AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D1.2: Periodic Progress Report N°: 2

Covering period 01.01.2004 — 31.12.2004

Abstract

This periodic progress report covers the second 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: *v1.0*	Person-months required: *1*
Date of delivery: *18.02.2005*	Due on: *31.01.2005*
Classification: *public*	Total pages: *57*

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.

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 extend the definition of the High-Level Protocol Specification Language (HLPSL) and of the Intermediate Format (IF) so to enable the specification and formal analysis of security-sensitive, state-of-the-art Internet protocols. To extend the implementation of the translator from HLPSL to IF.

WP3 – Context & Properties Specification To build constructs for expressing security goals and assumptions about the environment. To support the specification and the analysis under more sophisticated assumptions such as, e.g., the use of non-perfect encryption primitives.

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 capable of deriving positive statements about protocol security, i.e. verify that the protocols achieve their security objectives.

WP6 – Selection & Specification of Protocols To extend the AVISPA library with new security problems (i.e. protocols and the security properties they are designed to achieve) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation.

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 second reporting period have been achieved, all success criteria set out in the Technical Annex have been met, and 11 of the 12 planned deliverables have been produced on time. As agreed upon by the Project Officer the delivery date for Deliverable 4.1 "Compositionality" was moved to the next reporting period.

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 During the first year of the project, we have formalised the High-Level Protocol Specification Language (HLPSL) and the Intermediate Format (IF), and have implemented an automated translator HLPSL2IF from HLPSL to IF. In the second year we have extended both HLPSL and IF, as well as HLPSL2IF, in order to consider a larger class of protocols and security properties, and thus be able to propose more possibilities of analysis. Besides for syntactic modifications, we have, for example, added the possibility of declaring variables of compound types, we have improved the description of composition of roles, and we have improved the description of constraints in IF. In addition to the above modifications, we have enriched the translator with further options in order to improve its simplicity and usability.

WP4&5 During this second year of the project, we have focused on infinite-state model-checking. Besides for the introduction of a verification algorithm for time-sensitive security protocols, we have extended and generalised the results that we achieved during the first project year and continued the development and integration of heuristics, optimisations, and reduction, and abstraction techniques, both general and specific to the individual back-ends. These techniques are implemented in the three back-ends of the AVISPA Tool that constituted version 1 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 integrated a fourth back-end into the AVISPA Tool, namely

TA4SP, which is based on tree automata techniques and has been developed by INRIA.

The resulting architecture of the AVISPA Tool v.2 is depicted in Figure 1.

WP6&7 During the first year of the project we have identified and selected a large number of security protocols (along with the associated security properties) to be used as testbed for thoroughly assessing the AVISPA Tool. The resulting collection of

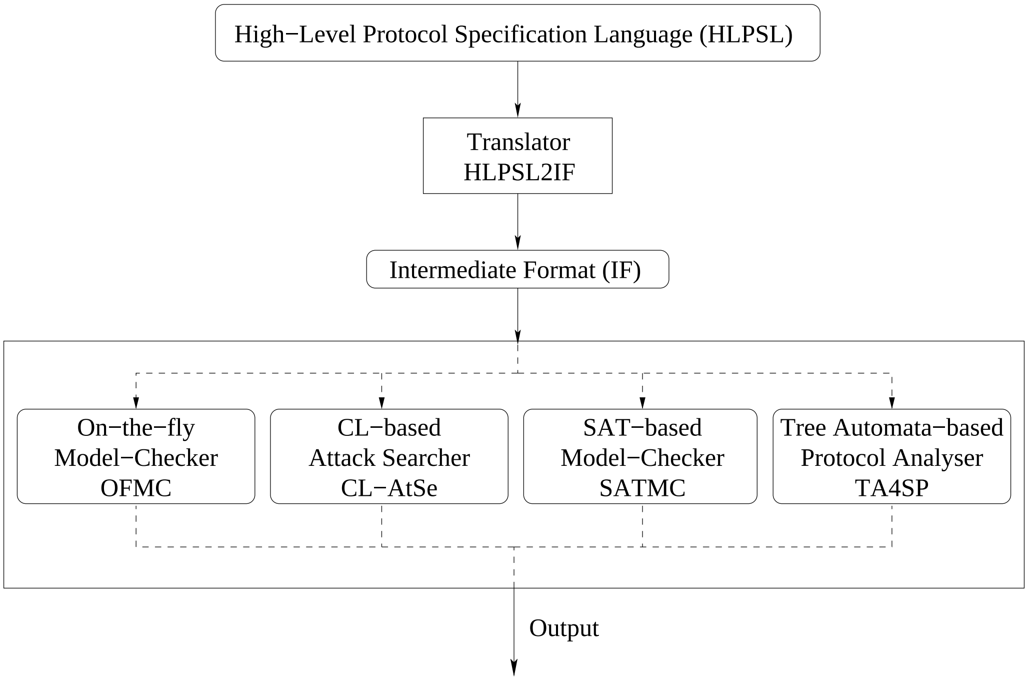


Figure 1: Architecture of the AVISPA Tool v.2

candidate protocols and security problems was given in Deliverable 6.1 [34]. During the second year of the project we have formalised in HLPSL a large number of these problems and we have used them to assess the AVISPA Tool, thereby demonstrating proof-of-concept on a large collection of practically relevant, industrial protocols.

As described in [34], the following criteria, which refine the ones given in the Technical Annex, are used for the assessment of the AVISPA tool at month 24:

Coverage: at least 40 security problems from 10 groups of the AVISPA library should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 30) of these 40 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 demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 112 problems from 14 groups, and the tool successfully analyses 110 problems in less than 25 minutes of CPU time per problem (globally, the entire library of 110 problems requires 69

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

Success criteria at month 24	**Objectives**	**Results**
Coverage	40 problems from 10 groups	112 problems from 14 groups
Effectiveness	30 problems	110 problems
Performance	< 1 hour per problem	< 25 minutes per problem (all 110 problems in 69 minutes)

minutes of CPU time to be analysed). All the above requirements (namely coverage, effectiveness, and performance) are therefore more than fulfilled.

The activities for the Project Management workpackage (WP1) included *(i)* the supervision of the technical activity and of the production of the deliverables, *(ii)* the organisation of project meetings (restricted to the AVISPA personnel), and *(iii)* the writing of the *Periodic Progress Report* (this document). All these objectives have been realised successfully: 4 project meetings with a large number of attendees from all project partners have been held. 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 management of the AVISPA Web-Site (`www.avispa-project.org`), the organisation of project workshops and of a tutorial, and the presentation of the project's achievements at conferences and in invited talks. All these objectives have been realised successfully. Dissemination has followed standard scientific channels: 18 papers have been published in international conferences and journals, two workshops have been organised, and a number of invited talks, paper presentations, and a tutorial were given in the context of major scientific events. Additionally, we have actively sought for contacts and exchanges of ideas with representatives of research projects on related themes that are currently being carried out at the national, EU, or international level.

In the rest of the project, we plan to continue the dissemination of our results by presenting the AVISPA project at the Open Security Area Directorate Meeting (SAAG) of IETF, by organising the second edition of the workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'05) and the second edition of the tutorial on Automated Validation of Security Protocols (AVASP'05), and by continuing to publish our results in international conferences and journals.

We have also continued the dialogue between AVISPA and the Internet Engineering Task Force (IETF). This is particularly important as the large collection of practically relevant, security-sensitive, industrial protocols that AVISPA is studying are mostly being standardised by the IETF. The list of chosen candidate protocols and related problems, as described in Deliverable 6.1 [34], has been made available to the IETF and discussed with the security area directors.

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 second project year has led the foundations of a push-button technology, based on automated deduction, for validating security-sensitive protocols like those used in electronic commerce, telecommunications, multi-media, and other application areas. We believe that this technology will pave the way to the construction of industrial-strength protocol validation tools that will reduce time-to-market and increase trust in the security of applications, thereby improving the competitiveness of European companies working in these application areas.

2 Work Progress Overview

2.1 Specific objectives for the reporting period

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

1. To extend the specification languages HLPSL and IF so to support the specification of protocols, security goals, and threat models of industrial complexity; to extend the implementation of the HLPSL2IF translator from HLPSL to IF.
2. To build constructs for expressing security goals and assumptions about the environment; to support the specification and the analysis under more sophisticated assumptions such as, e.g., the use of non perfect encryption primitives.
3. To advance of state-of-the-art in automated deduction techniques to scale up to this new level of complexity.
4. To investigate mechanisms capable of deriving positive statements about protocol security, i.e. verify that they achieve their security objectives.
5. To implement the new techniques in the AVISPA Tool.
6. To extend the AVISPA library with new security problems (protocols and security properties) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation.
7. To tune the AVISPA Tool and demonstrate proof-of-concept on the AVISPA Library.
8. To initiate the migration of this technology into standardisation organisations such as the IETF so that both the scientific and the industrial community can benefit from the advances achieved by this project.

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

The architecture of version 2 of the AVISPA Tool is depicted in Figure 1: specifications of security protocols and properties written in a high-level protocol specification language (the HLPSL specification language) are automatically translated (by the HLPSL2IF translator) into a format amenable to formal analysis (the Intermediate Format IF, which is a low-level specification language); the resulting specifications are then given as input to the different back-ends of the AVISPA Tool: OFMC, CL-AtSe, SATMC, and the newly added TA4SP. Upon termination, each back-end reports whether the input problem was solved (positively or negatively) and displays an attack on the protocol whenever one is found.

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

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

A significant amount of work and attention have been devoted to the extension of the specification languages HLPSL and IF, as well as to the development of the HLPSL2IF translator. An important effort has also been done for improving the output format of each back-end. The main extensions and modifications are the following:

HLPSL. We have carried out a number of syntactic improvements, such as the notation for sets and lists that are the standard ones now, and the syntax for encryption. The principal extensions concern:

- The possibility to declare variables of compound type; before, the generic type `message` had to be used instead.
- Some algebraic properties can be considered: exclusive-or (`xor(_,_)`) and exponentiation (`exp(_,_)`) can be used in messages.
- A more precise description of authentication goals, avoiding possible ambiguities.

We have also considered a number of assumptions on the environment as well as some other algebraic properties and several other security properties, and investigated their specification in HLPSL.

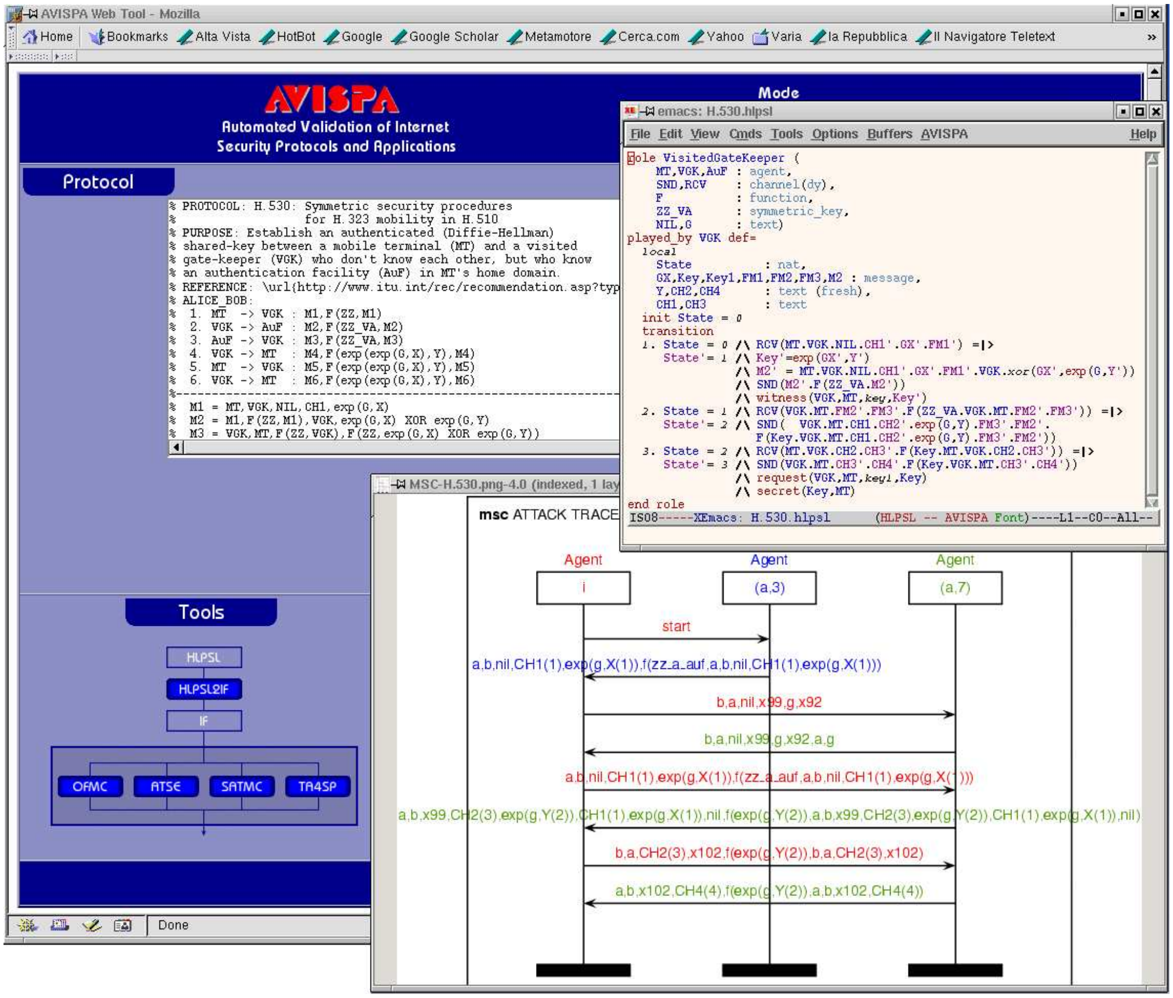
IF. The IF has reached a stable form and therefore only a few, minor changed proved necessary:

- support to declarations of variables of compound type;
- more expressive syntax for constraints attached to left-hand sides of rules.

HLPSL2IF. The HLPSL2IF translator has been updated for taking into account the modifications in the specification languages. Moreover, it has been extended for the following points:

- the composition of roles is better handled, avoiding false errors detections as in the previous version; it also prepares to the future translation of sequential compositions;
- goals splitting has been improved, selecting only appropriate user predicates in transition rules;
- more options are now available, for printing warnings, debugging informations, but also for indicating in which directory to put the output files.

OF. The Output Format, common to all the back-ends, has been modified for giving a more precise description of the result; it indicates the conditions under which the properties of a given protocol have been studied; and if an attack is found, it is very clearly described.


AVISPA Web Tool - Mozilla
Home
Bookmarks
Alta Vista
HotBot
Google
Google Scholar
Metamotore
Cerca.com
Yahoo
Varia
la Repubblica
Il Navigatore Teletext
AVISPA
Automated Validation of Internet
Security Protocols and Applications
Mode
Protocol
Tools
HLPSL
HLPSL2IF
IF
OFMC
ATSE
SATMC
TA4SP
Done
emacs: H.530.hlpsl
File Edit View Cmds Tools Options Buffers AVISPA Help
MSC-H.530.png-4.0 (indexed, 1 lay
msc ATTACK TRACE
Agent
i
Agent
(a,3)
Agent
(a,7)
start
a,b,nil,CH1(1),exp(g,X(1)),f(zz_a_auf,a,b,nil,CH1(1),exp(g,X(1)))
b,a,nil,x99,g,x92
b,a,nil,x99,g,x92,a,g
a,b,nil,CH1(1),exp(g,X(1)),f(zz_a_auf,a,b,nil,CH1(1),exp(g,X(1)))
a,b,x99,CH2(3),exp(g,Y(2)),CH1(1),exp(g,X(1)),nil,f(exp(g,Y(2)),a,b,x99,CH2(3),exp(g,Y(2)),CH1(1),exp(g,X(1)),nil)
b,a,CH2(3),x102,f(exp(g,Y(2)),b,a,CH2(3),x102)
a,b,x102,CH4(4),f(exp(g,Y(2)),a,b,x102,CH4(4))

```
% PROTOCOL: H.530: Symmetric security procedures
%                  for H.323 mobility in H.510
% PURPOSE: Establish an authenticated (Diffie-Hellman)
% shared-key between a mobile terminal (MT) and a visited
% gate-keeper (VGK) who don't know each other, but who know
% an authentication facility (AuF) in MT's home domain.
% REFERENCE: \url{http://www.itu.int/rec/recommendation.asp?typ
% ALICE_BOB:
%  1. MT  -> VGK : M1,F(ZZ,M1)
%  2. VGK -> AuF : M2,F(ZZ_VA,M2)
%  3. AuF -> VGK : M3,F(ZZ_VA,M3)
%  4. VGK -> MT  : M4,F(exp(exp(G,X),Y),M4)
%  5. MT  -> VGK : M5,F(exp(exp(G,X),Y),M5)
%  6. VGK -> MT  : M6,F(exp(exp(G,X),Y),M6)
%--------------------------------------------------------------
%  M1 = MT,VGK,NIL,CH1,exp(G,X)
%  M2 = M1,F(ZZ,M1),VGK,exp(G,X) XOR exp(G,Y)
%  M3 = VGK,MT,F(ZZ,VGK),F(ZZ,exp(G,X) XOR exp(G,Y))
```

```
role VisitedGateKeeper (
    MT,VGK,AuF : agent,
    SND,RCV    : channel(dy),
    F          : function,
    ZZ_VA      : symmetric_key,
    NIL,G      : text)
played_by VGK def=
  local
    State                    : nat,
    GX,Key,Key1,FM1,FM2,FM3,M2 : message,
    Y,CH2,CH4                : text (fresh),
    CH1,CH3                  : text
  init State = 0
  transition
  1. State = 0 /\ RCV(MT.VGK.NIL.CH1'.GX'.FM1') =|>
     State'= 1 /\ Key'=exp(GX',Y')
               /\ M2' = MT.VGK.NIL.CH1'.GX'.FM1'.VGK.xor(GX',exp(G,Y'))
               /\ SND(M2'.F(ZZ_VA.M2'))
               /\ witness(VGK,MT,key,Key')
  2. State = 1 /\ RCV(VGK.MT.FM2'.FM3'.F(ZZ_VA.VGK.MT.FM2'.FM3')) =|>
     State'= 2 /\ SND(  VGK.MT.CH1.CH2'.exp(G,Y).FM3'.FM2'.
                 F(Key.VGK.MT.CH1.CH2'.exp(G,Y).FM3'.FM2'))
  3. State = 2 /\ RCV(MT.VGK.CH2.CH3'.F(Key.MT.VGK.CH2.CH3')) =|>
     State'= 3 /\ SND(VGK.MT.CH3'.CH4'.F(Key.VGK.MT.CH3'.CH4'))
               /\ request(VGK,MT,key1,Key)
               /\ secret(Key,MT)
end role
ISO8-----XEmacs: H.530.hlpsl     (HLPSL -- AVISPA Font)----L1--C0--All--
```

Figure 2: A screen-shot of the AVISPA Tool.

The documentation of the two specification languages, of the output format and of the translator has also been improved and is available on request for external users. The translator and a README file are available on the project web site.

As displayed in Fig.2, we have equipped the AVISPA Tool with a web-based graphical user interface that supports the editing of protocol specifications and allows the user to select and configure the different back-ends of the tool. If an attack on a protocol is found, the interface displays it as a message-sequence chart. For instance, Fig.2 shows part of the specification of Siemens' H.530 protocol (top-right window) and the attack that AVISPA has found (bottom window), reported on in [16]. The interface features specialised menus for both novice and expert users. We have also developed an XEmacs mode for pretty-printing HLPSL and IF specifications, and executing automatically the HLPSL2IF translator and the back-ends.

The relevant deliverables produced during the reporting period are:

- D2.2 – Algebraic Properties [2]
- D2.4 – Interface
- D3.1 – Security Properties [4]
- D3.2 – Assumptions on Environment [5]
- D4.5 – AVISPA tool v.2 [6]

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

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

During the second year of the project, we have integrated in the AVISPA Tool a fourth back-end:

TA4SP, based on tree automata techniques, developed and maintained by the LIFC group affiliated with INRIA.

Moreover, we have devised a number of new heuristics, optimisations, and reduction and abstraction techniques, both general and specific to the individual back-ends, both for verification and for error-detection. We have implemented them in the back-ends and carried out experiments to assess their strength. Significant improvements have thus been obtained that enabled the AVISPA Tool to tackle the new, more complex protocols added to the AVISPA Library.

The relevant deliverables produced during the reporting period are:

- D4.5 – AVISPA Tool v.2 [6]
- D5.2 – Infinite-state Model-Checking [7]

2.2.3 Analysis of industrial protocols (WP6&7).

During the second year of the project we have formalised in HLPSL a large number of the security problems that have been identified as practically relevant in Deliverable 6.1 [34]. The resulting collection of specifications (called the AVISPA Library) has then been used to thoroughly assess the AVISPA Tool, thereby demonstrating proof-of-concept on a large collection of practically relevant, industrial protocols.

As described in [34], the following criteria, which refine the ones given in the Technical Annex, are used as for the assessment of the AVISPA tool at month 24:

Coverage: at least 40 security problems from 10 groups of the AVISPA library should be specifiable in the HLPSL.

Effectiveness: the AVISPA Tool should successfully analyse at least 75% (i.e. 30) of these 40 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 demonstrate the success of our work in the reporting period. As summarised in Table 1, we have been able to formalise in the HLPSL 112 problems from 14 groups, and the tool successfully analyses 110 problems in less than 25 minutes of CPU time per problem (globally, the entire library of 110 problems requires 69 minutes of CPU time to be analysed). All the above requirements (namely coverage, effectiveness, and performance) are therefore more than fulfilled.

The relevant deliverables produced during the reporting period are:

- D6.2 – Specification of the problems in the high-level specification language [8]
- D7.3 – Assessment of the AVISPA Tool v. 2 [9]

2.2.4 Deviations from the work-plan.

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

1. The delivery date for Deliverable 4.1 “Compositionality” was moved from month 24 to month 28, in order to have more time to investigate this important issue.

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.

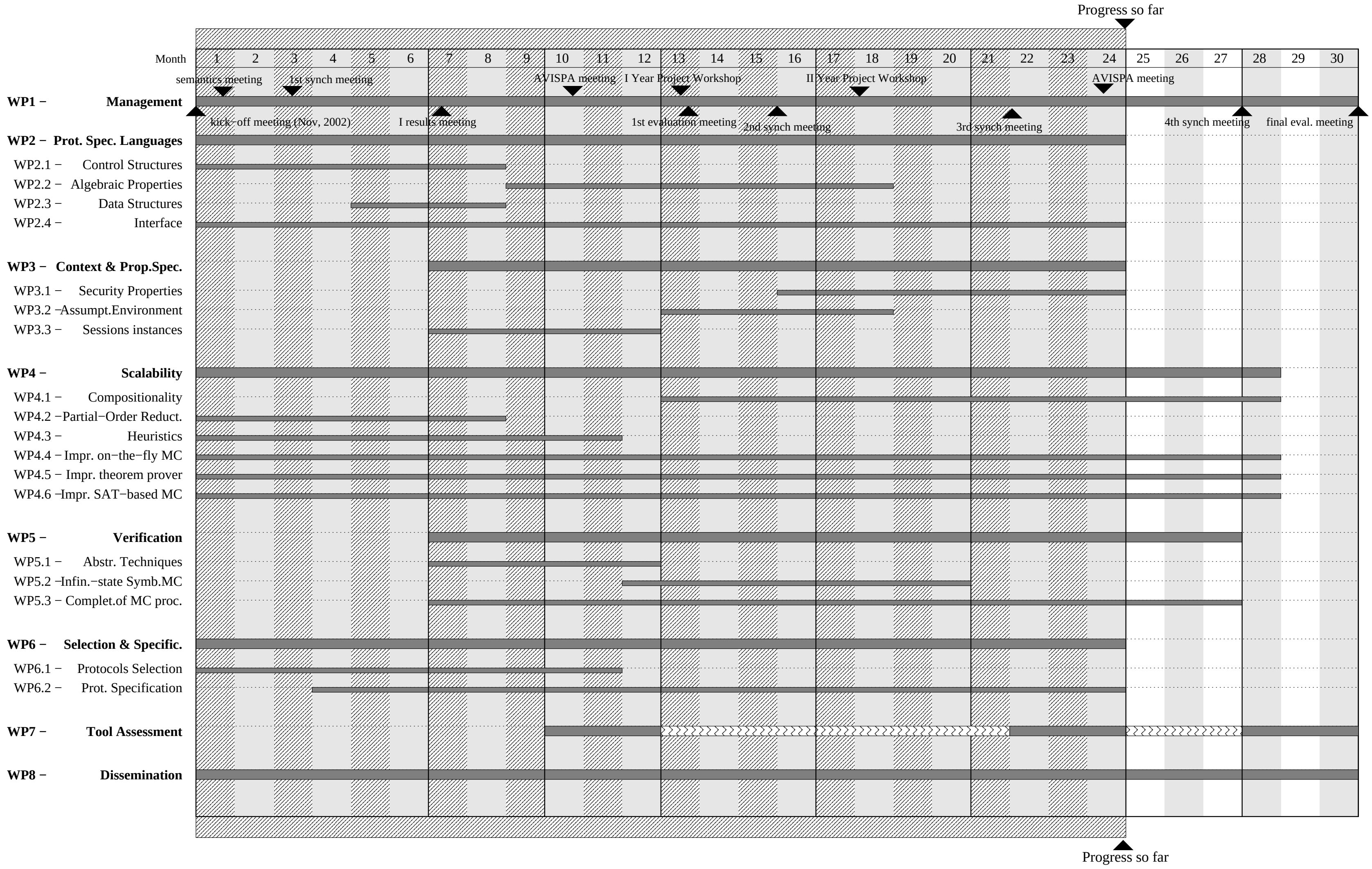


Figure 3: GANTT Chart of the AVISPA Project

2.4 Deliverables produced during the reporting period

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

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**
1.2	1.0	Periodic Progress Report N°: 2	R	Pub.	31.01.2005	31.01.2005
2.2	1.0	Algebraic Properties	R&O	Pub.	30.06.2004	30.07.2004
2.4	1.0	Interface	O	Pub.	31.12.2004	31.01.2005
3.1	1.0	Security Properties	R&O	Pub.	31.12.2004	31.01.2005
3.2	1.0	Assumptions on Environment	R&O	Pub.	30.06.2004	30.07.2004
4.5	1.0	AVISPA Tool v.2	R&O	Pub.	31.07.2004	31.08.2004
5.2	1.0	Infinite-state model-checking	R&O	Pub.	30.08.2004	23.09.2004
6.2	1.0	Specification of the Problems in the HLPSL	R&O	Pub.	31.12.2004	31.01.2005
7.3	1.0	Assessment of the AVISPA Tool v.2	R	Pub.	31.12.2004	31.01.2005
8.4	1.0	Year 1 Project Workshop	R	Pub.	31.01.2004	31.07.2004
8.5	1.0	Year 2 Project Workshop	R	Pub.	31.07.2004	20.08.2004

[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°: 1.2
Title: **Periodic Progress Report N°: 2**
Due date: 31.01.2005
Delivery Date: 31.01.2005

Short Description: This periodic progress report covers the second 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°: 2.2
Title: **Algebraic Properties**
Due date: 30.06.2004
Delivery Date: 30.07.2004

Short Description: The current automated methods for protocol analysis assume the so-called *perfect encryption hypothesis*: one needs a decryption key to extract the plain text from the cipher text, and, moreover, a cipher text can be generated only with the appropriate key and message (no collision). In other words, the current automated protocol analysis methods assume that there are no relations between the messages apart from the standard ones entailed by the Dolev-Yao intruder model. A first step towards a less abstract model is to take into account some algebraic properties of the cryptographic primitives, such as the multiplicativity of RSA or the properties induced by chaining methods for block ciphers. Many real attacks and protocol weaknesses rely on these properties.

In this deliverable, we report on some generalisations of the decidability result of [49], which states that insecurity for finitely many protocol sessions is in NP, to some cases where messages may contain operators with algebraic properties and where the Dolev-Yao intruder is extended by the ability to compose and decompose messages with these operators. More precisely, we give a linear bound on the size of messages exchanged in minimal attacks and present an NP procedure for deciding insecurity. The main case that we consider is the one of the XOR operator. The decidability result for XOR is non-trivial due to the complex interaction of the XOR properties and the standard Dolev-Yao intruder rules. The technical problems raised by the equational laws are somewhat related to those encountered in semantic unification. We show also that the Dolev-Yao intruder equipped with the ability to exploit prefix properties of encryption algorithms based on cipher-block-chaining (CBC) falls into our framework as well. The decidability results presented are the first, besides the ones by Comon and Shmatikov [41], that go beyond the perfect encryption assumption. It is also possible with the same technique to simulate an intruder that can exploit exponentiation function properties and therefore we are able to find attacks on protocols based on Diffie-Hellman key exchange technique. Finally, we can take into account the commutation properties of public keys for some protocols based on RSA when the same modulus is employed for defining the keys.

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°: 2.4
Title: **Interface**
Due date: 31.12.2004
Delivery Date: 31.12.2004

Short Description: This deliverable discusses the work that we carried out to define and implement the interface of the AVISPA tool so to make it effectively usable by the protocol modellers and, more generally, the users of tool. We have defined and implemented two interface modes: an Emacs mode and a graphical web-interface. First, we have specified and implemented an *Emacs mode* in order to obtain a pretty print of protocol specifications, i.e. of HLPSL and IF files. This mode highlights the keywords and the comments, and allows the users to run the back-ends of the AVISPA tool on the specification written in the current buffer.
Second, and most important, we have specified and implemented a *graphical user interface*, that is runnable on the world-wide-web. This interface offers a *basic mode*, that runs all the back-ends of the AVISPA tool on the chosen protocol, and an *expert mode*, that allows a user to run a chosen back-end on the chosen protocol. Another advantage of this graphical interface is the possibility to modify some parameters of the selected back-end. In both modes, after the run, the result is printed, indicating that a flaw has been found, or that the protocol is secure under the conditions of the initial specification, or that no decision is possible. The user can view the source specification (in HLPSL) and the intermediate one (in IF). Moreover, the AVISPA tool supports *message sequence charts* to represent protocol attacks: whenever a flaw is found, the user can view in a diagram the sequence of messages exchanged for generating this flaw. Note also that in order to give to the user clear and precise information on the protocol analysis, we have further improved (with respect to previous deliverables) the output format that is common to all the back-ends of the AVISPA tool.

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°: 3.1
Title: **Security Properties**
Due date: 31.12.2004
Delivery Date: 31.12.2004

Short Description: Security protocols are designed to ensure certain security properties; that is, the goals which the protocol should achieve. Authentication of principals and secrecy of confidential data are classical examples of such goals, though many others exist. Deliverable 6.1 lists the security properties relevant for the protocols of the AVISPA Library, as well as a selection of interesting properties currently under discussion at the Internet Engineering Task Force (IETF) but, as yet, beyond the scope of formal analysis. In this deliverable, we investigate the specification and formalisation of a number of security properties, such as different forms of authentication, secrecy, anonymity, and non-repudiation. Our current methods are well suited to automatically – and very efficiently – check for violations of security properties goals like authentication and secrecy. Furthermore, many other security properties closely resemble authentication and secrecy. It is, therefore, particularly desirable to find reductions from complex properties into boolean or temporal combinations of these simpler properties for which efficient analysis techniques already exist. We adopt this approach wherever possible.

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

DELIVERABLE SUMMARY SHEET

Project Number: IST-2001-39252

Project Acronym: AVISPA

Title: Automated Validation of Internet Security Protocols and Applications

Deliverable N°: 3.2

Title: **Assumptions on Environment**

Due date: 30.06.2004

Delivery Date: 30.07.2004

Short Description: In protocol analysis, the *environment* refers to the formal definition of the conditions under which a security protocol executes. This environment comprises many elements. Among them we count, for instance, the deductive powers assumed of the intruder and the properties of the communication channels over which messages are sent, including the (perhaps differing) intruder types to which said channels are vulnerable. Modern Internet protocols are designed to be executed in a variety of environments. The ability to specify a rich set of assumptions on the protocol analysis environment is therefore important for the specification and analysis of such protocols. This deliverable presents four techniques that span three different classes of environmental assumptions in order to yield a more expressive set of such assumptions.

First, the *compound typing* approach allows us to explicitly specify how honest principals interprets message parts that they cannot decrypt. Experimental results gathered to date show this technique yields a significant performance gain and can therefore extend the scope of tools like SATMC. Second, we investigate alternative *channel assumptions* in order to model networks comprised of heterogeneous communication channels which may be characterised by different intruder models. Third, the *Oracle rules* we define are a useful means of extending the intruder's deductive powers, and they can be employed to better model fine-grained properties of cryptographic operations, bringing vulnerabilities to attacks like low-exponent attacks on RSA into the scope of our analyses. Finally, we present a novel approach to analysing guessing attacks in which the intruder exploits poorly chosen passwords. This models an important real-world vulnerability and improves on previous approaches in that it is simpler, more declarative, and closer to general intuition regarding guessing 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°: 4.5
Title: **AVISPA Tool v.2**
Due date: 31.07.2004
Delivery Date: 31.08.2004

Short Description: This deliverable describes version 2 of the AVISPA Tool for security protocol analysis, focussing in particular on the modifications and improvements with respect to version 1 of the tool. The architecture of the AVISPA Tool v. 2 is depicted in Figure 1. Specifications of security protocols and properties written in the High-Level Protocol Specification Language (HLPSL [31]) are automatically translated (by the translator HLPSL2IF) into IF [32] specifications, which are then given as input to the different back-ends of the AVISPA Tool. Besides the three original back-ends of the tool, namely OFMC, CL-AtSe, and SATMC, we describe a new back-end, TA4SP, which has been developed by the CASSIS group at INRIA and integrated into the current version of the AVISPA Tool. Whenever it terminates, each back-end of the AVISPA Tool outputs the result of its analysis using a common and precisely defined format stating 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
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°: 5.2
Title: **Infinite-state model-checking**
Due date: 31.08.2004
Delivery Date: 23.09.2004

Short Description: Protocol verification requires the analysis of an infinite number of configurations and therefore calls for infinite-state model checking techniques. In Deliverable 5.1, we have proposed several sound abstractions for reducing the verification to a finite number of states. In this deliverable, we first introduce a verification algorithm for time-sensitive security protocols. The verification is performed by symbolic exploration of upward closed set of configurations. We then present an extension of the tree automata technique introduced in Deliverable 5.1, which allows us to reduce the number of states generated by the approximation function and therefore handle more protocols from the AVISPA library. Finally, we report on some finer abstractions on nonces in fixed-point computations, which allow us to analyse the ASW contract signing protocol and to point to a new attack on it.

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°: 6.2
Title: **Specification of the Problems in the High-Level Specification Language**
Due date: 31.12.2004
Delivery Date: 31.01.2005

Short Description: This document presents the specifications of the protocols and security problems that we have actually modelled in the HLPSL and analysed with the AVISPA tool. This set of protocols is a large subset of those described in Deliverable 6.1. For each of the protocols, we describe their purpose, the messages exchange in the Alice&Bob notation, the corresponding security problems, any attacks found, and finally we give the actual HLPSL code. Where appropriate, we add further explanations and comments.

Partners owning: Siemens
Partners contributed: UNIGE, 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°: 7.3
Title: **Assessment of the AVISPA Tool v.2**
Due date: 31.12.2004
Delivery Date: 31.01.2005

Short Description: In this document, we report on the assessment of the AVISPA Tool at project month 24. The results of the assessment demonstrate the achievement of the project's objectives for the reporting period. We have been able to formalise in the HLPSL 112 problems from 14 groups, and the AVISPA Tool v.2 successfully analyses 110 problems in less than 25 minutes of CPU time per problem (globally, the whole library of 110 problems requires 69 minutes to be analysed). All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the AVISPA Tool v.2. Moreover, the tool is able to detect the same new (i.e. previously unknown in literature) attacks discovered by the AVISPA Tool v.1 and with better performance.

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°: 8.4
Title: **Year 1 Project Workshop**
Due date: 31.01.2004
Delivery Date: 20.08.2004

Short Description: The Year 1 Project Workshop of the AVISPA Project was held at INRIA-Lorraine (Nancy) on January 23, 2004, and was devoted to recent advances on the specification of security protocols and their properties, as well as on the techniques for their automatic analysis. The technical program of the workshop was enriched by the talks of two internationally reknown invited speakers, namely

- Prof. Peter Ryan from the University of Newcastle (UK), and
- Dr. Yassine Lakhnech from VERIMAG (Grenoble, France).

The results of the workshop have been significant in terms of dissemination, cross-fertilisation of ideas, and establishment of new synergies with other research teams.

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

DELIVERABLE SUMMARY SHEET

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

Deliverable N°: 8.5
Title: **Year 2 Project Workshop**
Due date: 31.07.2004
Delivery Date: 20.08.2004

Short Description: The Year 2 Project Workshop of the AVISPA Project, titled "Workshop on Automated Reasoning for Security Protocol Analysis" (ARSPA), was held at the University College, Cork (Ireland), on July 4, 2004, in the context of the 2nd International Joint Conference on Automated Reasoning (IJCAR'04). The workshop brought together researchers and practitioners from both the security and the automated reasoning communities, from academia and industry, who are working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols. The results of the workshop have been significant in terms of dissemination and cross-fertilisation of ideas. Accepted contributions have been included in the informal workshop proceedings, which were available at the workshop (and are available, together with the slides of the presentations, at the home page of the workshop: `http://www.avispa-project.org/arspa`). The workshop proceedings will be published as a special issue of the Electronic Notes in Theoretical Computer Science. Moreover, the members of the program committee of ARSPA will guest-edit a Special Issue of the Journal of Automated Reasoning collecting original papers on automated reasoning techniques and tools for the formal specification and analysis of security protocols.

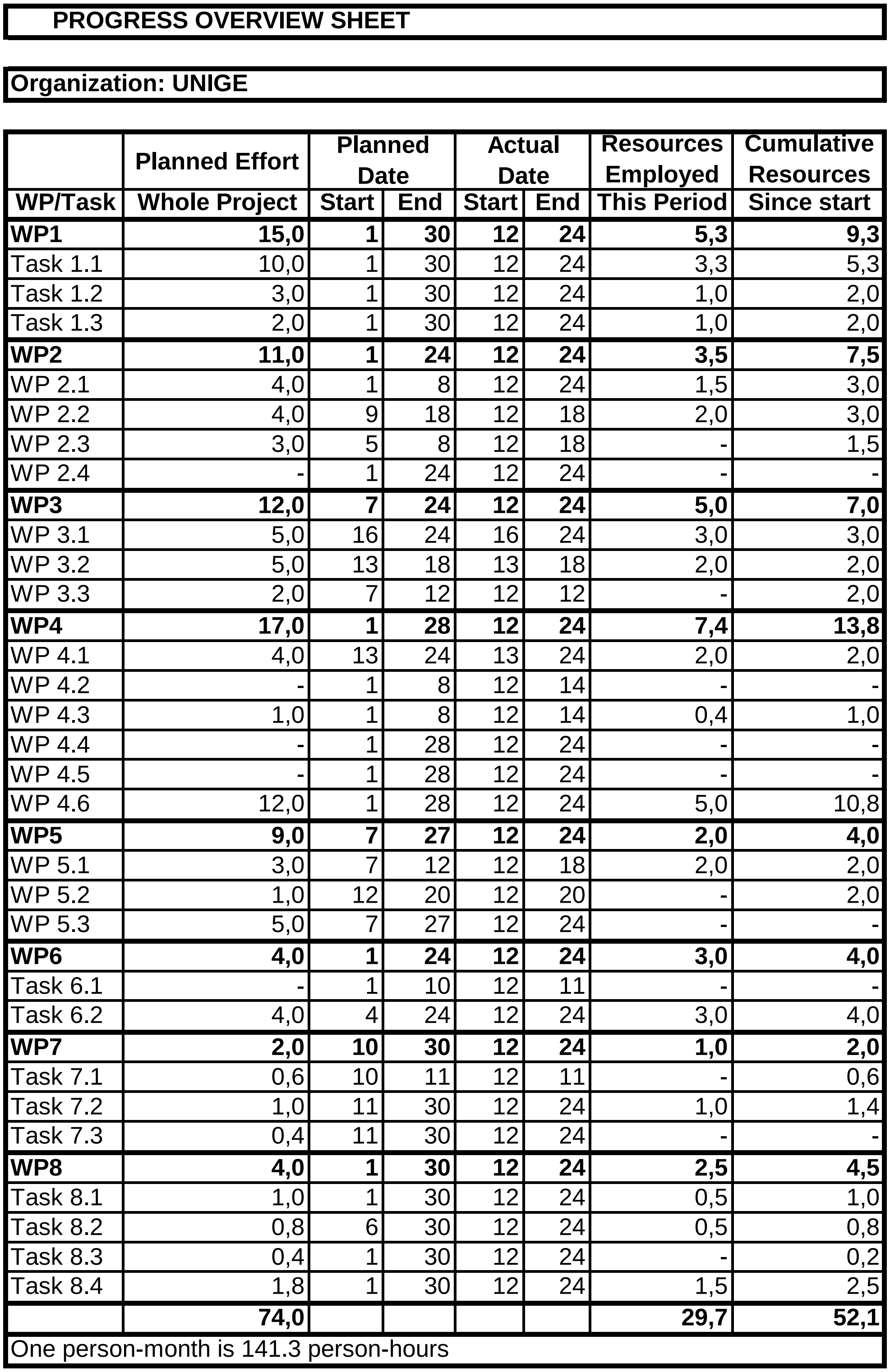
Partners owning: UNIGE
Partners contributed: ETHZ, INRIA, Siemens
Made available to: public

2.5 Comparison of planned activities and actual work accomplished

The activity within the project 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 01.01.2004 — 31.12.2004

	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	**4,5**	**5,3**	**15**	**9,3**	**0,3**	**0,4**	**1**	**0,8**	**0,4**	**0,4**	**1**	**0,8**	**0,4**	**0,4**	**1**	**0,8**
Task 1.1	3,5	3,3	10	5,3	0	0	0	0	0	0	0	0	0	0	0	0
Task 1.2	0,6	1	3	2	0,3	0,4	1	0,8	0,4	0,4	1	0,8	0,4	0,4	1	0,8
Task 1.3	0,4	1	2	2	0	0	0	0	0	0	0	0	0	0	0	0
WP2	**3**	**3,5**	**11**	**7,5**	**5**	**6**	**22**	**16**	**5**	**3**	**13**	**11**	**0,3**	**4,4**	**2**	**7,2**
WP 2.1	0	1,5	4	3	0	0	8	8	0	0	3	3	0	4,2	1	6,2
WP 2.2	3	2	4	3	2	2	5	3	3	2	5	4	0,3	0	0,5	0,3
WP 2.3	0	0	3	1,5	0	1	3	2	0	1	3	4	0	0,2	0,5	0,7
WP 2.4	0	0	0	0	3	3	6	3	2	0	2	0	0	0	0	0
WP3	**10**	**5**	**12**	**7**	**15**	**13**	**15**	**13**	**10**	**10**	**15**	**14**	**6,5**	**2**	**7**	**3**
WP 3.1	5	3	5	3	8	6	8	6	5	5	6	5	4	1	4	1
WP 3.2	5	2	5	2	7	7	7	7	5	5	5	5	2,5	0,5	2,5	1,5
WP 3.3	0	0	2	2	0	0	0	0	0	0	4	4	0	0,5	0,5	0,5
WP4	**8**	**7,4**	**17**	**14**	**1**	**1**	**6**	**3**	**3**	**4**	**17**	**13**	**0**	**0,5**	**0**	**0,5**
WP 4.1	4	2	4	2	0	0	0	0	1	1	4	1	0	0	0	0
WP 4.2	0	0	0	0	0	0	0	0	0	0,5	4	4,5	0	0	0	0
WP 4.3	0	0,4	1	1	0	0	1	1	0	0	4	3	0	0	0	0
WP 4.4	0	0	0	0	0	0	0	0	2	2,5	5	4,5	0	0,5	0	0,5
WP 4.5	0	0	0	0	1	1	5	2	0	0	0	0	0	0	0	0
WP 4.6	4	5	12	11	0	0	0	0	0	0	0	0	0	0	0	0
WP5	**1**	**2**	**9**	**4**	**2,5**	**3**	**8**	**6**	**3**	**3**	**8**	**6**	**1,5**	**0**	**3**	**0**
WP 5.1	0	2	3	2	0	0	2	2	0	0	3	3	0	0	1,5	0
WP 5.2	1	0	1	2	2	2,5	3	3	3	3	3	3	1,5	0	1,5	0
WP 5.3	0	0	5	0	0,5	0,5	3	1	0	0	2	0	0	0	0	0
WP6	**0**	**3**	**4**	**4**	**1**	**1,8**	**2**	**2**	**2**	**3**	**4**	**5**	**8,7**	**7,1**	**18**	**16**
Task 6.1	0	0	0	0	0	0	0	0	0	0	0	0	0	1,1	6	4,1
Task 6.2	0	3	4	4	1	1,8	2	2	2	3	4	5	8,7	6	12	12
WP7	**0,1**	**1**	**2**	**2**	**0,5**	**0,8**	**2**	**1,1**	**0,9**	**0,9**	**2**	**1,3**	**0,4**	**3,2**	**2**	**3,2**
Task 7.1	0	0	0,6	0,6	0	0	0	0	0	0	0	0	0	0	0	0
Task 7.2	0,1	1	1	1,4	0,3	0,3	1	0,6	0,4	0,4	1	0,8	0,4	3,2	2	3,2
Task 7.3	0	0	0,4	0	0,2	0,5	1	0,5	0,5	0,5	1	0,5	0	0	0	0
WP8	**0,4**	**2,5**	**4**	**4,5**	**0,7**	**1,4**	**4**	**2,8**	**1,4**	**1,4**	**4**	**2,8**	**0,6**	**1,4**	**3**	**2,6**
Task 8.1	0	0,5	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Task 8.2	0	0,5	0,8	0,8	0,2	0,4	1	0,8	0,4	0,4	1	0,8	0,3	0,7	1,5	1,2
Task 8.3	0	0	0,4	0,2	0	0	0	0	0	0	0	0	0,1	0,2	0,5	0,4
Task 8.4	0,4	1,5	1,8	2,5	0,5	1	3	2	1	1	3	2	0,2	0,5	1	1



PROGRESS OVERVIEW SHEET

Organization: UNIGE

	Planned Effort	**Planned Date**		**Actual Date**		**Resources Employed**	**Cumulative Resources**
WP/Task	**Whole Project**	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP1	**15,0**	**1**	**30**	**12**	**24**	**5,3**	**9,3**
Task 1.1	10,0	1	30	12	24	3,3	5,3
Task 1.2	3,0	1	30	12	24	1,0	2,0
Task 1.3	2,0	1	30	12	24	1,0	2,0
WP2	**11,0**	**1**	**24**	**12**	**24**	**3,5**	**7,5**
WP 2.1	4,0	1	8	12	24	1,5	3,0
WP 2.2	4,0	9	18	12	18	2,0	3,0
WP 2.3	3,0	5	8	12	18	-	1,5
WP 2.4	-	1	24	12	24	-	-
WP3	**12,0**	**7**	**24**	**12**	**24**	**5,0**	**7,0**
WP 3.1	5,0	16	24	16	24	3,0	3,0
WP 3.2	5,0	13	18	13	18	2,0	2,0
WP 3.3	2,0	7	12	12	12	-	2,0
WP4	**17,0**	**1**	**28**	**12**	**24**	**7,4**	**13,8**
WP 4.1	4,0	13	24	13	24	2,0	2,0
WP 4.2	-	1	8	12	14	-	-
WP 4.3	1,0	1	8	12	14	0,4	1,0
WP 4.4	-	1	28	12	24	-	-
WP 4.5	-	1	28	12	24	-	-
WP 4.6	12,0	1	28	12	24	5,0	10,8
WP5	**9,0**	**7**	**27**	**12**	**24**	**2,0**	**4,0**
WP 5.1	3,0	7	12	12	18	2,0	2,0
WP 5.2	1,0	12	20	12	20	-	2,0
WP 5.3	5,0	7	27	12	24	-	-
WP6	**4,0**	**1**	**24**	**12**	**24**	**3,0**	**4,0**
Task 6.1	-	1	10	12	11	-	-
Task 6.2	4,0	4	24	12	24	3,0	4,0
WP7	**2,0**	**10**	**30**	**12**	**24**	**1,0**	**2,0**
Task 7.1	0,6	10	11	12	11	-	0,6
Task 7.2	1,0	11	30	12	24	1,0	1,4
Task 7.3	0,4	11	30	12	24	-	-
WP8	**4,0**	**1**	**30**	**12**	**24**	**2,5**	**4,5**
Task 8.1	1,0	1	30	12	24	0,5	1,0
Task 8.2	0,8	6	30	12	24	0,5	0,8
Task 8.3	0,4	1	30	12	24	-	0,2
Task 8.4	1,8	1	30	12	24	1,5	2,5
	74,0					**29,7**	**52,1**

One person-month is 141.3 person-hours

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	• Detailed planning and scheduling of project activities • Correspondence with Project Officer • Maintenance of concurrent versioning system for distributed management of software and documentation
Task 1.2	• Organisation of the 2nd AVISPA Synchronisation Meeting • Organisation of the AVISPA meeting held in Cork on July 7, 2004 • Organisation of the 3rd AVISPA Synchronisation Meeting • Organisation of the AVISPA meeting held in München on 15-17.12.2004
Task 1.3	• Budgetary overviews • Management of cost statements
WP2	
WP 2.1	• Definition of the formal semantics of 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	• Authentication properties
WP 3.2	• Compound Typing
WP 3.3	
WP4	
WP 4.1	• Analysis of the related work on compositionality
WP 4.2	
WP 4.3	
WP 4.4	
WP 4.5	
WP 4.6	• Protocol Verification in SATMC • Support to Compound Types in SATMC • Optimised Intruder Model in SATMC
WP5	
WP 5.1	• Abstraction in SAT-based model-checking
WP 5.2	• Model-checking of time-sensitive security protocols
WP 5.3	
WP6	
Task 6.1	
Task 6.2	• Formal specification of selected problems
WP7	
Task 7.1	
Task 7.2	• Assessment of the AVISPA Tool v.2
Task 7.3	
WP8	
Task 8.1	
Task 8.2	• Organisation of the 2nd Year Project Workshop • Organisation of Project Meetings
Task 8.3	
Task 8.4	• Writing of scientific publications

Deliverables due this period

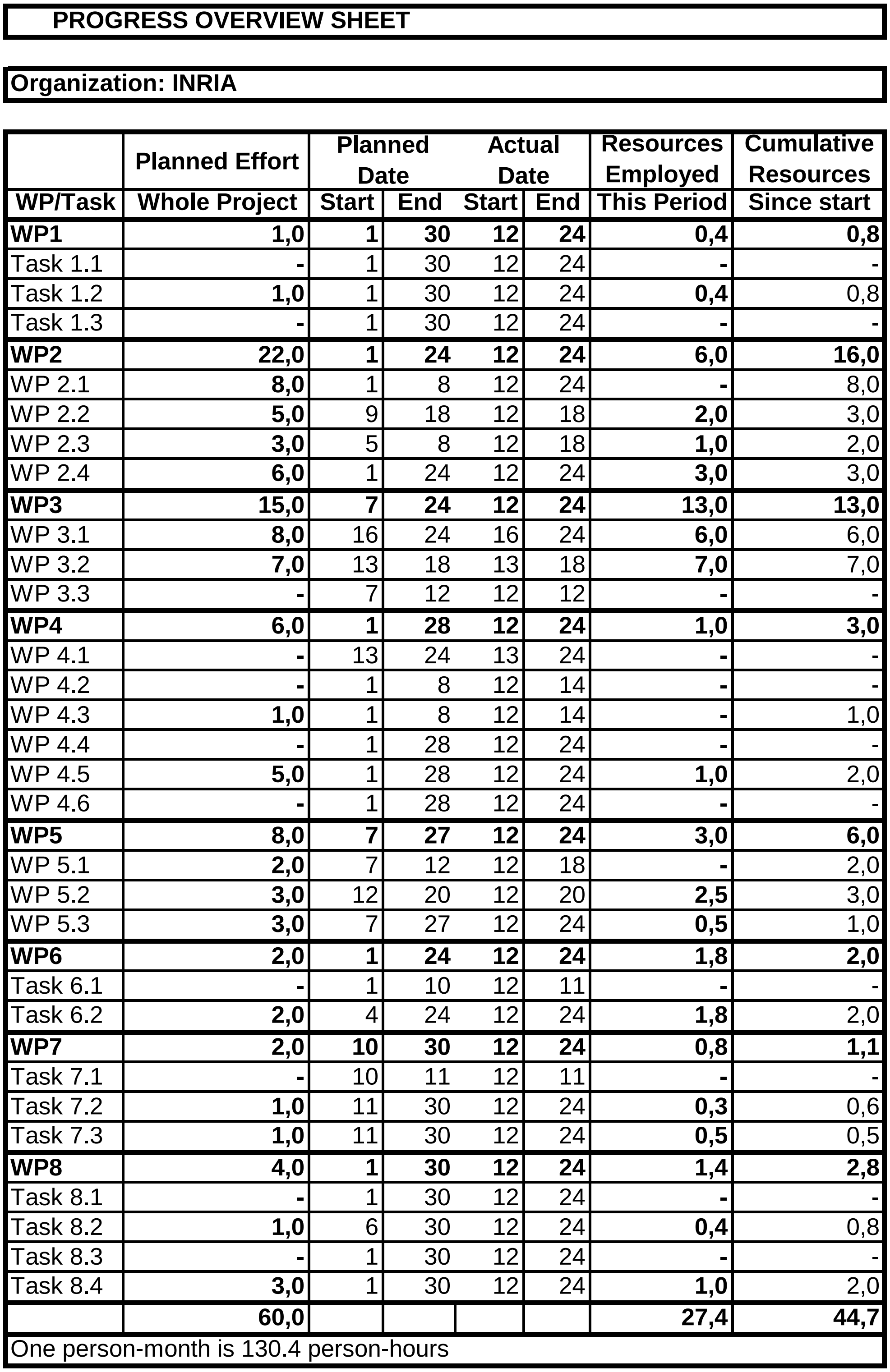
Number	Title	Status
D1.2	Periodic Progress Report N°: 2	Final
D7.3	Assessment of AVISPA Tool v.2	Final
D8.4	Year 1 Project Workshop	Final
D8.5	Year 2 Project Workshop	Final

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

1. A. Armando and L. Compagna. An Optimized Intruder Model for SAT-based Model-Checking of Security Protocols. In *Proceedings of ARSPA'04*, 2004. Available at `www.avispa-project.org`
2. A. Armando and L. Compagna. SATMC: a SAT-based Model Checker for Security Protocols. In *Proceedings of 9th European Conference on Logics in Artificial Intelligence (JELIA'04)*, September 27-30, 2004, Lisbon, Portugal. Springer-Verlag, 2004. Available at `www.avispa-project.org`.
3. A. Armando, L. Compagna, and Y. Lierler. Automatic Compilation of Protocol Insecurity Problems into Logic Programming. In *Proceedings of 9th European Conference on Logics in Artificial Intelligence (JELIA'04)*, September 27-30, 2004, Lisbon, Portugal. Springer-Verlag, 2004. Available at `www.avispa-project.org`.
4. G. Delzanno and P. Ganty. Automatic Verification of Time Sensitive Cryptographic Protocols. In Proceedings of the 10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2004). Barcelona, Spain, March 29 - April 2, 2004.
5. Alessandro Armando and Luca Viganò, editors of *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04)*. Electronic Notes in Computer Science, Elsevier Science, in print. Preprint available at `www.avispa-project.org/arspa` and `www.avispa-project.org`.
6. Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Mödersheim, Laurent Vigneron. A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. In *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS'04)*, Automated Software Engineering n. 180, pages 193–205. Austrian Computer Society, 2004. Available at `www.avispa-project.org`
7. Organisation of ARSPA'04: the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
8. Organisation of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`
9. Talks on the AVISPA Project and the SATMC back-end at IRST, Trento.

Planned actions for the next period

- Design and development of domain specific encodings for SATMC.
- Compositional reasoning.
- Development of AVISPA Tool v.3.
- Assessment of AVISPA Tool v.3.
- Writing of the Technology Implementation Plan.
- Project Management.
- Writing of scientific publications.
- Editing of the Special Issue of the Journal of Automated Reasoning on "Automated Reasoning for Security Protocol Analysis".
- Presentation of AVISPA in a plenary session at 62nd IETF Meeting that will be held in Minneapolis on March 6-11, 2005.



PROGRESS OVERVIEW SHEET

Organization: INRIA

	Planned Effort	Planned Date		Actual Date		Resources Employed	Cumulative Resources
WP/Task	**Whole Project**	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP1	**1,0**	**1**	**30**	**12**	**24**	**0,4**	**0,8**
Task 1.1	-	1	30	12	24	-	-
Task 1.2	1,0	1	30	12	24	0,4	0,8
Task 1.3	-	1	30	12	24	-	-
WP2	**22,0**	**1**	**24**	**12**	**24**	**6,0**	**16,0**
WP 2.1	8,0	1	8	12	24	-	8,0
WP 2.2	5,0	9	18	12	18	2,0	3,0
WP 2.3	3,0	5	8	12	18	1,0	2,0
WP 2.4	6,0	1	24	12	24	3,0	3,0
WP3	**15,0**	**7**	**24**	**12**	**24**	**13,0**	**13,0**
WP 3.1	8,0	16	24	16	24	6,0	6,0
WP 3.2	7,0	13	18	13	18	7,0	7,0
WP 3.3	-	7	12	12	12	-	-
WP4	**6,0**	**1**	**28**	**12**	**24**	**1,0**	**3,0**
WP 4.1	-	13	24	13	24	-	-
WP 4.2	-	1	8	12	14	-	-
WP 4.3	1,0	1	8	12	14	-	1,0
WP 4.4	-	1	28	12	24	-	-
WP 4.5	5,0	1	28	12	24	1,0	2,0
WP 4.6	-	1	28	12	24	-	-
WP5	**8,0**	**7**	**27**	**12**	**24**	**3,0**	**6,0**
WP 5.1	2,0	7	12	12	18	-	2,0
WP 5.2	3,0	12	20	12	20	2,5	3,0
WP 5.3	3,0	7	27	12	24	0,5	1,0
WP6	**2,0**	**1**	**24**	**12**	**24**	**1,8**	**2,0**
Task 6.1	-	1	10	12	11	-	-
Task 6.2	2,0	4	24	12	24	1,8	2,0
WP7	**2,0**	**10**	**30**	**12**	**24**	**0,8**	**1,1**
Task 7.1	-	10	11	12	11	-	-
Task 7.2	1,0	11	30	12	24	0,3	0,6
Task 7.3	1,0	11	30	12	24	0,5	0,5
WP8	**4,0**	**1**	**30**	**12**	**24**	**1,4**	**2,8**
Task 8.1	-	1	30	12	24	-	-
Task 8.2	1,0	6	30	12	24	0,4	0,8
Task 8.3	-	1	30	12	24	-	-
Task 8.4	3,0	1	30	12	24	1,0	2,0
	60,0					**27,4**	**44,7**

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 • Organisation of the first AVISPA workshop in January 2004
Task 1.3	
WP2	
WP 2.1	
WP 2.2	• Addition of axioms in the specification languages
WP 2.3	• Improvements of the syntax and semantics of the IF
WP 2.4	• Design and development of a graphical interface runable on the web
WP3	
WP 3.1	• Formalisation of security properties and description of their representation in HLPSL
WP 3.2	• Definition of compound typing in HLPSL and IF • Definition of Oracle rules for extending the Intruder's deduction abilities
WP 3.3	
WP4	
WP 4.1	• Analysis of the related work on compositionality
WP 4.2	
WP 4.3	
WP 4.4	
WP 4.5	• Improvement of the implementation of CL-AtSe
WP 4.6	
WP5	
WP 5.1	
WP 5.2	• Definition of tree automata approximations • Implementation of TA4SP
WP 5.3	• Study of the completeness of the tree automata approach
WP6	
Task 6.1	
Task 6.2	• Formal specification of selected problems
WP7	
Task 7.1	
Task 7.2	• Preparation of the assessment of AVISPA Tool v.2
Task 7.3	• Identification of protocols classes that cannot yet be handled by CL-AtSe
WP8	
Task 8.1	
Task 8.2	• Organisation of the first and second AVISPA workshops
Task 8.3	
Task 8.4	• Writing of scientific publications

Deliverables due this period

Number	Title	Status
D2.2	Algebraic Properties	Final
D2.4	Interface	Final
D5.2	Infinite-state model checking	Final

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

1. Y. Chevalier, L. Vigneron. Strategy for Verifying Security Protocols with Unbounded Message Size. Journal of Automated Software Engineering 11, 2, April 2004, p. 141–166.
2. Y. Boichut, P.-C. Heam, O. Kouchnarenko, F. Oehl. Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In *Proc. Int. Workshop on Automated Verification of Infinite-State Systems (AVIS'2004), joint to ETAPS'04*, p. 1–11, Barcelona, Spain, 2004. The final version will be published in ENTCS, Elsevier.
3. Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, J. Mantovani, S. Mödersheim, L. Vigneron. A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. In *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS'04)*, Automated Software Engineering n. 180, pages 193–205. Austrian Computer Society, 2004. Available at `www.avispa-project.org`

4 Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani. Deciding the Security of Protocols with Commuting Public Key Encryption. In *Workshop on Automated Reasoning for Security Protocol Analysis - ARSPA'2004, Electronic Notes in Theoretical Computer Science - ENTCS*, Cork, Ireland, Jul 2004.

5 Y. Chevalier, L. Vigneron. Rule-based Programs describing Internet Security Protocols. In *5th Int. Workshop on Rule-Based Programming (RULE)*, S. Abdennadher, C. Ringeissen (editors), Aachen, Germany, June 2004.

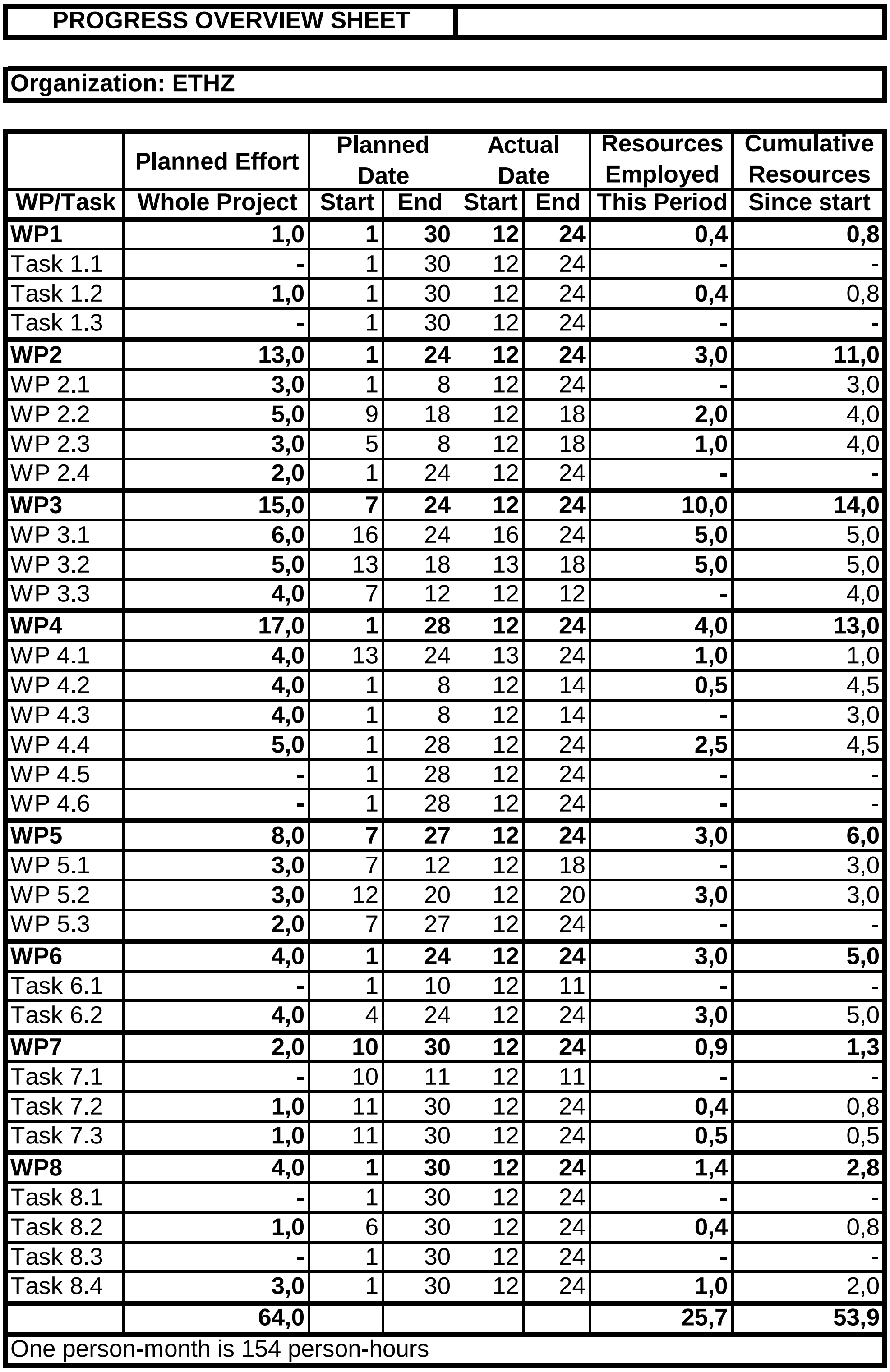
6 Y. Chevalier. A Simple Constraint Combination Procedure for Cryptographic Protocols with Xor. In *18th Int. Workshop on Unification*, M. Kohlhase (editor), Cork, Ireland, July 2004. Long version available as INRIA Research Report RR-5224.

7 M. Rusinowitch. A Decidable Analysis of Security Protocols. In *18th IFIP World Computer Congress on Theoretical Computer Science - TCS'2004*, J.-J. Lévy, E. Mayr, J. Mitchell (editors), Kluwer Academic Publishers, Toulouse, France, August 2004. Invited talk.

8 L. Vigneron. Automatic Verification of Security Protocols. In *18th Int. Workshop on Unification*, M. Kohlhase (editor), Cork, Ireland, July 2004. Invited talk.

Planned actions for the next period

- Improvement of CL-AtSe for a better te of algebraic properties.
- Design of a more complete graphical interface for a better use of the AVISPA Tool.
- Formal definition and implementation of new goals.
- Complete integration of the tree automata abstraction in the AVISPA Tool.
- Scientific publications and dissemination of results.
- Editing of the Special Issue of the Journal of Automated Reasoning on "Automated Reasoning for Security Protocol Analysis"



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**	**12**	**24**	**0,4**	**0,8**
Task 1.1	**-**	1	30	12	24	**-**	-
Task 1.2	**1,0**	1	30	12	24	**0,4**	0,8
Task 1.3	**-**	1	30	12	24	**-**	-
WP2	**13,0**	**1**	**24**	**12**	**24**	**3,0**	**11,0**
WP 2.1	**3,0**	1	8	12	24	**-**	3,0
WP 2.2	**5,0**	9	18	12	18	**2,0**	4,0
WP 2.3	**3,0**	5	8	12	18	**1,0**	4,0
WP 2.4	**2,0**	1	24	12	24	**-**	-
WP3	**15,0**	**7**	**24**	**12**	**24**	**10,0**	**14,0**
WP 3.1	**6,0**	16	24	16	24	**5,0**	5,0
WP 3.2	**5,0**	13	18	13	18	**5,0**	5,0
WP 3.3	**4,0**	7	12	12	12	**-**	4,0
WP4	**17,0**	**1**	**28**	**12**	**24**	**4,0**	**13,0**
WP 4.1	**4,0**	13	24	13	24	**1,0**	1,0
WP 4.2	**4,0**	1	8	12	14	**0,5**	4,5
WP 4.3	**4,0**	1	8	12	14	**-**	3,0
WP 4.4	**5,0**	1	28	12	24	**2,5**	4,5
WP 4.5	**-**	1	28	12	24	**-**	-
WP 4.6	**-**	1	28	12	24	**-**	-
WP5	**8,0**	**7**	**27**	**12**	**24**	**3,0**	**6,0**
WP 5.1	**3,0**	7	12	12	18	**-**	3,0
WP 5.2	**3,0**	12	20	12	20	**3,0**	3,0
WP 5.3	**2,0**	7	27	12	24	**-**	-
WP6	**4,0**	**1**	**24**	**12**	**24**	**3,0**	**5,0**
Task 6.1	**-**	1	10	12	11	**-**	-
Task 6.2	**4,0**	4	24	12	24	**3,0**	5,0
WP7	**2,0**	**10**	**30**	**12**	**24**	**0,9**	**1,3**
Task 7.1	**-**	10	11	12	11	**-**	-
Task 7.2	**1,0**	11	30	12	24	**0,4**	0,8
Task 7.3	**1,0**	11	30	12	24	**0,5**	0,5
WP8	**4,0**	**1**	**30**	**12**	**24**	**1,4**	**2,8**
Task 8.1	**-**	1	30	12	24	**-**	-
Task 8.2	**1,0**	6	30	12	24	**0,4**	0,8
Task 8.3	**-**	1	30	12	24	**-**	-
Task 8.4	**3,0**	1	30	12	24	**1,0**	2,0
	64,0					**25,7**	**53,9**

One person-month is 154 person-hours

Main contribution during this period	
WP/Task	**Action**
WP1	
Task 1.1	
Task 1.2	• Organisation of and participation in the project meetings.
WP2	
WP 2.1	• Formal definition of the HLPSL.
WP 2.2	• Integration of algebraic properties.
WP 2.3	• Formal definition of the IF.
WP 2.4	• Formal definition of the Output Format.
WP3	
WP 3.1	• Reduction of standard security goals to authentication and secrecy. • Formalisation of various security properties.
WP 3.2	• Investigation of different assumptions on the environment. • Compound Typing. • A novel approach to the analysis of guessing attacks. • Definition of a distributed temporal logic for the specification of object and meta level protocol properties.
WP 3.3	
WP4	
WP 4.1	• Analysis of the related work on compositionality
WP 4.2	• Further improvements of Constraint Differentiation, a POR-inspired technique for the symbolic approach.
WP 4.3	• Further improvements of the heuristics.
WP 4.4	• Extension and improvement of the OFMC back-end.
WP 4.5	
WP 4.6	
WP5	
WP 5.1	• Finer definition of the abstraction techniques. • Protocol Verification in OFMC (further implementation of OFMC/FP, the 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 set of selected problems
WP7	
Task 7.1	
Task 7.2	• Assessment of the AVISPA Tool v.2
Task 7.3	
WP8	
Task 8.1	
Task 8.2	Organisation of the ARSPA'04 workshop. Organisation of the ARSPA'05 workshop.
Task 8.3	
Task 8.4	• Writing of scientific publications • Organisation of the tutorials AVASP'04 and AVASP'05.

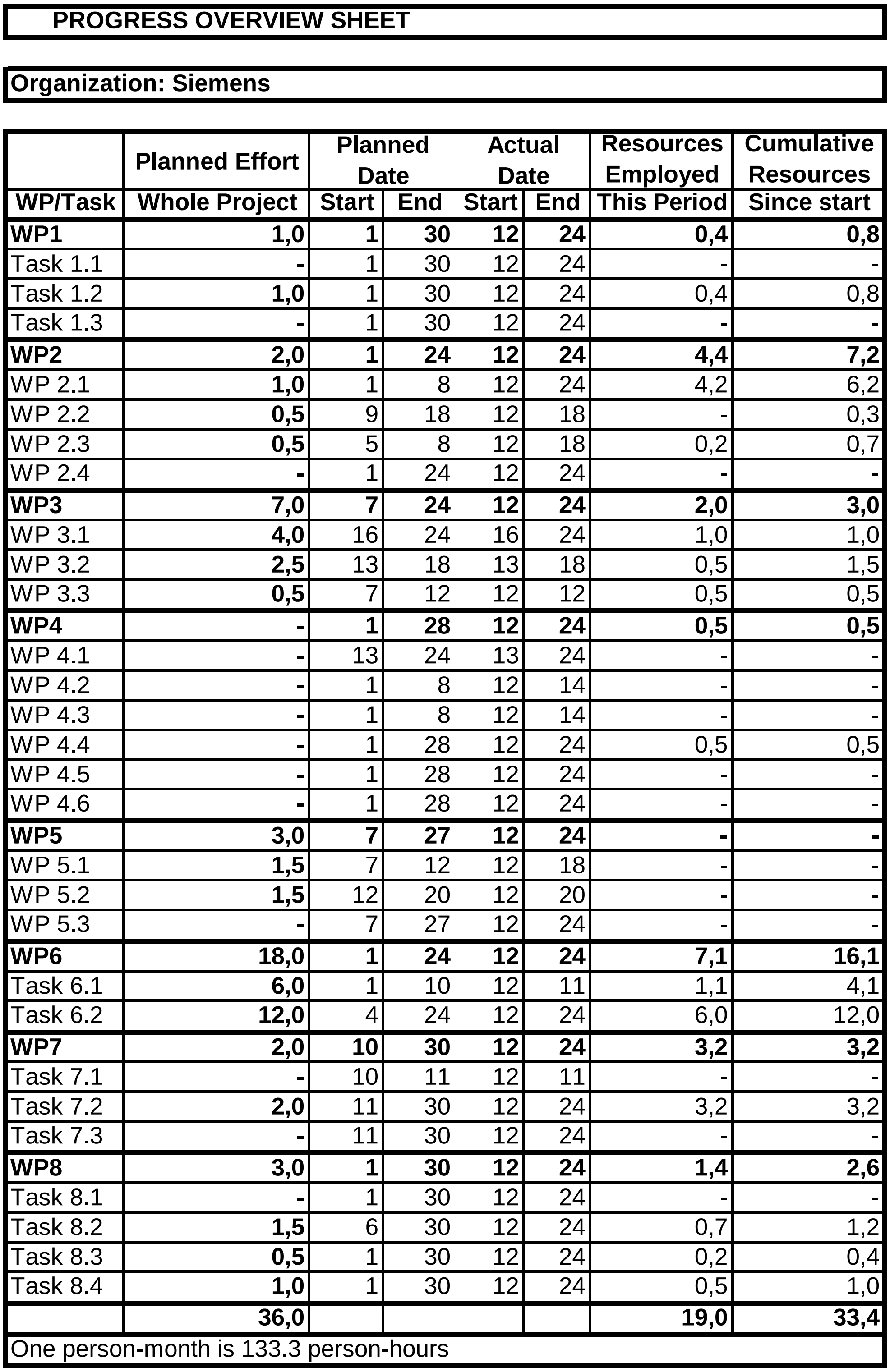
Deliverables due this period

Number	Title	Status
D3.1	Security Properties	Final
D3.2	Assumptions on Environment	Final
D4.5	AVISPA Tool v.2	Final

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

1. Paul Hankes Drielsma and Sebastian Mödersheim. The ASW Protocol Revisited: A Unified View. In A. Armando and L. Viganò, editors, *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04).* Electronic Notes in Computer Science, Elsevier Science, in print. Preprint available at `www.avispa-project.org/arspa` and `www.avispa-project.org`
2. Carlos Caleiro, Luca Viganò, David Basin. Metareasoning about Security Protocols using Distributed Temporal Logic. In A. Armando and L. Viganò, editors, *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04).* Electronic Notes in Computer Science, Elsevier Science, in print. Preprint available at `www.avispa-project.org/arspa` and `www.avispa-project.org`
3. Carlos Caleiro, Luca Viganò, David Basin. Towards a Metalogic for Security Protocol Analysis. In W.A. Carnielli, F.M. Dionísio, P. Mateus, editors, *Proceedings of the Workshop on the Combination of Logics: Theory and Applications (Comblog'04)*, pages 187–196. ISBN 972-99289-0-8, Center for Logic and Computation, Departamento de Matemática, Instituto Superior Técnico, Lisbon, Portugal, 2004. Available at `www.avispa-project.org`
4. Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Mödersheim, Laurent Vigneron. A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. In *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS'04)*, Automated Software Engineering n. 180, pages 193–205. Austrian Computer Society, 2004. Available at `www.avispa-project.org`
5. David Basin, Sebastian Mödersheim, Luca Viganò. OFMC: A symbolic model checker for security protocols. *International Journal of Information Security.* Springer-Verlag, 2004. Available at `www.avispa-project.org`
6. Alessandro Armando and Luca Viganò, editors of *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04).* Electronic Notes in Computer Science, Elsevier Science, in print. Preprint available at `www.avispa-project.org/arspa` and `www.avispa-project.org`
7. Organisation of ARSPA'04: the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
8. Editing of the special issue of the Journal of Automated Reasoning (JAR) on "Automated Reasoning for Security Protocol Analysis". See `www.avispa-project.org/arspa`
9. Organisation of ARSPA'05: the ICALP 2005 Workshop on Automated Reasoning for Security Protocol Analysis. See `www.avispa-project.org/arspa`
10. Organisation of AVASP'04: the IJCAR'04 Tutorial on Automated Validation of Security Protocols. See `www.avispa-project.org/avasp`
11. Organisation of AVASP'05: the ETAPS 2005 Tutorial on Automated Validation of Security Protocols. See `www.avispa-project.org/avasp`
12. Invited talk on the OFMC back-end and the AVISPA Project at the Faculty of Mathematics of the University of Bologna, Italy, October 25th, 2004.
13. Invited talk on the OFMC back-end and the AVISPA Project at the Dagstuhl Seminar "SPP". Dagstuhl, Germany, November 5th – 10th, 2004.

Planned actions for the next period
• 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. • Extension of the guessing intruder. • Techniques for infinite-state symbolic model-checking and extension of OFMC for the analysis of infinite numbers of sessions. • Support to compositional reasoning. • Formalisation of selected problems in HLPSL. • Development of the AVISPA Tool v.3. • Assessment of the AVISPA Tool v.3 • Organisation of the 3nd Year Project Workshop, the ICALP 2005 workshop ARSPA'05 (`www.avispa-project.org/arspa`). • Organisation of the ETAPS'05 tutorial AVASP'05 (`www.avispa-project.org/avasp`). • Editing of the Special Issue of the Journal of Automated Reasoning on "Automated Reasoning for Security Protocol Analysis". • 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**	**12**	**24**	**0,4**	**0,8**
Task 1.1	**-**	1	30	12	24	-	-
Task 1.2	**1,0**	1	30	12	24	0,4	0,8
Task 1.3	**-**	1	30	12	24	-	-
WP2	**2,0**	**1**	**24**	**12**	**24**	**4,4**	**7,2**
WP 2.1	**1,0**	1	8	12	24	4,2	6,2
WP 2.2	**0,5**	9	18	12	18	-	0,3
WP 2.3	**0,5**	5	8	12	18	0,2	0,7
WP 2.4	**-**	1	24	12	24	-	-
WP3	**7,0**	**7**	**24**	**12**	**24**	**2,0**	**3,0**
WP 3.1	**4,0**	16	24	16	24	1,0	1,0
WP 3.2	**2,5**	13	18	13	18	0,5	1,5
WP 3.3	**0,5**	7	12	12	12	0,5	0,5
WP4	**-**	**1**	**28**	**12**	**24**	**0,5**	**0,5**
WP 4.1	**-**	13	24	13	24	-	-
WP 4.2	**-**	1	8	12	14	-	-
WP 4.3	**-**	1	8	12	14	-	-
WP 4.4	**-**	1	28	12	24	0,5	0,5
WP 4.5	**-**	1	28	12	24	-	-
WP 4.6	**-**	1	28	12	24	-	-
WP5	**3,0**	**7**	**27**	**12**	**24**	**-**	**-**
WP 5.1	**1,5**	7	12	12	18	-	-
WP 5.2	**1,5**	12	20	12	20	-	-
WP 5.3	**-**	7	27	12	24	-	-
WP6	**18,0**	**1**	**24**	**12**	**24**	**7,1**	**16,1**
Task 6.1	**6,0**	1	10	12	11	1,1	4,1
Task 6.2	**12,0**	4	24	12	24	6,0	12,0
WP7	**2,0**	**10**	**30**	**12**	**24**	**3,2**	**3,2**
Task 7.1	**-**	10	11	12	11	-	-
Task 7.2	**2,0**	11	30	12	24	3,2	3,2
Task 7.3	**-**	11	30	12	24	-	-
WP8	**3,0**	**1**	**30**	**12**	**24**	**1,4**	**2,6**
Task 8.1	**-**	1	30	12	24	-	-
Task 8.2	**1,5**	6	30	12	24	0,7	1,2
Task 8.3	**0,5**	1	30	12	24	0,2	0,4
Task 8.4	**1,0**	1	30	12	24	0,5	1,0
	36,0					**19,0**	**33,4**

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

<table>
<tr><th colspan="3">Deliverables due this period</th></tr>
<tr><th>Number</th><th>Title</th><th>Status</th></tr>
<tr><td>D6.1</td><td>List of selected problems</td><td>Final</td></tr>
<tr><th colspan="3">Dissemination actions (articles, workshops, conferences, etc.)</th></tr>
<tr><td colspan="3">1. J. Cuellar. On the Security of Internet Protocols. Invited talk at the 7th Meeting of the SPP Security, 24-26 November 2004 in Castle Dagstuhl. See also http://www.telematik.uni-freiburg.de/spps/spp_treffen.php?spp_id=7.
2. Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, J. Mantovani, S. Mödersheim and L. Vigneron. A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. Talk by J. Cuellar at the Workshop on Specification and Automated Processing of Security Requirements - SAPS'04. http://polaris.lcc.uma.es/SAPS04/program.html</td></tr>
<tr><th colspan="3">Planned actions for the next period</th></tr>
<tr><td colspan="3">• Update and extend the library of formalised problems in HLPSL.
• Contribute to documentation of HLPSL and the tool.
• Produce a modeler's tutorial.
• Scientific publications and presentations, in particular on the formal semantics of HLPSL.
• Presentation at ETAPS 2005 tutorial, Edinburgh, 3rd April 2005.
• Further dissemination of results.</td></tr>
</table>

2.6 State-of-the-art update

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

For instance, there has been a lot of activity this year on detecting attacks in the context of models that generalise the standard Dolev-Yao intruder model. Decision procedure for handling guessing attacks and algebraic properties have been proposed [43, 42, 50]. These extensions are closely related to some AVISPA results and have been and will be taken into consideration in our future plans. There has also been an interesting advance [46] in relating formal models and computational models. We have already started to investigate how to integrate these results in our approach.

2.6.1 The Project PROUVE

The French project PROUVE has started this year and INRIA-Lorraine is a partner of this project (administrative coordinator), together with France Telecom R&D, laboratories LSV (ENS de Cachan, France) and Verimag (Grenoble, France). The objective of PROUVE project is to verify security-sensitive protocols provided by France Telecom R&D. Like for the AVISPA Tool, the PROUVE platform will rely on a high-level specification language close to the language used in textbooks. Three tools will be applied to the case-studies: H1 (LSV), Hermes (Verimag) [40] and CL-AtSe. In contrast to AVISPA, PROUVE is oriented towards the specific applications provided by France Telecom R&D.

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

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

Moreover, we have invited Yassine Lakhnech of Verimag to present their results at the AVISPA workshop held on January 23, 2004, in Nancy. People from Verimag have attended the IJCAR Workshop ARSPA. We have frequent contacts with LSV Cachan, too, with many reciprocal visits.

2.6.2 ECSS Group, Eindhoven

The Eindhoven Computer Science Security Group (led by Prof. Sjouke Mauw) has been working on the formal verification of black box security protocols, which is closely related to our research. Their approach is based on process algebra and on the μCRL language, which allows one to combine data and processes. The approach is quite similar to the model-checking one of CASPER. In general some approximations have to be done and there is no guarantee that an attack was not overlooked [45]. They have not investigated completeness of their approach.

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

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

2.6.3 Blanchet's Logic Programming Approach

Bruno Blanchet (MPI for computer science, Saarbrücken, Germany, and ENS, France) has developed a tool where protocols and security properties are expressed as Horn clauses and he provides strategies to saturate these sets of clauses [30, 35, 36, 37]. The tool allows one to prove security properties for an unbounded number of sessions, in particular strong secrecy (which means that an intruder cannot see any difference when the value of the secret changes). Note, however, that the tool may raise some false attack since nonces are abstracted by constants or function symbols, so that attacks have to be constructed by the user itself.

Action taken We shall invite Bruno Blanchet to share his experience in our third year workshop, ARSPA'05.

2.6.4 The Project DEGAS

A related European project, DEGAS IST-2001-32072 (`http://www.omnys.it/degas/`), is dedicated to the design of an environment for developing global applications. For instance, a case study considered in this project is mobile home-banking. The specification language is UML and the abstract language for verification tasks is based on process algebra. The related Italian project Mefisto (`http://mefisto.web.cs.unibo.it`) on formal methods for security ended in November 2003. In particular, this project has attempted to extend protocol verification to more realistic and detailed models including time and probabilistic information flow.

In the context of these projects, a translation has been designed from Alice&Bob protocol notation to a process algebra that is similar to the spi-calculus [38]. This translation allows one to derive a precise description of the protocol behaviour, and is similar to translations previously devised for CAPSL/CIL [44], CASRUL [39], 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 [38], the approach does not address asymmetric cryptography, imperfect cryptography, timing issues, type flaw attacks related to bit-string representations. All these topics are currently investigated by the AVISPA project.

Action to be taken We have invited some of the principal investigators of the DEGAS project to our next workshop: Pierpaolo Degano of the University of Pisa will co-chair the ARSPA'05 workshop together with Luca Viganò of ETHZ, and Hanne Riis Nielson of the Technical University of Denmark has joined the program committee of the workshop. Moreover, we have begun a detailed comparison of the approach of the DEGAS project with our abstraction techniques, and in particular with the tree automata techniques discussed in [33]. We believe that it will be possible for them to reuse our technology, which is more efficient according to the experimental results.

2.6.5 The CAPSL Environment

In the past four years, Jonathan Millen from SRI International, the main developer of the CAPSL environment, has been regularly collaborating with David Basin's group at ETHZ, closely following our project's results and suggesting a number of possible collaborations. For instance, recent work by Millen [47, 48] is closely related to our current work on exponentiation, XOR encryption, and algebraic properties, and we have begun a fruitful exchange of ideas and results.

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

2.7 Planned work for the next reporting period

The next reporting period (01.01.2005 — 30.06.2005) will be devoted to strengthening the repertoire of techniques for the automatic analysis of security protocols, to assess the technical achievements, and to disseminate the results of the project. In accordance with the Technical Annex we plan to address the following technical issues:

- Further improvements to the back-ends (WP4 – Deliverable 4.6 “AVISPA tool v.3”)
- Identify classes of security protocols for which our automatic analysis procedures are complete (WP5 – Deliverable 5.3 “Completeness Issue”)
- Exploit the compositional structure of protocols (WP4 – Deliverable 4.1 “Compositionality”)
- Assess the achievement of the project (WP7 – Deliverable 7.4 “Assessment of the AVISPA tool v.3”)
- Disseminate the results of the project (WP8 – Deliverable 8.6 “Year 3 Project Workshop” and Deliverable 8.7 “Technology Implementation Plan”)

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 62nd IETF Meeting that will be held in Minneapolis on March 6-11, 2005.
- 3rd Year Project Workshop. The second edition of the workshop “Automated Reasoning for Security Protocols Analysis” (ARSPA’05) will be held in Lisbon, on July 16th, 2005, in the context of the 32nd International Colloquium on Automata, Languages and Programming (ICALP 2005) (`http://www.avispa-project.org/arspa/`), and will be chaired by Luca Viganò (ETHZ) and Prof. Pierpaolo Degano of the University of Pisa (Italy). 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), Sebastian Mödersheim and Luca Viganò (ETHZ) will hold the one-day tutorial on Automated Validation of Security Protocols AVASP’05 in the context of the 8th European Joint Conference on Theory and Practice of Software (ETAPS 2005), Edinburgh, Scotland, April 3rd, 2005.

2.8 Assessment of project results and achievements

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

Specification Languages. We have a formally defined high-level protocol specification language HLPSL and a lower-level IF specification language. Both languages have been extended to support fully typed specifications (by adding compound types) and algebraic properties (exclusive-or and exponential). In addition, all the verification tools have a common output format, defined for clearly explaining under what conditions each tool is run. All this makes the AVISPA Tool the most user-friendly, but also expressive and powerful tool for specifying protocols.

Problems Specification. We have specified in HLPSL 33 protocols from 14 groups drawn from the list given in [34] thereby obtaining a total 112 security problems.

The AVISPA Tool v.2. We have devoted considerable effort to develop version 2 of the AVISPA Tool. In particular we have carried out the following extensions:

- The HLPSL2IF translator has been updated so to reflect the extensions to the HLPSL and the IF.
- A graphical user interface has been added.
- XEmacs mode files have been produced to assist the editing of HLPSL specifications.
- OFMC has been strengthened by improving the previously implemented symbolic techniques and heuristics and introducing new ones, in order to search more efficiently for attacks in both typed and untyped models. Moreover, OFMC also provides preliminary support for algebraic properties and guessing.
- CL-AtSe 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. It can look for attacks either in a typed model, or in an untyped one.
- SATMC, the SAT-based model-checker developed and maintained by UNIGE, has been improved with new, more encoding techniques that make the system considerably faster.
- TA4SP, a new back-end based on tree automata techniques has been integrated into the AVISPA Tool.

Assessment of the AVISPA Tool v.2. By feeding the 112 security problems formalised in HLPSL to the AVISPA Too v.2, 110 problems are successfully analysed in less than 25 minutes of CPU time per problem (globally, the entire library of 110 problems requires 69 minutes of CPU time to be analysed). All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the AVISPA Tool v.2. Moreover, the tool is able to detect the same new (i.e. previously unknown in literature) attacks discovered by the AVISPA Tool v.1 and with better performance.

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

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

We have continued the dialogue between AVISPA and the Internet Engineering Task Force (IETF), by officially presenting and discussing our list of candidate security protocols and problems with their security experts (including the security area directors) at the "Open Security Area Directorate Meeting" during the 59th IETF meeting in Seoul, South Korea, February 29-March 4, 2004. The slides of the presentation are available online in the proceedings of the IETF, at `http://www.ietf.org/proceedings/04mar/slides/saag-1/index.html` and `http://www.ietf.org/proceedings/04mar/slides/saag-1/saag-1.ppt`. The presentation was very welcome and the goals of the AVISPA project were seen to be very high and valuable.

3 Project Management and Coordination

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

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

- **2nd AVISPA Synchronisation Meeting**, 29–30.03.2004, DIST, University of Genova. This meeting was devoted to synchronising the activities among the partners. A proposal for the translating HLPSL v.1 into HLPSL v.2 was proposed and approved. Moreover, special sessions were devoted to discuss open technical issues about the upcoming deliverables, namely D2.2 “Algebraic Properties”, D3.2 “Assumptions on Environment”, D4.5 “AVISPA Tool v.2”, and D5.2 “Infinite state Model-Checking”, and D8.5 “Year 2 Project Workshop”.

- **AVISPA meeting**, 07.07.2004, University College of Cork, Ireland. Given that a significant number of AVISPA personnel was attending IJCAR’04, we found it convenient to have a brief meeting aimed at checking the progress of the project and the production of the deliverables due by month 20.

- **3rd AVISPA Synchronisation Meeting**, 21–23.09.2004, DIST, University of Genova. This meeting was devoted to synchronising the activities among the partners. Special sessions were devoted to discuss open technical issues about the upcoming deliverables, namely D7.3 “Assessment of AVISPA Tool v.2”, D6.2 “Specification of problems in HLPSL”, D2.4 “Interface”, and D3.1 “Security Properties”.

- **AVISPA Meeting**, 15-17.12.2004, Siemens, München, Germany. This meeting was devoted to check the activities carried out by the partners related to the upcoming deliverables, namely D7.3 “Assessment of AVISPA Tool v.2”, D6.2 “Specification of problems in HLPSL”, D2.4 “Interface”, D3.1 “Security Properties”, and D1.2 “Year 2 Progress Report”.

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

- The *translator task-force* has been given the task of updating the syntax and semantics of the specification languages HLPSL and IF, as well as to adapt and improve the translator HLPSL2IF.

- The *modelling task-force* has been given the task of formalising the selected security problems. Both task-forces have been regularly reporting their achievements in special sessions during the project meetings.

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

- avispa-general@avispa-project.org is devoted to general announcements such as advertising a project meeting or a new project publication. This mailing list comprises all the people involved in the project both at the technical level and at the management and administrative level. More than 900 messages have been exchanges on this mailing list since the beginning of the project.

- avispa-tech@avispa-project.org is devoted to the exchange of technical information between the partners. This mailing list comprises all the scientists from the partner groups. More than 3,200 messages have been exchanges on this mailing list since the beginning of the project.

- 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. More than 300 messages have been exchanges on this mailing list since the beginning of the project.

- avispa-modeling@avispa-project.org is the mailing list used by the modelling task-force. More than 1,000 messages have been exchanges on this mailing list since the beginning of the project.

- avispa-compiler@avispa-project.org is the mailing list used by the translator task-force. More than 60 messages have been exchanges on this mailing list since the beginning of the project.

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

- the *Internal Section* (www.avispa-project.org/internal) is used to enable the sharing of reserved documents among the partners;

- the *EC Section* (www.avispa-project.org/internal/EU) contains the deliverables in electronic form as well as the up-to-date list of deliverables.

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

4 Cost Breakdown

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

Table 4. Costs in euro for the reporting period: 01.01.2004 --- 31.12.2004

	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	135.007	150.839	364.463	257.823	90.663	105.838	213.428	173.112	133.426	126.541	333.565	7.420	106.417	159.360	264.568	278.522
2. Durable Equipment	6.506	7.749	16.264	14.853	-	-	-	-	-	-	-	-	-	-	-	-
3. Subcontracting	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4. Travel and subsistence	8.000	4.099	21.994	14.668	10.000	6.545	26.000	17.030	8.500	7.295	20.000	4.259	-	-	-	-
5. Consumables	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6. Computing	100	50	300	145	-	-	-	-	-	-	-	-	-	-	-	-
7. Protection of Knowledge	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8. Other specific costs	1.000	-	11.000	150	1.000	5.263	11.489	6.493	1.000	-	2.750	-	-	-	8.000	-
Subtotal	**150.613**	**162.738**	**414.021**	**287.640**	**101.663**	**117.646**	**250.917**	**196.634**	**142.926**	**133.836**	**356.315**	**11.679**	**106.417**	**159.360**	**272.568**	**278.522**
Indirect Costs																
9. Overheads	63.386	69.524	175.702	121.476	140.644	132.485	323.621	225.366	7.146	-	17.815	-	95.178	111.607	236.626	195.203
Total	**213.999**	**232.262**	**589.723**	**409.116**	**242.307**	**250.131**	**574.538**	**422.000**	**150.072**	**133.836**	**374.130**	**11.679**	**201.595**	**270.967**	**509.194**	**473.725**

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 presented 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 62nd IETF Meeting on March 6-11, 2005.

Talks. All of the 15 articles that have been published in international conferences (cf. Section 7) have been presented at the respective meetings. Additionally, we have organised and/or given talks in the following scientific events. These talks aimed at introducing the high-level project objectives, the protocols and problems that the project is analysing, and the techniques and results achieved:

- Talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Faculty of Mathematics of the University of Bologna, Italy, October 25th, 2004.
- Talk on the OFMC back-end and the AVISPA Project by L. Viganò (ETHZ) at the Dagstuhl Seminar "SPP". Dagstuhl, Germany, November 5th – 10th, 2004.
- 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 attendees: about 300).
- Talks on the AVISPA Project by A. Armando (UNIGE) and on SATMC by L. Compagna (UNIGE) at the Istituto per la Ricerca Scientifica e Tecnologica (ITC-IRST), Trento, Italy.
- Talk on the TA4SP back-end and HLPSL by Y. Boichut (INRIA) at the Institut de Recherche en Informatique et Système Aléatoire (IRISA), Rennes, France, December 9th, 2004.

Project Workshops and Tutorials.

- The First Project Workshop, Nancy, January 23, 2004. (`http://qsl.loria.fr/Externe/Evennements/JourneeQSL/Journee23-01-2004/programme.htm`) All members of the AVISPA project attended the workshop. Dr. Peter Ryan (University of Newcastle, U.K.) and Dr. Yassine Lakhnech (Verimag, Grenoble, France) acted as invited speakers and took a very active role in the meeting.

- The Second Project Workshop: Workshop on Automated Reasoning for Security Protocols Analysis (ARSPA'04) co-located with the Second International Joint Conference on Automated Reasoning (IJCAR'04) in Cork (Ireland), July 4, 2004. (Number of attendees: about 50).

- The Third Project Workshop will take place on July 16th, 2005 (i.e. just after the end of the project), in the context of the 32nd International Colloquium on Automata, Languages and Programming (ICALP 2005).

- Full day tutorial on Automated Validation of Security Protocols (AVASP'04) held on July 5, 2004 at the University College Cork, Ireland in the context of the Second International Joint Conference on Automated Reasoning (IJCAR'04). (Tutorial Web-Site: `http://www.avispa-project.org/avasp`)

- Full day tutorial on Automated Validation of Security Protocols (AVASP'05), in the context of the 8th European Joint Conference on Theory and Practice of Software (ETAPS 2005), Edinburgh, Scotland, April 3rd, 2005.

Editing.

- Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04). Electronic Notes in Computer Science, Elsevier Science, in print. Alessandro Armando and Luca Viganò, editors. Preprint available at `www.avispa-project.org/arspa` and `www.avispa-project.org`.

- Special Issue of the Journal of Automated Reasoning on "Automated Reasoning for Security Protocol Analysis". A large number of papers (21) has been submitted. The review process is in progress.

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 e

`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.

- A “Software” section from which the HLSPL2IF translator and the back-ends can be downloaded and the AVISPA Tool can be accessed via a web-based graphical user interface.
- Three sections especially dedicated to (1) internal communication among AVISPA partners, (2) communication with the European Commission, (3) communication with the IETF.
- A number of relevant links: other projects, institutions and companies that are related to AVISPA.

6 AVISPA Deliverables

[1] AVISPA. Deliverable 1.2: Periodic Progress Report N°: 2. Available at http://www.avispa-project.org, 2005.

[2] AVISPA. Deliverable 2.2: Algebraic Properties. Available at http://www.avispa-project.org, 2004.

[3] AVISPA. Deliverable 2.4: Interface. Available at http://www.avispa-project.org, 2005.

[4] AVISPA. Deliverable 3.1: Security Properties. Available at http://www.avispa-project.org, 2005.

[5] AVISPA. Deliverable 3.2: Assumptions on Environment. Available at http://www.avispa-project.org, 2004.

[6] AVISPA. Deliverable 4.5: AVISPA Tool v.2. Available at http://www.avispa-project.org, 2005.

[7] AVISPA. Deliverable 5.2: Infinite-state model-checking. Available at http://www.avispa-project.org, 2004.

[8] AVISPA. Deliverable 6.2: Specification of the Problems in the HLPSL. Available at http://www.avispa-project.org, 2005.

[9] AVISPA. Deliverable 7.3: Assessment of the AVISPA Tool v.2. Available at http://www.avispa-project.org, 2005.

[10] AVISPA. Deliverable 8.4: Year 1 Project Workshop. Available at http://www.avispa-project.org, 2004.

[11] AVISPA. Deliverable 8.5: Year 2 Project Workshop. Available at http://www.avispa-project.org, 2004.

7 AVISPA Publications

[12] A. Armando and L. Compagna. An optimized intruder model for sat-based model-checking of security protocols. In *Proceedings of the IJCAR04 Workshop ARSPA*, 2004. To appear in ENTCS, available at `http://www.avispa-project.org`.

[13] A. Armando and L. Compagna. SATMC: a SAT-based model checker for security protocols. In *Proceedings of the 9th European Conference on Logics in Artificial Intelligence (JELIA'04)*, volume 3229 of *LNAI*, pages 730–733, Lisbon, Portugal, 2004. Springer-Verlag.

[14] A. Armando, L. Compagna, and Y. Lierler. Automatic compilation of protocol insecurity problems into logic programming. In *Proceedings of the 9th European Conference on Logics in Artificial Intelligence (JELIA'04)*, volume 3229 of *LNAI*, pages 617–627, Lisbon, Portugal, 2004. Springer-Verlag.

[15] A. Armando and L. Viganò, editors. *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04).* Electronic Notes in Computer Science. Elsevier Science, Amsterdam, The Netherlands, to appear.

[16] D. Basin, S. Mödersheim, and L. Viganò. OFMC: A Symbolic Model-Checker for Security Protocols. *International Journal of Information Security*, 2004.

[17] Y. Boichut, P.-C. Heam, O. Kouchnarenko, and F. Oehl. Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In *Proc. Int. Workshop on Automated Verification of Infinite-State Systems (AVIS'2004), joint to ETAPS'04*, pages 1–11, Barcelona, Spain, 2004. The final version will be published in EN in Theoretical Computer Science, Elsevier.

[18] Y. Boichut, P.-C. Heam, O. Kouchnarenko, and F. Oehl. Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In *Proceedings of Automated Verification of Infinite States Systems (AVIS'04)*, ENTCS, 2004. To appear.

[19] C. Caleiro, L. Viganò, and D. Basin. Towards a metalogic for security protocol analysis. In W. A. Carnielli, F. M. Dionísio, and P. Mateus, editors, *Proceedings of the Workshop on the Combination of Logics: Theory and Applications (Comblog'04)*, pages 187–196. Center for Logic and Computation, Departamento de Matemática, Instituto Superior Técnico, Lisbon, Portugal, 2004.

[20] C. Caleiro, L. Viganò, and D. Basin. Metareasoning about Security Protocols using Distributed Temporal Logic. In *Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04)*, Electronic Notes in Computer Science. Elsevier Science, Amsterdam, The Netherlands, to appear.

[21] Y. Chevalier. A simple constraint combination procedure for cryptographic protocols with xor. In M. Kohlhase, editor, *18th Int. Workshop on Unification*, Cork, Ireland, July 2004. Long version available as INRIA Research Report RR-5224.

[22] Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drieslma, J. Mantovani, S. Mödersheim, and L. Vigneron. *A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols*, volume 180 of *Automated Software Engineering*, pages 193–205. Austrian Computer Society, Austria, September 2004.

[23] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the Security of Protocols with Commuting Public Key Encryption. In *Workshop on Automated Reasoning for Security Protocol Analysis - ARSPA'2004*, Electronic Notes in Theoretical Computer Science - ENTCS, Cork, Ireland, Jul 2004.

[24] Y. Chevalier and L. Vigneron. Rule-based Programs describing Internet Security Protocols. In S. Abdennadher and C. Ringeissen, editors, *5th Int. Workshop on Rule-Based Programming (RULE)*, Aachen, Germany, June 2004.

[25] Y. Chevalier and L. Vigneron. Strategy for Verifying Security Protocols with Unbounded Message Size. *Journal of Automated Software Engineering*, 11(2):141–166, April 2004.

[26] G. Delzanno and P. Ganty. Automatic verification of time sensitive cryptographic protocols. In K. Jensen and A. Podelski, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 10th International Conference, TACAS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings*, volume 2988 of *Lecture Notes in Computer Science*, pages 342–356. Springer, 2004.

[27] P. Hankes Drielsma and S. Mödersheim. The asw protocol revisited: A unified view. In *Proceedings of the IJCAR04 Workshop ARSPA*, 2004. To appear in ENTCS, available at `http://www.avispa-project.org`.

[28] M. Rusinowitch. A decidable analysis of security protocols. In J.-J. Lévy, E. Mayr, and J. Mitchell, editors, *18th IFIP World Computer Congress on Theoretical Computer Science - TCS'2004*, Toulouse, France, August 2004. Kluwer Academic Publishers.

[29] L. Vigneron. Automatic verification of security protocols. In M. Kohlhase, editor, *18th Int. Workshop on Unification*, Cork, Ireland, July 2004. Invited talk.

8 References

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

[31] AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language. Available at `http://www.avispa-project.org`, 2003.

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

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

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

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

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

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

[38] 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.

[39] 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.

[40] 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.

[41] H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. Symp. on Logic in Computer Science (LICS'03), IEEE Computer Society Press*, 2003.

[42] R. Corin, J. Doumen, and S. Etalle. Analysing password protocol security against off-line dictionary attacks. In *Proceedings of 2nd International Workshop on Security Issues with Petri Nets and other Computational Models (WISP)*. Electronic Notes in Theoretical Computer Science, 2004.

[43] S. Delaune and F. Jacquemard. A theory of guessing attacks and its complexity. Research Report LSV-04-1, Lab. Specification and Verification, ENS de Cachan, Cachan, France, Jan. 2004.

[44] 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/`.

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

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

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

[48] 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.

[49] M. Rusinowitch and M. Turuani. Protocol Insecurity with Finite Number of Sessions is NP-complete. In *Proceedings of CSFW'01*. IEEE Computer Society Press, 2001. Available at `http://www.avispa-project.org`.

[50] V. Shmatikov. Decidable analysis of cryptographic protocols with products and modular exponentiation. In *Proceedings of the 13th European Symposium on Programming (ESOP '04)*, LNCS 2986. Springer-Verlag, 2004.