, it is often the case that multiple protocol sessions must be considered in parallel in order to discover an attack. We have devised and implemented a

number of techniques to specify (ground or symbolic) parallel protocol session instances in a security problem, and thereby enlarge the class of attacks that can be considered by our tool and speed up their detection.

The relevant deliverables produced during the reporting period are:

- D2.1 – The High-Level Protocol Specification Language [1]
- D2.3 – The Intermediate Format [2]
- D3.3 – Session Instances [3]

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

The scalability of the three 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 three 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.

We have devised a number of new heuristics, optimisations, and reduction and abstraction techniques, both general and specific to the individual back-ends. We have implemented them in the back-ends and carried out experiments to assess their strength. Significant improvements have thus been obtained leading, in some cases, to improvements of several orders of magnitude in the performance of the back-ends [10].

The relevant deliverables produced during the reporting period are:

- D4.2 – Partial-Order Reduction [4]
- D4.3 – Heuristics [5]
- D4.4 – AVISPA Tool v.1 [6]
- D5.1 – Abstractions [7]

2.2.3 Analysis of industrial protocols (WP6&7).

In order to assess the scalability of the back-ends of the AVISPA Tool, and to demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols, we have selected a set of candidate protocols currently being drafted by the IETF, along with the security properties these protocols are expected to enjoy. As a result of this activity, we have identified a set of security problems, where a problem is given by both a protocol

and a security property the protocol should satisfy. This set, which we call the AVISPA library, contains a total of 384 security problems and 79 protocols, mostly from the IETF, divided into 33 groups.

We have also assessed the coverage and relevance of the proposed set of problems, taking into account the comments of IETF representatives. The AVISPA library covers most of the recent and ongoing IETF activities on security and security-sensitive applications, including protocols from practically all IETF areas (not only from the security area) and from all TCP/IP layers.

We use the AVISPA library as the basis for the success criteria for the project. As described in Deliverable 6.1 [8], the following criteria, which refine the ones given in the Technical Annex, are used for the assessment of the AVISPA tool:

Coverage: at least 20 security problems from 5 groups should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 15) of these 20 problems by either verifying that the protocol satisfies the desired security property (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 of the assessment of the AVISPA Tool at month 12 demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 54 problems from 8 groups, and the AVISPA Tool successfully analyses all the 54 problems in a few minutes. All the above requirements (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the tool. Moreover, the tool has been able to detect new (i.e. previously unknown) attacks to some of the protocols analysed.[1] These results give evidence that the project is swiftly advancing the specification and deduction technologies towards the point where industrial-scale, security-sensitive protocols can be specified and automatically analysed.

The relevant deliverables produced during the reporting period are:

- D6.1 – List of Selected Problems [8]
- D7.1 – Experimental Setup [9]
- D7.2 – Assessment of the AVISPA Tool [10]

[1] It is also important to note that the ETHZ and Siemens partners have applied the OFMC back-end to analyse the H.530 protocol of the ITU [42], a protocol developed by Siemens to provide mutual authentication and key agreement in mobile roaming scenarios in multimedia communication. As discussed in detail in [14], OFMC takes only 1.6 seconds to detect a previously unknown attack to H.530. The weakness is serious enough that Siemens has changed the protocol accordingly, and Sebastian Mödersheim of ETHZ participated in the new patent that was recently submitted.

2.2.4 Deviations from the work-plan.

A few, minor changes from the work-plan described in the Technical Annex have been proposed to and agreed upon by the Project Officer:

1. Deliverable 2.1 "Syntax and semantics of new control structures" and Deliverable 2.3 "Syntax and semantics of new data structures" have been renamed to "The High-Level Protocol Specification Language" and "The Intermediate Format Specification Language" respectively. The original objective of these deliverables was the description of the new features of the two specification languages with respect to the languages defined and used in the AVISS project, and the old titles were chosen under the assumption that the specification languages of AVISPA would be obtained by extending those of AVISS. However, the upgrade of the two specification languages has required considerable changes, substantially increasing the expressive power of the languages (as described above), and we thus found it convenient to write self-contained documents describing the two languages from scratch.

2. The delivery date for Deliverable 4.3 "Heuristics" was moved from month 8 to month 11, in order to have more time to formalise the heuristics and carry out experiments during the development of the AVISPA Tool v.1 (Deliverable 4.4, due by month 11).

3. The delivery date for Deliverable 6.1 "List of Selected Problems" was moved from month 10 to month 11. This change allowed us to receive and incorporate feedback on our list of security problems from the Open Security Area Directorate of the IETF in the "Open Security Area Directorate Meeting" during the 58th IETF meeting (Minneapolis, November 9-14, 2003).

4. The delivery date for Deliverable 8.4 "Year 1 Project Workshop Report" has been moved from month 10 to month 13. This was necessary in order to avoid having the 1st Project Workshop being too close to the *Security Protocols Verification (SPV)* workshop organised by Michaël Rusinowitch, the site-leader of the INRIA project partner, at month 9. (See Section 3 for more details.)

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

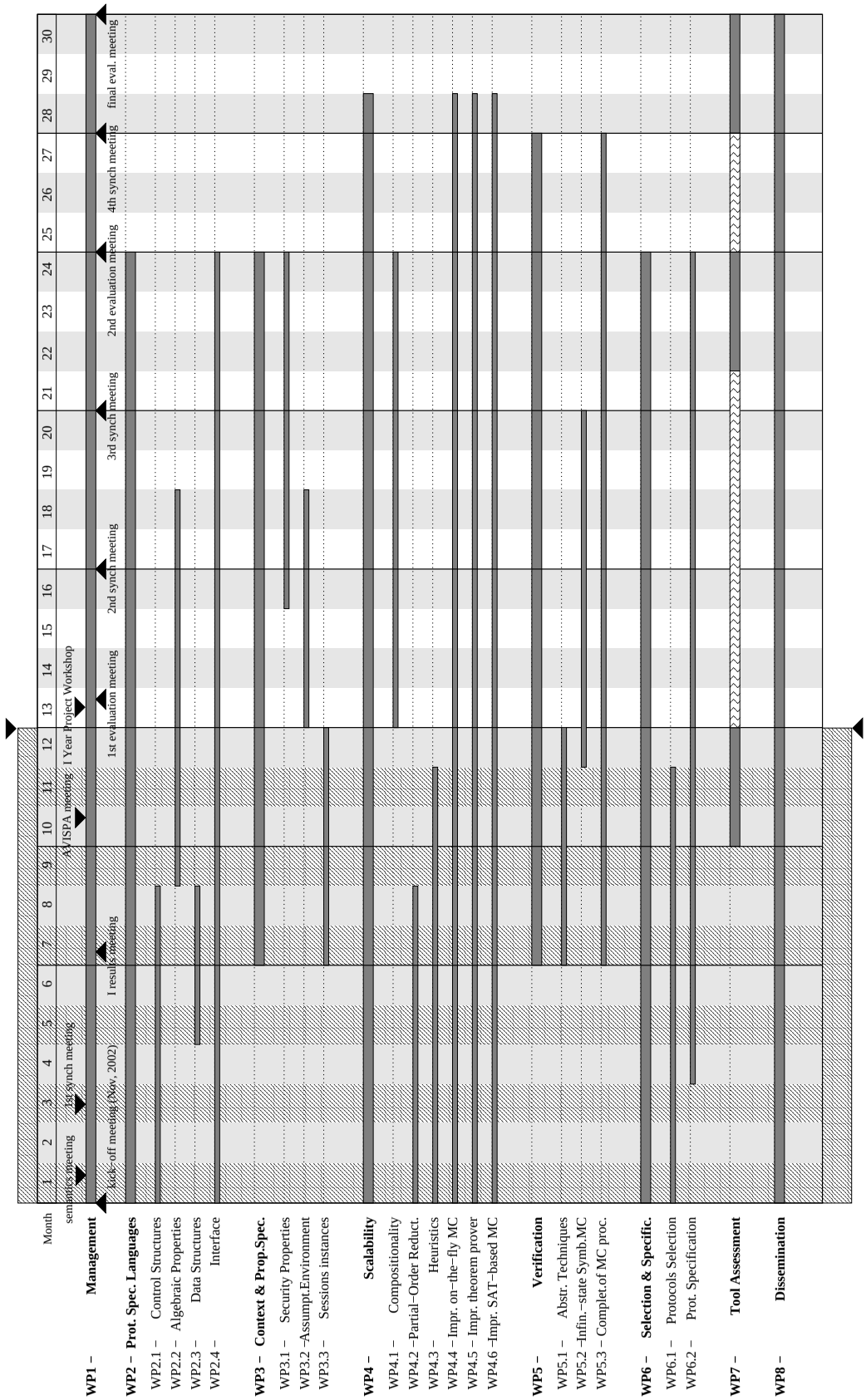

Figure 2: GANTT Chart of the AVISPA Project

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
1.1	1.0	Periodic Progress Report N°: 1	R	Pub.	31.01.2004	12.01.2004
2.1	1.0	The High-Level Protocol Specification Language	R&O	Pub.	31.08.2003	31.08.2003
2.3	1.0	The Intermediate Format	R&O	Pub.	31.08.2003	31.08.2003
3.3	1.0	Session Instances	R&O	Pub.	31.12.2003	12.01.2004
4.2	1.0	Partial-Order Reduction	R&O	Pub.	31.08.2003	31.08.2003
4.3	1.0	Heuristics	R&O	Pub.	30.11.2003	12.12.2003
4.4	1.0	AVISPA Tool v.1	R&O	Pub.	30.11.2003	12.12.2003
5.1	1.0	Abstractions	R&O	Pub.	31.12.2003	12.01.2004
6.1	1.0	List of Selected Problems	R&O	Pub.	30.11.2003	12.12.2003
7.1	1.0	Experimental Setup	S	Pub.	30.11.2003	12.12.2003
7.2	1.0	Assessment of the AVISPA Tool	R	Pub.	31.12.2003	12.01.2004
8.2	1.0	Project Presentation	R	Pub.	31.03.2003	31.03.2003
8.3	1.0	Dissemination and Use Plan	R	Pub.	31.03.2003	31.03.2003

[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°: 1.1
Title: Periodic Progress Report N°: 1
Due date: 31.01.2004
Delivery Date: 12.01.2004

Short Description: This periodic progress report covers the first year 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°: 2.1
Title: The High-Level Protocol Specification Language
Due date: 31.08.2003
Delivery Date: 31.08.2003

Short Description: In this deliverable, we define the syntax and semantics of the High-Level Protocol Specification Language (HLPSL) that we employ for specifying protocols and their properties with the AVISPA Tool.
HLPSL is an expressive language for modelling communication and security protocols, which draws its semantic roots from Lamport's Temporal Logic of Actions (TLA [44]). TLA is an elegant and powerful language which lends itself well to specifying concurrent systems (see, e.g., [45]) precisely like the types of protocols we seek to model. Syntactically, however, specifying protocols in a raw logic can be a daunting task. Moreover, the domain of protocol analysis calls for several syntactic constructs (such as message structure) and semantic concepts (like the notion of an intruder) that are problem-independent and arise in every model. The development of HLPSL has taken this objectives into account:

- HLPSL provides a convenient, human readable, and easy to use language, yet powerful enough to support the specification of modern Internet protocols. To this end, HLPSL has been defined in such a way as to closely resemble a language for defining guarded transitions within a state-transition system, and is equipped with constructs that allow for the modular specification of protocols.
- HLPSL has a formal semantics: HLPSL is based on Lamport's TLA and its semantics is given by a translation to a subset of TLA.
- HLPSL is amenable to automated formal analysis. This is achieved by an automatic translation of HLPSL into the Intermediate Format (IF [2]).

Partners owning: INRIA
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°: 2.3
Title: The Intermediate Format
Due date: 31.08.2003
Delivery Date: 31.08.2003

Short Description: This deliverable introduces the Intermediate Format (IF), a tool-independent, low-level protocol specification language suitable for automated deduction. Specifications of security protocols and properties written in the High-Level Protocol Specification Language (HLPSL) are automatically translated in IF specifications, which are then given as input to the different back-ends that constitute the AVISPA Tool.
We defined a preliminary version of the IF as part of the AVISS project ("AVISS: Automated Verification of Infinite State Systems", FET-Open Project IST-2000-26410 [28, 29]). Since then, in order to be able to analyse the Internet security protocols and applications that we have been considering in the AVISPA project, we have completely redesigned the language. The most important new concept is the extension of the left-hand side of rules with conditions and negative facts, in order to allow for the explicit modelling of a wider class of protocols and properties in a natural way.

Partners owning: INRIA
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°: 3.3
Title: Session Instances
Due date: 31.12.2003
Delivery Date: 12.01.2004

Short Description: We model each honest agent as a process that can participate in an unbounded number of parallel *sessions*, i.e. executions of a given protocol, playing in any of the roles. When analysing a problem (i.e. a protocol specification paired with a security property that the protocol is intended to ensure), it is often the case that multiple protocol sessions must be considered in parallel in order to discover an attack.
In this deliverable, we describe different techniques that we have devised to specify such parallel sessions in a security problem. We begin by describing techniques for automatically generating ground session instances, based on a protocol specification and a desired number of sessions to be run in parallel. We also discuss methods for identifying and filtering out redundant and uninteresting sessions. We have implemented these ideas in a HLPSL preprocessor called ASG (Automatic Session Generator) which is also presented.
Finally, we introduce the notion of *symbolic sessions*, i.e. sessions in which protocol parameters are left as uninstantiated variables (this is in contrast to ground sessions, in which all protocol variables are instantiated with concrete values). This technique exploits the lazy intruder to search for satisfying assignments of protocol variables that will lead to attacks.

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°: 4.2
Title: Partial-Order Reduction
Due date: 31.08.2003
Delivery Date: 31.08.2003

Short Description: This deliverable reports on research carried out on *partial-order reduction (POR)*, a technique that has proved to be very successful in explicit state model-checking. POR is based on the observation that different interleavings of actions can be ignored if they result in equivalent successor states, and reducing the number of traces considered this way can dramatically reduce the search.
More specifically, we here introduce *constraint differentiation*, a new technique for reducing search when model-checking security protocols. Our technique is based on eliminating certain kinds of redundancies that arise in the search space when using symbolic exploration methods, in particular methods that employ constraints to represent and manipulate possible messages from an active intruder. Formally, we prove that constraint differentiation terminates and is correct and complete, in that it preserves the set of reachable states so that all state-based properties holding before reduction (such as the existence of an attack) hold after reduction. Practically, we have integrated this technique into the AVISPA-tool back-end OFMC and demonstrated its effectiveness by extensive experimentation. Our results show that constraint differentiation substantially reduces search and considerably improves the performance of OFMC, enabling its application to a wider class of problems. As a concrete example we consider in detail the analysis of the industrial protocol-suite IKE.
Constraint differentiation is independent of the technical and conceptual details of the various lazy intruder approaches and underlying protocol models, and can thus be adopted in other lazy intruder approaches. The SATMC back-end is not based on the lazy intruder, and hence will not exploit constraint differentiation, but nonetheless, like OFMC and CL-atse, SATMC successfully exploits a simple form of partial-order reduction that we call *step-compression*, and that is applied also in other approaches such as [27, 33, 37, 48].
Moreover, SATMC exploits an own, simple form of POR, which we also briefly describe in this deliverable: the model underlying SATMC is based on a declarative encoding into propositional logic which allows for a parallel execution of transitions, implicitly considering all possible sequential interleavings thereof without enumerating them.

Partners owning: ETHZ
Partners contributed: UNIGE
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°: 4.3
Title: Heuristics
Due date: 30.11.2003
Delivery Date: 12.12.2003

Short Description: A heuristics refers to a problem-solving procedure about which one cannot make formally verifiable statements regarding completeness and/or running time, but which, in practice, is often complete and efficient for many cases. In this deliverable, we investigate heuristics that speed up the search for attacks on security protocols.
We present here a collection of heuristics that substantially reduce search and improve the performance of the back-ends of the AVISPA tool. We also identify different classes of heuristics that are applicable to the problem of protocol analysis. Some, like the session compilation heuristics, can be applied at compile time, yielding a heuristically-modified IF specification. Others, like the "constraining rule variables" heuristics, are problem-specific and applicable during the search for attacks. These are particular to the problem of protocol falsification and may also depend on the model used in a specific back-end to the AVISPA tool. In still other cases, we can apply generic search heuristics by adapting them to our problem domain. In this deliverable, we discuss the application of one such standard search heuristic, A* [41], and its adaptation to the problem of protocol analysis.

Partners owning: ETHZ
Partners contributed: UNIGE
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°: 4.4
Title: AVISPA Tool v.1
Due date: 30.11.2003
Delivery Date: 12.12.2003

Short Description: This deliverable describes the AVISPA Tool version 1, the architecture of which is illustrated in Figure 1. Specifications of security protocols and properties written in the High-Level Protocol Specification Language (HLPSL [1]) are automatically translated (by the translator HLPSL2IF) into IF [2] specifications, which are then given as input to the different back-ends of the AVISPA Tool: OFMC, CL-atse, and SATMC. Upon termination, each back-end of the AVISPA Tool outputs the result of its analysis using a common output format, which is introduced in this deliverable. The output states whether the input problem was solved (positively or negatively), some of the system resources were exhausted, or the problem was not tackled by the required back-end for some reason.

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°: 5.1
Title: Abstractions
Due date: 31.12.2003
Delivery Date: 12.01.2004

Short Description: For automatic protocol verification to become feasible, it is often needed to abstract away from specification details or to introduce finite or regular descriptions for infinite sets of data. Abstractions in our protocol verification context are mappings from the original rewrite rules model into a simpler model such that every protocol flaw (of the original model) is contained in the abstract model. The converse usually does not hold, since, due to the simplification, we may have false positives in the abstract model even when the original model is flawless. In this deliverable, we present a number of different abstractions that we have considered in our protocol analysis tools. More specifically, we present abstractions of the nonces and of the intruder knowledge, which have been developed and implemented by the AVISPA group at INRIA, as well as a general approach for designing abstractions, which has been formalised by the group at ETHZ.

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°: 6.1
Title: List of Selected Problems
Due date: 30.11.2003
Delivery Date: 12.12.2003

Short Description: This deliverable contains the list of candidate protocols and problems for AVISPA. A problem is given by both a protocol and a security property the protocol should satisfy. (A protocol and a set of properties is a multiple problem.) Our list contains a total of 384 security problems and 79 protocols, mostly from the IETF, divided into 33 groups. This document also assesses the coverage of the proposed set of protocols, having taken into account the initial comments of IETF representatives.
Our list of protocols covers most of the recent and ongoing IETF activities on security and security-sensitive applications, including protocols from practically all IETF areas (not only from the security area) and from all TCP/IP layers. In specifying the IETF protocols and their associated problems, we expect that in many cases there will be a need to discuss the protocols with their developers in order to properly interpret the intended meaning of the (proposed) standards and to obtain the abstractions and simplifications required. Some of these may be necessary to deal with the limitations of our tools (e.g., with respect to the number of concurrent sessions, or agents, or on some data types), and some because certain features of the protocol (such as the cipher suites used, techniques for negotiating them, policy issues, or strength against some denial of service attacks) will be outside the scope of our analysis. Besides this, most of the IETF protocols are not written in a language that is readily translatable to a formal specification and the desired security properties are often not explicitly stated in the original documents describing the protocols. These discussions will be conducted in continuation of the process initiated in this deliverable and the proposed properties may be revised after further feedback from the IETF or other organisations.

Partners owning: Siemens
Partners contributed:
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°: 7.1
Title: Experimental Setup
Due date: 30.11.2003
Delivery Date: 12.12.2003

Short Description: the Experimental Setup is a collection of scripts written in the Unix language PERL, by means of which it is possible to automatically run the AVISPA Tool on a set of security problems, written in the High-Level Protocol Specification Language (HLPSL). The scripts first compile the HLPSL specifications to Intermediate Format (IF), and then feed the resulting IF specifications to the three AVISPA back-ends. Resource limits are imposed, usually 1 hour CPU time and 1GB memory, and timings and other relevant statistics are automatically collected after each problem has been solved (or not) by each back-end.

Partners owning: UNIGE
Partners contributed:
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°: 7.2
Title: Assessment of the AVISPA Tool
Due date: 31.12.2003
Delivery Date: 12.01.2004

Short Description: In this deliverable, we report on the assessment of the AVISPA Tool at project month 12. The results of the assessment demonstrate the success of our work in the reporting period. We have been able to formalise in the HLPSL 54 problems from 8 groups, and the AVISPA Tool successfully analyses all the 54 problems in a few minutes. All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the tool. Moreover, the tool has been able to detect new (i.e. previously unknown) attacks to some of the protocols analysed. These results give evidence that the project is swiftly advancing the specification and deduction technologies towards the point where industrial-scale, security-sensitive protocols can be specified and automatically 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°: 8.2
Title: Project Presentation
Due date: 31.03.2003
Delivery Date: 31.03.2003

Short Description: The Project Presentation is a short description of the project objectives, approach, and expected results, as well as the participants in the project. It is used by the Commission to provide information about the project. This deliverable consists of a written document and a slide presentation.

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°: 8.3
Title: Dissemination and Use Plan
Due date: 31.03.2003
Delivery Date: 31.03.2003

Short Description: This document describes the plans for the dissemination of knowledge during the project as well as tentative exploitation plans. The scientific advances made by the AVISPA project in modelling and validating Internet security-sensitive protocols are expected to have strong potential commercial and industrial exploitation as they can significantly contribute to the rigorous quality assurance and establishment of trust in the core protocols of a broad spectrum of application areas in current and future communication technology. The tool resulting from the AVISPA project, as well as reports on the protocol analysis performed during the project, will be made available to protocol designers and will be presented to the IETF and other standardisation bodies. We believe that the tool and accompanying methodology will help the standardisation organisations develop robust, correctly functioning, secure protocols for the Internet.

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

2.5 Comparison of planned activities and actual work accomplished

The activity within the project largely proceeded as planned in the Technical Annex. As a consequence only a few, minor changes turned out to be necessary: in some cases we found it appropriate to anticipate some of the work originally planned for the second year, in other cases we found it convenient to postpone it. 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.

Table 3: Effort in person months for reporting period 01.01.2003 — 31.12.2003

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

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**	**1**	**12**	**4,0**	**4,0**
Task 1.1	10,0	1	30	1	12	2,0	2,0
Task 1.2	3,0	1	30	1	12	1,0	1,0
Task 1.3	2,0	1	30	1	12	1,0	1,0
WP2	**11,0**	**1**	**24**	**1**	**12**	**4,0**	**4,0**
WP 2.1	4,0	1	8	1	12	1,5	1,5
WP 2.2	4,0	9	18	9	12	1,0	1,0
WP 2.3	3,0	5	8	5	12	1,5	1,5
WP 2.4	-	1	24	1	12	-	-
WP3	**12,0**	**7**	**24**	**7**	**12**	**2,0**	**2,0**
WP 3.1	5,0	16	24	16	12	-	-
WP 3.2	5,0	13	18	13	12	-	-
WP 3.3	2,0	7	12	7	12	2,0	2,0
WP4	**17,0**	**1**	**28**	**1**	**12**	**6,4**	**6,4**
WP 4.1	4,0	13	24	13	12	-	-
WP 4.2	-	1	8	1	12	-	-
WP 4.3	1,0	1	8	1	12	0,6	0,6
WP 4.4	-	1	28	1	12	-	-
WP 4.5	-	1	28	1	12	-	-
WP 4.6	12,0	1	28	1	12	5,8	5,8
WP5	**9,0**	**7**	**27**	**7**	**12**	**2,0**	**2,0**
WP 5.1	3,0	7	12	7	12	-	-
WP 5.2	1,0	12	20	12	12	2,0	2,0
WP 5.3	5,0	7	27	7	12	-	-
WP6	**4,0**	**1**	**24**	**1**	**12**	**1,0**	**1,0**
Task 6.1	-	1	10	1	11	-	-
Task 6.2	4,0	4	24	4	12	1,0	1,0
WP7	**2,0**	**10**	**30**	**10**	**12**	**1,0**	**1,0**
Task 7.1	0,6	10	11	10	11	0,6	0,6
Task 7.2	1,0	11	30	11	12	0,4	0,4
Task 7.3	0,4	11	30	11	12	-	-
WP8	**4,0**	**1**	**30**	**1**	**12**	**2,0**	**2,0**
Task 8.1	1,0	1	30	1	12	0,5	0,5
Task 8.2	0,8	6	30	6	12	0,3	0,3
Task 8.3	0,4	1	30	1	12	0,2	0,2
Task 8.4	1,8	1	30	1	12	1,0	1,0
	74,0					**22,4**	**22,4**
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 • Setup and maintenance of concurrent versioning system for distributed management of software and documentation
Task 1.2	• Organisation of the Kick-off meeting • Organisation of Month 12 Synchronisation Meeting
Task 1.3	• Budgetary overviews • Management of cost statements
WP2	
WP 2.1	• Formal definition of the syntax of the IF • Procedural abstraction in the HLPSL
WP 2.2	• Addition of axioms in the specification languages
WP 2.3	• Definition of the type system of the IF
WP 2.4	• Formal definition of the Output Format
WP3	
WP 3.1	
WP 3.2	
WP 3.3	• Implementation of the automatic of the ground session instances generator
WP4	
WP 4.1	
WP 4.2	
WP 4.3	• Definition of and experimentation with the *Constraining Rule Variables* heuristics
WP 4.4	
WP 4.5	
WP 4.6	• Design and implementation of the Abstraction/Check/Refine Loop in SATMC • Implementation of the Graphplan-based encodings in SATMC
WP5	
WP 5.1	
WP 5.2	• Model-checking of time-sensitive security protocols
WP 5.3	
WP6	
Task 6.1	
Task 6.2	• Formal specification of a first set of selected problems
WP7	
Task 7.1	• Implementation of the experimental setup
Task 7.2	• Assessment of the AVISPA Tool v.1
Task 7.3	• Comparative analysis of the back-ends
WP8	
Task 8.1	• Setup and management of the project web-site `www.avispa-project.org`
Task 8.2	• Organisation of the 1st Year Project Workshop
Task 8.3	• Preparation of the Project Presentation • Preparation of the Technology and Implementation Plan
Task 8.4	• Writing of scientific publications

Deliverables due this period		
Number	**Title**	**Status**
D1.1	Periodic Progress Report N°: 1	Final
D7.1	Experimental Setup	Final
D7.2	Assessment of AVISPA Tool v.1	Final
D8.2	Project Presentation	Final
D8.3	Dissemination and Use Plan	Final

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

1. P. Ammirati and G. Delzanno. Constraint-based Automatic Verification of Time Dependent Security Properties. In *Proceedings of SPV'03*, 2003. Available at `www.avispa-project.org`
2. A. Armando and L. Compagna. Abstraction-driven SAT-based Analysis of Security Protocols. In *Proceedings of SAT 2003*, LNCS 2919. Springer-Verlag, 2003. Available at `www.avispa-project.org`.
3. A. Armando, L. Compagna and P. Ganty. SAT-based Model-Checking of Security Protocols using Planning Graph Analysis. In K. Araki, S. Gnesi, and D. Mandrioli, editors, *Proceedings of the 12th International Symposium of Formal Methods Europe (FME'03)*, LNCS 2805, pages 875–893. Springer-Verlag, 2003. Available at `www.avispa-project.org`.
4. G. Delzanno and P. Ganty. Symbolic Methods for Automatically Proving Secrecy and Authentication in Infinite-state Models of Cryptographic Protocols. In *Proceedings of the Workshop on Issues in Security and Petri Nets (WISP'03)*, 2003. Available at `www.avispa-project.org`.
5. G. Delzanno and P. Ganty. Automatic Verification of Time Sensitive Cryptographic Protocols. In *Proceedings of TACAS'04*, 2004. Available at `www.avispa-project.org`.

Planned actions for the next period

- Completeness results for SATMC.
- Development of abstraction techniques.
- Design and development of domain specific encodings for SATMC.
- Formalisation of selected problems in HLPSL.
- Development of AVISPA Tool v.2.
- Assessment of AVISPA Tool v.2.
- Organisation of the 2nd Year Project Workshop (the workshop "Automated Reasoning for Security Protocols Analysis", ARSPA, which will be held in Cork (Ireland), on July 4th, 2004, in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR'04) (`http://www.4c.ucc.ie/ijcar/`).
- Scientific publications and dissemination of results.

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**	**1**	**12**	**0,4**	**0,4**
Task 1.1	**-**	1	30	1	12	**-**	-
Task 1.2	**1,0**	1	30	1	12	**0,4**	0,4
Task 1.3	**-**	1	30	1	12	**-**	-
WP2	**22,0**	**1**	**24**	**1**	**12**	**10,0**	**10,0**
WP 2.1	**8,0**	1	8	1	12	**8,0**	8,0
WP 2.2	**5,0**	9	18	9	12	**1,0**	1,0
WP 2.3	**3,0**	5	8	5	12	**1,0**	1,0
WP 2.4	**6,0**	1	24	1	12	**-**	-
WP3	**15,0**	**7**	**24**	**7**	**12**	**-**	**-**
WP 3.1	**8,0**	16	24	16	12	**-**	-
WP 3.2	**7,0**	13	18	13	12	**-**	-
WP 3.3	**-**	7	12	7	12	**-**	-
WP4	**6,0**	**1**	**28**	**1**	**12**	**2,0**	**2,0**
WP 4.1	**-**	13	24	13	12	**-**	-
WP 4.2	**-**	1	8	1	12	**-**	-
WP 4.3	**1,0**	1	8	1	12	**1,0**	1,0
WP 4.4	**-**	1	28	1	12	**-**	-
WP 4.5	**5,0**	1	28	1	12	**1,0**	1,0
WP 4.6	**-**	1	28	1	12	**-**	-
WP5	**8,0**	**7**	**27**	**7**	**12**	**3,0**	**3,0**
WP 5.1	**2,0**	7	12	7	12	**2,0**	2,0
WP 5.2	**3,0**	12	20	12	12	**0,5**	0,5
WP 5.3	**3,0**	7	27	7	12	**0,5**	0,5
WP6	**2,0**	**1**	**24**	**1**	**12**	**0,2**	**0,2**
Task 6.1	**-**	1	10	1	11	**-**	-
Task 6.2	**2,0**	4	24	4	12	**0,2**	0,2
WP7	**2,0**	**10**	**30**	**10**	**12**	**0,3**	**0,3**
Task 7.1	**-**	10	11	10	11	**-**	-
Task 7.2	**1,0**	11	30	11	12	**0,3**	0,3
Task 7.3	**1,0**	11	30	11	12	**-**	-
WP8	**4,0**	**1**	**30**	**1**	**12**	**1,4**	**1,4**
Task 8.1	**-**	1	30	1	12	**-**	-
Task 8.2	**1,0**	6	30	6	12	**0,4**	0,4
Task 8.3	**-**	1	30	1	12	**-**	-
Task 8.4	**3,0**	1	30	1	12	**1,0**	1,0
	60,0					**17,3**	**17,3**
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	• Formal definition of the HLPSL and of the IF • Implementation of the HLPSL2IF translator
WP 2.2	• Addition of axioms in the specification languages
WP 2.3	• Definition of the syntax and semantics of the IF
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	• Design and implementation of CL-atse
WP 4.6	
WP5	
WP 5.1	• Formal definition of abstraction techniques; implementation of Is2TiF
WP 5.2	
WP 5.3	
WP6	
Task 6.1	
Task 6.2	• Formal specification of a first set of selected problems
WP7	
Task 7.1	
Task 7.2	• Preparation of the assessment of AVISPA Tool v.1
Task 7.3	
WP8	
Task 8.1	
Task 8.2	• Organisation of the 1st Year Project Workshop
Task 8.3	
Task 8.4	• Writing of scientific publications

Deliverables due this period		
Number	**Title**	**Status**
D2.1	The High-Level Protocol Specification Language	Final
D2.3	The Intermediate Format	Final
D5.1	Abstractions	Final

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

1. Y. Chevalier, Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques. Thèse de doctorat, Université Henri Poincaré, Nancy, December 2003.
2. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents. In Proceedings of the Foundations of Software Technology and Theoretical Computer Science, FST TCS'03, LNCS 2914. Springer-Verlag, 2003. Available at `www.avispa-project.org`
3. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. In Proceedings of the Logic In Computer Science Conference (LICS'03), pages 261-270. IEEE Computer Press, 2003. Available at `www.avispa-project.org`
4. Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions. In M. Baaz, editor, Proceedings of CSL'03, LNCS 2803. Springer-Verlag, 2003. Available at `www.avispa-project.org`
5. M. Rusinowitch. Automated Analysis of Security Protocols. In G. Vidal, editor, Proceedings of the 12th International Workshop on Functional and (Constraint) Logic Programming (WFLP'03). Electronic Notes in Theoretical Computer Science 86(3), 2003. Available at `www.avispa-project.org`
6. M. Rusinowitch. Organisation of the Workshop on Security Protocols Verification, September 6, 2003. Marseille. `http://www.loria.fr/~rusi/spv.html`
7. M. Rusinowitch and M. Turuani. Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete. Theoretical Computer Science, 299:451-475, 2003. Available at `www.avispa-project.org`
8. M. Turuani, Sécurité des Protocoles Cryptographiques: Décidabilité et Complexité. Thèse de doctorat, Université Henri Poincaré, Nancy, December 2003.

Planned actions for the next period

- Improvement of CL-atse for a better consideration of algebraic properties.
- Design of a more complete graphical interface for a better use of the AVISPA Tool v.2.
- Formal definition and implementation of new goals.
- Complete integration of the tree automata abstraction in the AVISPA Tool.
- Scientific publications and dissemination of results.

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**	**1**	**12**	**0,4**	**0,4**
Task 1.1	**-**	1	30	1	12	**-**	-
Task 1.2	**1,0**	1	30	1	12	**0,4**	0,4
Task 1.3	**-**	1	30	1	12	**-**	-
WP2	**13,0**	**1**	**24**	**1**	**12**	**8,0**	**8,0**
WP 2.1	**3,0**	1	8	1	12	**3,0**	3,0
WP 2.2	**5,0**	9	18	9	12	**2,0**	2,0
WP 2.3	**3,0**	5	8	5	12	**3,0**	3,0
WP 2.4	**2,0**	1	24	1	12	**-**	-
WP3	**15,0**	**7**	**24**	**7**	**12**	**4,0**	**4,0**
WP 3.1	**6,0**	16	24	16	12	**-**	-
WP 3.2	**5,0**	13	18	13	12	**-**	-
WP 3.3	**4,0**	7	12	7	12	**4,0**	4,0
WP4	**17,0**	**1**	**28**	**1**	**12**	**9,0**	**9,0**
WP 4.1	**4,0**	13	24	13	12	**-**	-
WP 4.2	**4,0**	1	8	1	12	**4,0**	4,0
WP 4.3	**4,0**	1	8	1	12	**3,0**	3,0
WP 4.4	**5,0**	1	28	1	12	**2,0**	2,0
WP 4.5	**-**	1	28	1	12	**-**	-
WP 4.6	**-**	1	28	1	12	**-**	-
WP5	**8,0**	**7**	**27**	**7**	**12**	**3,0**	**3,0**
WP 5.1	**3,0**	7	12	7	12	**3,0**	3,0
WP 5.2	**3,0**	12	20	12	12	**-**	-
WP 5.3	**2,0**	7	27	7	12	**-**	-
WP6	**4,0**	**1**	**24**	**1**	**12**	**2,0**	**2,0**
Task 6.1	**-**	1	10	1	11	**-**	-
Task 6.2	**4,0**	4	24	4	12	**2,0**	2,0
WP7	**2,0**	**10**	**30**	**10**	**12**	**0,4**	**0,4**
Task 7.1	**-**	10	11	10	11	**-**	-
Task 7.2	**1,0**	11	30	11	12	**0,4**	0,4
Task 7.3	**1,0**	11	30	11	12	**-**	-
WP8	**4,0**	**1**	**30**	**1**	**12**	**1,4**	**1,4**
Task 8.1	**-**	1	30	1	12	**-**	-
Task 8.2	**1,0**	6	30	6	12	**0,4**	0,4
Task 8.3	**-**	1	30	1	12	**-**	-
Task 8.4	**3,0**	1	30	1	12	**1,0**	1,0
	64,0					**28,2**	**28,2**
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 • Organisation of the first AVISPA synchronisation meeting (13–14.03.2003) • Organisation of the AVISPA Meeting on the HLPSL2IF translator (21-23.10.2003)
WP2	
WP 2.1	• Formal definition of the syntax and semantics of the HLPSL
WP 2.2	
WP 2.3	• Formal definition of the syntax and semantics of the IF • Extension with negation, inequalities, conditions, and sets to support advanced protocols.
WP 2.4	
WP3	
WP 3.1	• Reduction of standard security goals to authentication and secrecy
WP 3.2	
WP 3.3	• Design and first experimentation with symbolic sessions
WP4	
WP 4.1	
WP 4.2	• Constraint differentiation as a POR-inspired technique for the symbolic approach • Formalisation of the technique and completeness proof with respect to the standard model • Implementation of the technique in the OFMC-core module
WP 4.3	• Search heuristics framework • Session compilation
WP 4.4	• Extension and improvement of the OFMC back-end (in particular, the OFMC-core module)
WP 4.5	
WP 4.6	
WP5	
WP 5.1	• Formal definition of the abstraction techniques • Formal comparison and relation with other abstract and alternative protocol models • Preliminary implementation of OFMC/FP, the new verification module of OFMC for an unbounded number of sessions
WP 5.2	• Symbolic representation of agents
WP 5.3	
WP6	
Task 6.1	
Task 6.2	• Formal specification of a first set of selected problems
WP7	
Task 7.1	
Task 7.2	• Assessment of the AVISPA Tool v.1
Task 7.3	
WP8	
Task 8.1	
Task 8.2	
Task 8.3	
Task 8.4	• Writing of scientific publications

Deliverables due this period		
Number	**Title**	**Status**
D3.3	Session Instances	Final
D4.2	Partial-Order Reduction	Final
D4.3	Heuristics	Final
D4.4	AVISPA Tool v.1	Final

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

1. D. Basin, S. Mödersheim, and L. Viganò. An On-The-Fly Model-Checker for Security Protocol Analysis. In E. Snekkenes and D. Gollmann, editors, *Proceedings of ESORICS'03*, LNCS 2808, pages 253–270. Springer-Verlag, 2003. Available at `www.avispa-project.org`
2. D. Basin, S. Mödersheim, and L. Viganò. Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols. In V. Atluri and P. Liu, editors, *Proceedings of CCS'03*, pages 335–344. ACM Press, 2003. Available at `www.avispa-project.org`
3. D. Basin, S. Mödersheim, and L. Viganò. Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols (Extended Abstract). In *Proceedings of SPV'03*, 2003. Available at `www.avispa-project.org`
4. Talk on the OFMC back-end and the AVISPA project at the Dagstuhl Seminar on Language-Based Security. Dagstuhl, Germany, 5th – 10th October, 2003.

Planned actions for the next period

- Extension of the OFMC/FP module for the analysis of infinite numbers of sessions.
- Extension of both protocol specification languages and of the back-ends for supporting more advanced protocols, including algebraic properties, complex data-structures and alternative intruder models.
- Support to compositional reasoning.
- Techniques for infinite-state symbolic model-checking.
- Extension of the preliminary unification algorithm in OFMC.
- Formalisation of selected problems in HLPSL.
- Development of the AVISPA Tool v.2.
- Assessment of the AVISPA Tool v.2.
- Organisation of the 2nd Year Project Workshop (the workshop "Automated Reasoning for Security Protocols Analysis", ARSPA, which will be held in Cork (Ireland), on July 4th, 2004, in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR'04) (`http://www.4c.ucc.ie/ijcar/`).
- Scientific publications and dissemination of results.

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**	**1**	**12**	**0,4**	**0,4**
Task 1.1	**-**	1	30	1	12	-	-
Task 1.2	**1,0**	1	30	1	12	0,4	0,4
Task 1.3	**-**	1	30	1	12	-	-
WP2	**2,0**	**1**	**24**	**1**	**12**	**2,8**	**2,8**
WP 2.1	**1,0**	1	8	1	12	2,0	2,0
WP 2.2	**0,5**	9	18	9	12	0,3	0,3
WP 2.3	**0,5**	5	8	5	12	0,5	0,5
WP 2.4	**-**	1	24	1	12	-	-
WP3	**7,0**	**7**	**24**	**7**	**12**	**1,0**	**1,0**
WP 3.1	**4,0**	16	24	16	12	-	-
WP 3.2	**2,5**	13	18	13	12	1,0	1,0
WP 3.3	**0,5**	7	12	7	12	-	-
WP4	**-**	**1**	**28**	**1**	**12**	**-**	**-**
WP 4.1	**-**	13	24	13	12	-	-
WP 4.2	**-**	1	8	1	12	-	-
WP 4.3	**-**	1	8	1	12	-	-
WP 4.4	**-**	1	28	1	12	-	-
WP 4.5	**-**	1	28	1	12	-	-
WP 4.6	**-**	1	28	1	12	-	-
WP5	**3,0**	**7**	**27**	**7**	**12**	**-**	**-**
WP 5.1	**1,5**	7	12	7	12	-	-
WP 5.2	**1,5**	12	20	12	12	-	-
WP 5.3	**-**	7	27	7	12	-	-
WP6	**18,0**	**1**	**24**	**1**	**12**	**9,0**	**9,0**
Task 6.1	**6,0**	1	10	1	11	3,0	3,0
Task 6.2	**12,0**	4	24	4	12	6,0	6,0
WP7	**2,0**	**10**	**30**	**10**	**12**	**-**	**-**
Task 7.1	**-**	10	11	10	11	-	-
Task 7.2	**2,0**	11	30	11	12	-	-
Task 7.3	**-**	11	30	11	12	-	-
WP8	**3,0**	**1**	**30**	**1**	**12**	**1,2**	**1,2**
Task 8.1	**-**	1	30	1	12	-	-
Task 8.2	**1,5**	6	30	6	12	0,5	0,5
Task 8.3	**0,5**	1	30	1	12	0,2	0,2
Task 8.4	**1,0**	1	30	1	12	0,5	0,5
	36,0					**14,4**	**14,4**
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
Task 1.3	
WP2	
WP 2.1	• Formal definition of syntax and semantics of HLPSL
WP 2.2	• Preliminary study of translation of HLPSL into rules
WP 2.3	• Syntax for messages with complex structure
WP 2.4	
WP3	
WP 3.1	
WP 3.2	• Preliminary study on assumptions on environment
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	• Selection of candidate problems
Task 6.2	• Formal specification of a first set of selected problems
WP7	
Task 7.1	
Task 7.2	
Task 7.3	
WP8	
Task 8.1	
Task 8.2	• Participation in IETF Meetings
Task 8.3	• Preparation of the Technology and Implementation Plan
Task 8.4	• Project presentations, tutorials

Deliverables due this period		
Number	**Title**	**Status**
D6.1	List of selected problems	Final

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

1. Full day tutorial at the International Conference on Software Engineering And Formal Methods (SEFM 2003, Brisbane, Australia, 22nd - 27th September, 2003). Available at `www.svrc.uq.edu.au/Events/SEFM03` and `www.avispa-project.org`
2. Invited talk at the Industrial Day of the Formal Methods Europe Conference (FME 2003): Specifying and Verifying real-world Security Protocols. Available at `fme03.isti.cnr.it/iday-progr.htm` and `www.avispa-project.org`

Planned actions for the next period

- Update the list of protocols and properties, according to the discussions with the IETF the completeness of the list and the correctness of their security goals (properties).
- Formalisation of selected problems in HLPSL.
- Formalisation of resistance against Denial of Service (DoS) attacks in HLPSL.
- Verification of resistance against Denial of Service (DoS) attacks.
- Presentation at the IETF, Open Security Area Directorate Meeting (SAAG) in Seoul, 4th March 2004. `http://www.ietf.org/meetings/IETF-59.html`
- Scientific publications and presentations, and dissemination of results.

2.6 State-of-the-art update

There has been considerable activity in the scientific community dedicated to security protocol verification in 2003, as is testified by the large number of publications in conferences and workshops related to the domain. We address here only the most representative advanced, or concerted, efforts, which are significantly related to the AVISPA project, e.g. [31, 32, 34, 36]. For instance, [36] is a recent advance on the security verification problems showing that it is possible to reduce such problems to the case where only two agents are involved in the protocols.

2.6.1 The Projects EVA and PROUVE

The tool platform EVA has been developed for cryptographic protocols in the context of the French RNTL project EVA [40], by the two research laboratories LSV (ENS de Cachan, France) and Verimag (Grenoble, France) and the industrial partner Trusted Logic (France). Like for the AVISPA Tool, the EVA platform uses both a high-level specification language close to the language used in textbooks and a low-level specification language, used by the protocol analysers; an automatic translation from the high-level to the low-level language is also provided. Two tools are currently connected to the platform: Securify (LSV) and Hermes (Verimag) [34]. These tools are designed for verifying secrecy properties for an unbounded number of sessions, in order to *prove* properties on protocols. They have been successfully applied to (i.e. they construct secrecy proofs) for about 15 protocols of the Clark/Jacob library. (They can be used on-line at: `http://www-eva.imag.fr/`.) 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. In addition, only secrecy properties are considered by these tools, in contrast to our AVISPA Tool.

The project EVA ended in December 2003. A follow-up project PROUVE has been approved and INRIA-Lorraine is a partner of this project (administrative coordinator), as well as France Telecom R&D. We expect collaboration between AVISPA and PROUVE: although the specification languages, as well as the case-studies, are different, we believe that some back-end technologies can be shared.

Action taken We have invited Yassine Lakhnech, leader of EVA at Verimag, to present their results at the AVISPA workshop that will be held on January 23, 2004, in Nancy.

2.6.2 Blanchet's Logic Programming Approach

Bruno Blanchet (MPI for computer science, Saarbrücken, Germany) 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, 31]. The tool allows one to prove security properties for an unbounded number of sessions. But it may raise some false attack since nonces are abstracted by constants or function symbols. Thus, again, attacks have to be constructed by the user itself.

Action taken Bruno Blanchet has invited Michaël Rusinowitch of INRIA to present AVISPA at a seminar in his group and further reciprocal visits are planned.

2.6.3 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 crypto-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 [32]. This translation allows one to derive a precise description of the protocol behaviour, and is similar to translations previously devised for CAPSL/CIL [39], 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 [32], 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 shall invite the principal investigators of the DEGAS project to our next workshop, and we plan to compare in detail their approach with our abstraction techniques, and in particular with the tree automata techniques discussed in [7]. We believe that it will be possible for them to reuse our technology, which is more efficient according to the experimental results.

2.6.4 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. In particular, he gave a one-day lecture on security protocol analysis at the ZISC fall school on Formal Security Engineering, a one-week compact course for scientists and engineers

working in the field of Information Security focusing on rigorous methods for engineering secure complex networked information systems, which was held at ETH Zurich from September 22nd to September 26th, 2003.[2] During the school, we gave a demonstration of the AVISPA Tool v.1 to Millen, who has expressed his interest in our project and has suggested a number of possible collaborations. For instance, recent work by Millen [49, 47] is closely related to our current work on exponentiation, XOR encryption, and algebraic properties, and we expect 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 Planned work for the next reporting period

The next reporting period (01.01.2004 — 31.12.2004) will be devoted to strengthening the repertoire of techniques for the automatic analysis of security protocols. In accordance with the Technical Annex we plan to address the following technical issues:

- Support the specification of algebraic properties in the specification languages (WP2.2)
- Graphical User Interface for the AVISPA Tool (WP2.4)
- Support of different kinds of security properties (WP3.1)
- Assumptions on the environment (e.g. over-the-air communication) (WP3.2)
- Support to compositional reasoning (WP4.1)
- Further improvements to the back-ends (WP4.4, WP4.5, and WP4.6)
- Infinite-state symbolic model-checking (WP5.2)
- Completeness of model-checking procedures (WP5.3)
- Specification of all the selected security problems (WP6.2)

Moreover, we will continue the tool assessment (WP7) and the dissemination of results (WP8). In particular, special care will be devoted to the dissemination of results by means of the following actions:

- Presentation of AVISPA in a plenary session at the "Open Security Area Directorate" of IETF. This will presumably take place at the IETF Meeting-59 in Seoul, 4th March 2004.

[2] The Zurich Information Security Center (ZISC), which was founded in September 2003, is a collaboration between members of ETH Zurich and industry, with the aim of providing a coordinated program of state-of-the-art research and education in Information Security. David Basin, site leader of ETHZ, is also the director and one of the founding partners of the ZISC.

- 2nd Year Project Workshop. The workshop "Automated Reasoning for Security Protocols Analysis" (ARSPA) will be held in Cork (Ireland), on July 4th, 2004, in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR'04) (`http://www.4c.ucc.ie/ijcar/`), and will be chaired by Prof. Alessandro Armando (UNIGE) and Dr. Luca Viganò (ETHZ). The workshop will aim to bring together researchers and practitioners from both the security and the automated reasoning communities, from academia and industry, who are working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols. We expect about 30 attendees.

Jorge Cuellar (Siemens) and Sebastian Mödersheim and Luca Viganò (ETHZ) are also planning of organising a one-day tutorial on Automated Validation of Security Protocols to be also held in the context IJCAR.

2.8 Assessment of project results and achievements

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

Specification Languages. We have formally defined the high-level protocol specification language HLPSL, a very expressive, yet simple to use, language for the specification of distributed security-sensitive protocols. We have extended the IF specification language used in the AVISS project so to support the specification of sophisticated typed protocol models. Both the HLPSL and the IF are strictly more expressive than rival specification languages.

Selection of protocols. We have selected a wide corpus of practically relevant, security-sensitive, industrial protocols. These are mainly protocols currently being drafted by IETF, and we have assessed the coverage and relevance of the selected problems, taking also into account the comments of IETF representatives. This set of protocols is used within the project to thoroughly assess the AVISPA Tool.

The AVISPA Tool v.1. We have devoted considerable effort to the design and development of the AVISPA Tool v.1, which takes as input a HLPSL specification of a protocol and automatically analyses it. We have accomplished the following results:

- the HLPSL2IF translator has been implemented from scratch;
- OFMC, the on-the-fly model-checker developed and maintained by ETHZ, has been strengthened with new, powerful partial-order techniques, with heuristics, and with automated session compilation and symbolic sessions;
- CL-atse, the protocol analyser based on Constraint Logic developed and maintained by INRIA, implements new data structures and can now handle more sessions in parallel. Thanks to built-in unification modulo associativity procedure it can also tackle many type-flaws.

- SATMC, the SAT-based model-checker developed and maintained by UNIGE, has been improved with new, more sophisticated encoding techniques that make the system orders of magnitude faster.

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

- 13 articles have been published in international conferences and journals,
- 2 PhD theses have been completed,
- two workshops have been organised, and
- an invited talk, a scientific talk, and a tutorial were given in the context of major scientific events.

Moreover, we have initiated dialogue between AVISPA and the Internet Engineering Task Force (IETF), by discussing our list of candidate security protocols and problems with the security area directors at the Open Security Area Directorate of the IETF in the "Open Security Area Directorate Meeting" during the 58th IETF meeting (Minneapolis, November 9-14, 2003)

3 Project Management and Coordination

Project management was largely unproblematic. Three out of the four partners had already successfully cooperated in the AVISS Project (the FET Open project predecessor of AVISPA) and the integration of the new partner was straightforward. However, given the complexity of the technical objectives, particular attention has been paid to the coordination of the activities. To this end, the following measures proved to be particularly effective.

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

- **AVISPA warm-up meeting**, 29–30.11.2002, MRG-DIST, Genoa, Italy. (Program available at `http://www.avispa-project.org/Internal/Meetings/200211WarmUp`) This meeting was in effect the kick-off meeting as it was devoted to the refinement of the project work-plan. It was decided to have it one month before the actual start of the project in order to begin the actual work at the very start of the project. This proved to be a very important decision since as early as on January 15, 2003, a preliminary working draft of the IF specification language was already circulating among the partners and some key technical issues that needed to be addressed were clearly identified. From an organisational standpoint, we nominated a "Site Technical Coordinator" (STO) for each group, with the responsibility of supervising and monitoring the progress of the technical activities and the production of deliverables within the respective site.

- **Semantics meeting**, 21–23.01.2003, INRIA, Nancy, France. (Program available at `http://www.avispa-project.org/Internal/Meetings/200301Semantics`.) This meeting was devoted to defining a formal semantic of the IF and to initiate the design of the HLPSL.

- **1st AVISPA Synchronisation Meeting**, 13–14.03.2003, ETHZ, Zürich, Switzerland. (Program available at `http://www.avispa-project.org/Internal/Meetings/200303FirstSynch`.) This meeting was devoted to synchronising the activities among the partners. A proposal for the HLPSL2IF translator was proposed and discussed by the partners. Moreover, a first draft of the list of the selected security problems was presented by Siemens.

- **1st AVISPA Results Meeting** (08-09.07.2003) Siemens, München, Germany. It was during this meeting that the versions of the HLPSL and IF to be included in [1] and in [2] were approved by the partners. Finally, a proposal to add procedural abstraction to the HLPSL was discussed and approved.

- **AVISPA Meeting** (21-23.10.2003) ETHZ, Zürich, Switzerland. This meeting was almost fully devoted to the development of the HLPSL2IF translator.

Project Workshops and Tutorials. The following workshop was organised by Michaël Rusinowitch, site leader of INRIA.

- **SPV — Workshop on Security Protocols Verification**, 06.09.2003, Marseille, France. (Workshop Web-Site: `http://www.loria.fr/~rusi/spv.html`.)

It was decided to hold the 1st Project Workshop on January 23, 2004 at INRIA, Nancy. This is month 13 of the project and not month 10 as originally planned. This shift was necessary as otherwise the project workshop would have been too close to the SPV workshop, which was held at month 9 of the project. Two world-wide experts in computer security (namely, Dr. Peter Ryan, University of Newcastle, U.K., and Dr. Yassine Lakhnech, Verimag, Grenoble, France) have accepted our invitation to speak at the workshop.

The following tutorial was given by Jorge Cuellar, site leader of Siemens.

- **Full day tutorial at the International Conference on Software Engineering And Formal Methods** (SEFM 2003, Brisbane, Australia, 22nd – 27th September, 2003) `http://www.svrc.uq.edu.au/Events/SEFM03/` (Number of attendees: 10).

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 defining the syntax and semantics of the specification languages HLPSL and IF, as well as to design 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. Mailing lists have worked well to exchange ideas and coordinate activities. We have set up the following mailing lists:

- `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-techn@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) have been set up:

- 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) has been set up at the beginning of the project. 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 Euros (400,000 CHF).

Table 4. Costs in euro for the reporting period: 01.01.2003 --- 31.12.2003

	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	99.595	106.984	364.463	106.984	89.762	67.273	213.428	67.273	133.426	7.420	333.565	7.420	103.318	119.162	264.568	119.162
2. Durable Equipment	6.506	7.104	16.264	7.104	-	-	-	-	-	-	-	-	-	-	-	-
3. Subcontracting	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4. Travel and subsistence	9.000	10.569	21.994	10.569	10.000	10.485	26.000	10.485	7.500	4.259	20.000	4.259	-	-	-	-
5. Consumables	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6. Computing	100	95	300	95	-	-	-	-	-	-	-	-	-	-	-	-
7. Protection of Knowledge	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8. Other specific costs	1.000	150	11.000	150	1.000	1.230	11.489	1.230	1.000	-	2.750	-	-	-	8.000	-
Subtotal	**116.201**	**124.902**	**414.021**	**124.902**	**100.762**	**78.988**	**250.917**	**78.988**	**141.926**	**11.679**	**356.315**	**11.679**	**103.318**	**119.162**	**272.568**	**119.162**
Indirect Costs																
9. Overheads	50.157	51.952	175.702	51.952	139.254	92.881	323.621	92.881	7.096	-	17.815	-	92.406	83.596	236.626	83.596
Total	**166.358**	**176.854**	**589.723**	**176.854**	**240.016**	**171.869**	**574.538**	**171.869**	**149.022**	**11.679**	**374.130**	**11.679**	**195.724**	**202.758**	**509.194**	**202.758**

NOTE: The actual costs of Siemens include 14,453.20 due to subsequent mercantile adjustments for 2003.

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 will present this work in Seoul at the IETF Meeting-59 (see below). We are currently also planning to present the AVISPA initial results and tools in the plenary session of one of the following IETF Meetings.

Talks. All of the 12 articles that have been published in international conferences have been presented at the respective meetings. The following is the list of presented and planned, additional, talks at relevant international conferences and forums. These talks aim at introducing the high-level project objectives, the protocols and problems that the project is analysing, and the techniques and results achieved:

- Full day tutorial at the International Conference on Software Engineering And Formal Methods (SEFM 2003, Brisbane, Australia, 22nd – 27th September, 2003). `http://www.svrc.uq.edu.au/Events/SEFM03/` (Number of attendees: 10).
- Talk on the OFMC back-end and the AVISPA project at the Dagstuhl Seminar on Language-Based Security. Dagstuhl, Germany, 5th – 10th October, 2003. (Number of attendees: about 60)
- Invited talk at the Industrial Day of the Formal Methods Europe Conference (FME 2003): Specifying and Verifying real-world Security Protocols `http://fme03.isti.cnr.it/iday-progr.htm` (Number of attendees: about 30).
- The First Project Workshop, to take place in Nancy on the 23rd of January 2004. (`http://qsl.loria.fr/Externe/Evennements/JourneeQSL/Journee23-01-2004/programme.htm`) All members of the AVISPA project will attend the workshop and we have invited as guests two renowned international researchers who are working on related problems, namely Dr. Peter Ryan (University of Newcastle, U.K.) and Dr. Yassine Lakhnech (Verimag, Grenoble, France).
- Presentation of the AVISPA protocols and problems at the Open Security Area Directorate Meeting (SAAG) at Seoul, 4th March 2004. `http://www.ietf.org/meetings/IETF-59.html` (Number of expected attendees: about 300).
- Workshop on Automated Reasoning for Security Protocols Analysis (ARSPA) co-located with the Second International Joint Conference on Automated Reasoning

(IJCAR'04) in Cork (Ireland), July 4, 2004. (Number of expected attendees: about 30).

- The Third Project Workshop will take place in June 2005 (i.e. just before the end of the project). In order to maximise the dissemination of the project results we plan to organise this event in the context of a major scientific event such as, e.g., a meeting of the IETF.

Jorge Cuellar (Siemens) and Sebastian Mödersheim and Luca Viganò (ETHZ) are also planning of organising a one-day tutorial on Automated Validation of Security Protocols to be also held in the context IJCAR.

Publicly available Web-Site. AVISPA has a publicly available web-site that includes descriptions of the main project results and in particular our library of formal specifications of industrial protocols and applications. The web-site of the project is

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

and all information relevant to the project can be found there. The web-site 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 Fifth Framework Programme.
- The list of events related to AVISPA: meetings, conferences, workshops, and their availability to the public.
- Publications related to AVISPA, both in the scientific community and in the general press.
- 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 2.1: The High-Level Protocol Specification Language. Available at `http://www.avispa-project.org`, 2003.

[2] AVISPA. Deliverable 2.3: The Intermediate Format. Available at `http://www.avispa-project.org`, 2003.

[3] AVISPA. Deliverable 3.3: Session Instances. Available at `http://www.avispa-project.org`, 2003.

[4] AVISPA. Deliverable 4.2: Partial-Order Reduction. Available at `http://www.avispa-project.org`, 2003.

[5] AVISPA. Deliverable 4.3: Heuristics. Available at `http://www.avispa-project.org`, 2003.

[6] AVISPA. Deliverable 4.4: AVISPA tool v.1. Available at `http://www.avispa-project.org`, 2003.

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

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

[9] AVISPA. Deliverable 7.1: Experimental Setup. Available at `http://www.avispa-project.org`, 2003.

[10] AVISPA. Deliverable 7.2: Assessment of the AVISPA tool v.1. Available at `http://www.avispa-project.org`, 2003.

7 AVISPA Publications

[11] P. Ammirati and G. Delzanno. Constraint-based Automatic Verification of Time Dependent Security Properties. In *Proceedings of SPV'03*. Available at `http://www.avispa-project.org`, 2003.

[12] A. Armando and L. Compagna. Abstraction-driven SAT-based Analysis of Security Protocols. In *Proceedings of SAT 2003*, LNCS 2919. Springer-Verlag, 2003. Available at `www.avispa-project.org`.

[13] A. Armando, L. Compagna, and P. Ganty. SAT-based Model-Checking of Security Protocols using Planning Graph Analysis. In K. Araki, S. Gnesi, and D. Mandrioli, editors, *Proceedings of the 12th International Symposium of Formal Methods Europe (FME)*, LNCS 2805, pages 875–893. Springer-Verlag, 2003. Available at `www.avispa-project.org`.

[14] D. Basin, S. Mödersheim, and L. Viganò. An On-The-Fly Model-Checker for Security Protocol Analysis. In E. Snekkenes and D. Gollmann, editors, *Proceedings of ESORICS'03*, LNCS 2808, pages 253–270. Springer-Verlag, 2003. Available at `http://www.avispa-project.org`.

[15] D. Basin, S. Mödersheim, and L. Viganò. Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols. In V. Atluri and P. Liu, editors, *Proceedings of CCS'03*, pages 335–344. ACM Press, 2003. Available at `http://www.avispa-project.org`.

[16] D. Basin, S. Mödersheim, and L. Viganò. Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols (Extended Abstract). In *Proceedings of SPV'03*. Available at `www.loria.fr/~rusi/spv.html`, 2003. Available at `http://www.avispa-project.org`.

[17] Y. Chevalier. *Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques*. Phd, Université Henri Poincaré, Nancy, December 2003.

[18] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. In *Proceedings of the Logic In Computer Science Conference, LICS'03*, pages 261–270, 2003. Available at `http://www.avispa-project.org`.

[19] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents. In *Proceedings of the Foundations of Software Technology and Theoretical Computer Science, FST TCS'03*, LNCS 2914. Springer-Verlag, 2003. Available at `http://www.avispa-project.org`.

[20] Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions. In M. Baaz, editor, *Proceedings of CSL'2003*, LNCS 2803. Springer-Verlag, 2003. Available at `http://www.avispa-project.org`.

[21] G. Delzanno and P. Ganty. Symbolic Methods for Automatically Proving Secrecy and Authentication in Infinite-state Models of Cryptographic Protocols. In *Proceedings of the Workshop on Issues in Security and Petri Nets (WISP'03)*, 2003. Available at `http://www.avispa-project.org`.

[22] G. Delzanno and P. Ganty. Automatic Verification of Time Sensitive Cryptographic Protocols. In *Proceedings of TACAS'04*, 2004. Available at `http://www.avispa-project.org`.

[23] M. Rusinowitch. Automated Analysis of Security Protocols. In G. Vidal, editor, *Proceedings of the 12th International Workshop on Functional and (Constraint) Logic Programming, WFLP'03*, volume 86(3). Electronic Notes in Theoretical Computer Science, 2003. Available at `http://www.avispa-project.org`.

[24] M. Rusinowitch and M. Turuani. Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete. *Theoretical Computer Science*, 299:451–475, 2003. Available at `http://www.avispa-project.org`.

[25] M. Turuani. *Sécurité des Protocoles Cryptographiques: Décidabilité et Complexité.* Phd, Université Henri Poincaré, Nancy, December 2003.

8 References

[27] R. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In C. Palamidessi, editor, *Proceedings of Concur'00*, LNCS 1877, pages 380–394. Springer-Verlag, 2002.

[28] A. Armando, D. Basin, M. Bouallagui, Y. Chevalier, L. Compagna, S. Mödersheim, M. Rusinowitch, M. Turuani, L. Viganò, and L. Vigneron. The AVISS Security Protocol Analysis Tool. In *Proceedings of CAV'02*, LNCS 2404, pages 349–354. Springer-Verlag, 2002.

[29] AVISS. Deliverable 1.3: Final project report. For more information on the AVISS project see `http://www.avispa-project.org/theproject.html`, 2002.

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

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

[32] 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.

[33] M. Boreale. Symbolic trace analysis of cryptographic protocols. In *Proceedings of ICALP'01*, LNCS 2076, pages 667–681. Springer-Verlag, 2001.

[34] 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.

[35] Common Authentication Protocol Specification Language. URL: `http://www.csl.sri.com/~millen/capsl/`.

[36] H. Comon-Lundh and V. Cortier. Security properties: two agents are sufficient. In *Proceedings of ESOP'2003*, LNCS 2618, pages 99–113. Springer-Verlag, 2003.

[37] R. Corin and S. Etalle. An Improved Constraint-Based System for the Verification of Security Protocols. In *Proceedings of SAS 2002*, LNCS 2477, pages 326–341. Springer-Verlag, 2002.

[38] G. Denker and J. Millen. CAPSL Intermediate Language. In N. Heintze and E. Clarke, editors, *Proceedings of Workshop on Formal Methods and Security Protocols (FMSP'99)*. Available at `http://cm.bell-labs.com/cm/cs/who/nch/fmsp99/`. URL for CAPSL and CIL: `http://www.csl.sri.com/~millen/capsl/`, 1999.

[39] 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/`.

[40] EVA. Projet RNTL, Explication & Vérification AUtomatique. `http://www-eva.imag.fr/`, 2003.

[41] P. E. Hart, N. J. Nilsson, and B. Raphael. A formal basis for the heuristic determination of minimum cost paths. *IEEE Transactions on Systems Science and Cybernetics*, SSC-4(2):100–107, 1968.

[42] ITU-T Recommendation H.530: Symmetric Security Procedures for H.510 (Mobility for H.323 Multimedia Systems and Services), 2002.

[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] L. Lamport. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, May 1994.

[45] L. Lamport. *Specifying Systems*. Addison-Wesley, 2002.

[46] G. Lowe. Casper: a Compiler for the Analysis of Security Protocols. *Journal of Computer Security*, 6(1):53–84, 1998. See `http://web.comlab.ox.ac.uk/oucl/work/gavin.lowe/Security/Casper/`.

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

[48] J. K. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proceedings of the ACM Conference on Computer and Communications Security CCS'01*, pages 166–175, 2001.

[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.