AVISPA

IST–2001–39252

Automated Validation of
Internet Security Protocols and Applications

Dissemination and Use Plan

Deliverable 8.3
(see also Consortium Agreement)

Abstract

This is the Dissemination and Use Plan of AVISPA. It outlines the actions that will be taken to disseminate and use the knowledge obtained from the project.

Deliverable details

Report version: **1.01 (final)**

Date of delivery: **June 30th, 2003** Due on: **June 30th, 2003**

Classification: **public** Total pages: **12**

Person-months required: **0.5**

Project details

Contract Start Date: **Jan 1st, 2003** Duration: **30 months**

Project Co-ordinator: **Alessandro ARMANDO**

Partners: **University of Genova, ETH Zurich, INRIA Nancy, Siemens AG**

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

Automated Validation of
Internet Security Protocols and Applications

IST–2001–39252
Shared-cost FET Open Project

www.avispa-project.org

Dissemination and Use Plan

Deliverable 8.3

Abstract

This is the Dissemination and Use Plan of AVISPA. It outlines the actions that will be taken to disseminate and use the knowledge obtained from the project.

1. Introduction

AVISPA is a shared-cost RTD (FET open) project, funded by the European Commission under the Information Society Technologies Programme operating within the Fifth Framework Programme. This document is the Dissemination and Use Plan for AVISPA, and is structured as follows:

- in Section 2, *Overview and General Approach* we give an overview of the expected results, along with our approach to dissemination and use and some market projections;
- in Section 3, *Description of the Dissemination Plan* we describe the conferences and publications by means of which we will disseminate our results, the web-site we have set up, and the clustering and standardisation relevant to AVISPA;
- in Section 4, *Description of the Use Plan (by result)* we describe the use plans for each expected result.

2. Overview and General Approach

2.1. Overview of expected results

The AVISPA project aims at developing formal techniques and tools for the analysis of large-scale security-sensitive protocols as defined by standardisation organisations such as the Internet Engineering Task Force (IETF), the International Telecommunication Union (ITU), and the World Wide Web Consortium (W3C). These techniques and tool will be incorporated in the *AVISPA Protocol Analysis Tool.*

The main expected results are the following:

1. *Protocol Specification Languages.* We will develop two specification languages for formalising protocols, security goals, and threat models of industrial complexity. The *High-Level Protocol Specification Language* (*HLPSL*) will allow users to specify protocols at an adequate level of abstraction. The *Intermediate Format* (*IF*) will support the specification of protocols at a level of detail amenable to formal analysis. Both the syntax and the semantics of the two languages as well as a translation between the two will be rigorously defined.
2. *Techniques for the Automatic Analysis of Security Protocols.* A set of techniques for security protocol analysis based on Automated Deduction (namely *On-the-fly Model-Checking*, *Constraint-Based Theorem Proving* and *SAT-Based Model-Checking*) will be improved and extended in order to make them scale up to the validation of industrial-strength security protocols and applications.
3. *The AVISPA Tool.* The above results will be implemented into a software platform, called *AVISPA Protocol Analysis Tool*, which will support the automated validation of industrial-strength security protocols. The tool will automatically translate HLPSL specifications into IF and then feed them to one or more back-ends.

4. *The AVISPA Protocol Library.* A large number of practically relevant, industrial-strength security protocols and related problems will be collected into a library that will be publicly available to the scientific and the industrial communities. We will use this library to measure the adequacy of our specification languages as well as the effectiveness of our analysis techniques.

Table 1: overview of the results (D=dissemination, U=use)			
Result	*Type*	*D/U*	*Due at month(s)*
High-Level Protocol Specification Language (HLPSL)	Technical report	U	8
Intermediate Format (IF)	Technical report	U	8
On-the-fly Model-Checking	Software	U	11,19,27
Constraint-Based Theorem Prover	Software	U	11,19,27
SAT-Based Model-Checker	Software	U	11,19,27
AVISPA Protocol Library	Electronic repository	D&U	10,24
AVISPA Tool	Software	D&U	11,19,27

2.2. Approach to Dissemination and Use

Appropriate measures are planned to ensure an effective and timely dissemination of the project results to potential users, both at the European level and worldwide. The main targets of the dissemination activity will be industry, research institutions, and standardisation bodies working on the design of security-sensitive Internet protocols and applications. Moreover, since the European Society as a whole will ultimately benefit from the results of the project (in terms of increased reliability of and confidence in the Electronic Market), special measures are planned to reach the public.

Dissemination to industry, research institutions, and standardisation bodies will be carried out by a variety of means:

- Talks at relevant international conferences and forums (both presenting the technical achievements and introducing at a high level the project's objectives and results).
- Publication of papers in proceedings of international conferences as well as in international scientific journals.
- Organisation of workshops on project-related topics, including "project workshops" where attendance of external experts and professionals is based on invitation.
- Organisation of tutorials and thematic schools.
- Design and management of a publicly available web-site that includes descriptions of the main project results and, in particular, the AVISPA Protocol Library.

Press releases will be used to reach and make the Public aware of both the short-term and long-term impact of the project results.

The new techniques and methodologies as well as the prototype tool for the automated protocol analysis developed by the project will be made available to research-

ers and professionals working on the design of new security-sensitive Internet protocols and applications. The AVISPA consortium will make techniques and tools freely available in order to encourage people to perform quality assurance through protocol analysis and to use AVISPA results. We don't believe in a commercial market for security protocol analysis tools, for reasons of potential market volume and appropriate pricing. On the other hand, making results available for free highly increases the chance of AVISPA being accepted as a *de facto* standard methodology and toolset within standardisation bodies, thus opening a market for consulting and services relating to protocol analysis.

The new technology developed in the project will thus contribute to the standardisation and industrial consensus of new protocols, thereby improving the reliability and efficiency of protocols and networks, and hence will reduce their costs. We expect a particularly fruitful dialog between AVISPA and the Internet Engineering Task Force (IETF) and particular measures are planned to facilitate this collaboration. We are currently discussing with the area directors of the IETF, and we plan to present the initial results and tool in a future plenary session of the IETF.

2.3. Market Projections

In the current Internet world, the equipment and the software of all different vendors has to be interoperable. While operating systems on clients or servers and databases may be proprietary, the protocols used to communicate between the different systems have to be agreed upon by the industrial community as a whole. Most of those protocols are defined in one standardisation body. This is precisely the main market for the AVISPA tools: the security relevant protocols that are to be standardised by the industrial community and the standardisation bodies. The importance of those protocols is prominent and the potential impact of any security problems is impossible to overestimate. If the industry had to replace hundreds of millions of cellular phones or hundreds of thousands of equipment in communication towers because of an error in the firmware, this could have an enormous negative economical impact. On the other hand, the confidence in the security of the protocols and applications that provide the basis of today's e-commerce applications will significantly contribute to the economic development of the communications technology and business sector.

Individual companies or closed consortiums may also use the AVISPA Tool to validate proprietary protocols, but this is seen as a secondary market.

The scientific advances made by the AVISPA project in modelling and validating Internet security-sensitive protocols have strong potential commercial and industrial exploitation. They significantly contribute to rigorous quality assurance and establishment of trust in the core protocols of a broad spectrum of application areas in current and future communication technology. The main areas of application are: Mobility Management for laptops, handheld devices and cellular phones, Voice over IP (VoIP), secure provision of Quality of Service (QoS), Location Services, Presence Information, Secure Web Services, M-Commerce, Privacy, Security Infrastructure, Routing and Management Infrastructure, Data Streaming, Group Protocols and Multicast.

The tool resulting from the AVISPA project as well as reports on the protocol analysis performed during the project will be made available to protocol designers and will be presented to the IETF and other standardisation bodies. The tool and accompanying

methodology should help the standardisation organisations develop robust, correctly functioning, secure protocols for the Internet.

3. Description of the Dissemination Plan

3.1. Project Workshops and Conferences

Three official Project Workshops will be organised:

- The *First Project Workshop* will take place in Nancy in early November 2003. All members of the AVISPA project will attend the workshop and we will invite as guests a small group of international researchers and professionals who are working on related problems.
- Genova will be European Capital of Culture in 2004; therefore, the *Second Project Workshop* will take place in Genova in September/October 2004 in the context of a series of events organised by the University of Genova. This workshop will be open to external participants (with contributions selected by peer reviewing) and we aim to have published proceedings. Together with the Project Workshop we will organise a one-day "Dissemination Workshop" with invited speakers representing the main actors in IT security: industry, research, standardisation bodies, government, and funding agencies. The fact that Genova will be European Capital of Culture in 2004, and thus will host a large number of international events and symposiums, will allow for the workshop to have a wide resonance in the scientific and general press.
- The *Third Project Workshop* will take place in June 2005 (i.e. just before the end of the project). In order to maximise the dissemination of the project results we plan to organise this event in the context of a major scientific event such as, e.g., a meeting of the IETF.

Additionally, the members of AVISPA will play an active role in the organisation of a number of scientific events:

- Tutorial on *Automated Reasoning for Security Protocol Verification* at the International Joint Conference on Artificial Intelligence (IJCAI'03).

  http://www.ijcai-03.org/1024/html/programTutorials.html#MP1

- Workshop on *Security Protocols Verification* (SPV'03) to be held in Marseille on September 6, 2003. Michael Rusinowitch (INRIA Nancy) is Program Chair of the workshop.

  http://www.loria.fr/~rusi/spv.html

- *Fall School on Formal Security Engineering* held at ETH Zürich on September 22-26, 2003. Two researchers from the AVISPA team, David Basin (ETHZ) and Volkmar Lotz (Siemens AG) will be teaching at the school. Moreover, a number of junior members (PhD students in particular) of the AVISPA team will attend the school.

  http://www.zisc.ethz.ch/events/fallschool2003.html

- *Tutorial on Automated Validation of Security Protocols* to be held in the context of the 2nd International Joint Conference on Automated Reasoning, Cork (Ireland), July 4-8, 2004.

Moreover, we aim to present our work at international conferences and forums on computer security and on automated deduction, including but not limited to

- meetings of the IETF, ITU, and W3C,
- ESORICS (European Symposium on Research in Computer Security),
- CCS (Computer and Communication Security),
- CSFW (Computer Security Foundations Workshop),
- CAV (Computer-Aided Verification),
- CADE (International Conference on Automated Deduction),
- LICS (IEEE Symposium on Logic in Computer Science),
- IJCAR (International Joint Conference on Automated Reasoning),
- FME (Formal Methods Europe Conference Series),
- FORTE (IFIP TC6 WG 6.1 Joint International Conference on Formal Techniques for Networked and Distributed Systems)

as well as USENIX meetings and meetings organised by the IEEE and the ACM.

3.2. Publications

We aim to publish the results obtained in AVISPA in the proceedings of workshops and conferences (like those mentioned in Section 3.1), and in international journals such as:

- Journal of Computer Security,
- International Journal of Information Security,
- IEEE Security and Privacy,
- ACM Transactions on Information and System Security,
- Information Systems Security,
- Computers and Security,
- Journal of Cryptology,
- Theoretical Computer Science,
- Artificial Intelligence,
- Science of Computer Programming

and journals published by the ACM and the IEEE. Moreover, the AVISPA consortium has already achieved the following publications:

- A. Armando and L. Compagna, **Abstraction-driven SAT-based Analysis of Security Protocols**, Sixth International Conference on Theory and Applications of Satisfiability Testing (SAT 2003), 2003
- A. Armando, L. Compagna and P. Ganty, **SAT-based Model-Checking of Security Protocols using Planning Graph Analysis**, proceedings of the 12th International FME Symposium, 2003

- D. Basin, S. Moedersheim and L. Viganò, **An On-The-Fly Model-Checker for Security Protocol Analysis**, to appear in the proceedings of ESORICS 2003
- Y. Chevalier, R. Kusters, M. Rusinowitch and M. Turuani, **An NP Decision Procedure for Protocol Insecurity with XOR**, 18th IEEE Symposium on Logic in Computer Science (LICS 2003), 2003
- Y. Chevalier, R. Kusters, M. Rusinowitch, M. Turuani and L. Vigneron, **Extending the Dolev-Yao Intruder for Analysing an Unbounded Number of Sessions**, Computer Science Logic (CSL 03) and 8th Kurt Goedel Colloquium (8th KCG), 2003
- G. Delzanno and P. Ganty, **Symbolic Methods for Automatically Proving Secrecy and Authentication in Infinite-state Models of Cryptographic Protocols**, Proceedings of WISP, Workshop on Issues in Security and Petri Nets, 2003
- M. Rusinowitch and M. Turuani, **Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete**, Theoretical Computer Science, 2003

3.3. Web presence and information exchange

The web site of the AVISPA project is

http://www.avispa-project.org

and it 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 taking place in the context of the project: meetings, conferences, workshops, and their availability to the public.
- Publications originated from the project, both in the scientific community and in the general press.
- A number of relevant links: other projects, institutions and companies that are related to AVISPA.
- An internal protected section, containing contact details, internal mailing lists, details about the meetings (slides, notes and so on) and other temporary technical information needed by the consortium.
- A protected section containing the deliverables and other documents for the European Commission.

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

3.4. Clustering and standardisation

This section indicates the list of projects and organisations relevant to the on-going work (at European or national level) and with which information exchange might be beneficial.

EU:

Most relevant projects of the 5th framework (e.g., MAFTIA) are finishing, while the ones for the 6th framework are still not approved and running. We are in close contact with the initiators and members of some proposed projects (PRIME, ENORICS Network of excellence).

Germany:

Within the German Informatics Society (GI), activities on safety and security have recently been merged by founding a new department, called *Fachbereich Sicherheit*. Within this department, there are a number of working groups showing relations to AVISPA topics and with which continuous information exchange is considered to be beneficial. Some of the AVISPA project members are already actively taking part in these working groups:

- FoMSESS (GI WG: Formal Methods and Software Engineering for Safety and Security)

  http://www4.in.tum.de/~fomsess

- Datenschutzfördernde Technik (Privacy Enhancing Technologies) (PET)

  http://www.gi-fb-sicherheit.de/fg/pet.html

- E-Commerce, E-Government und Sicherheit (ECOM)

  http://www.gi-fb-sicherheit.de/fg/ecom.html

- Evaluation, Zertifizierung, Qualitätssicherung, Normung (EZQN)

  http://www.gi-fb-sicherheit.de/fg/ezqn.html

- Mobilität und Sicherheit (m-SEC)

  http://www.gi-fb-sicherheit.de/fg/m-sec.html

- Sicherheit in Netzen (NETSEC)

  http://www.gi-fb-sicherheit.de/fg/netsec.html

- Verlässliche IT-Systeme (VIS)

  http://www.iig.uni-freiburg.de/gi/vis/allgemein.html

Italy:

- Constraint-based Verification of Reactive systems (CoVer)

  http://www.disi.unige.it/person/DelzannoG/cover

France:

- Explication et Vérification Automatique de protocoles cryptographiques (EVA)

  http://www-eva.imag.fr

Relevant standardisation forums are:

- Internet Engineering Task Force (IETF)

http://www.ietf.org

- Open Mobile Alliance

http://www.openmobilealliance.org

- IEEE

http://grouper.ieee.org/groups

- ETSI - European Telecommunications Standards Institute

http://www.etsi.org

- ISO - International Standardisation Organisation

http://www.iso.ch

- ITU - International Telecommunication Union

http://www.itu.int

- W3C - World Wide Web Consortium

http://www.w3.org

- OASIS - Organisation for the Advancement of Structured Information Standards

http://www.oasis-open.org

- 3GPP-The 3rd Generation Partnership Project

http://www.3gpp.org

4. Description of the Use Plan (by result)

In this section, we describe the expected project results that have potential for exploitation, including those beyond the use of AVISPA as a whole as described above.

4.1. The AVISPA Tool

The main result of the project is the AVISPA Tool / set of tools. In a certain sense this result is not independent of the rest: it is impossible to use the tools without the language or the deduction techniques. Thus the AVISPA Tool will provide protocol designers from telecommunication and IT industry with an expressive formal language (with a formal semantics) for expressing their protocols and environments, and with powerful tools to verify them. Moreover, the protocol library will provide them with a good basis for developing new protocols by providing many examples and allowing the reuse of well-tested modules.

On the other hand, the user may be not interested in the techniques themselves or in the syntax and semantics of the language, but just in using our tools to validate their protocols.

The initial set of users of the AVISPA technology will be the security protocol designers of companies and institutes related to the companies and institutes of the pro-

ject participants, in particular Siemens AG. They are expected to benefit from the AVISPA Tool for enhancing trust and confidence in their own protocol proposals and in the protocol specifications that are currently being designed in the international standardisation communities and that will be adopted by the internet, mobile communications, and e-commerce industries. This usage will pave the way to the migration of our technology into industry standardisation organisations such as the IETF so that both the scientific and the industrial communities will be able to benefit from the advances achieved by the project.

4.2. Protocol Specification Languages

In order to facilitate the penetration of formal validation techniques in the protocol industry, we plan to promote our expressive *High-Level Protocol Specification Language (HLPSL)*, which is close to the ones used in text-books and IETF drafts, as a candidate for a standardised notation for protocols. HLPSL will allow for the explicit specification of the actions performed by message senders and receivers, and it will provide facilities for describing environments, security properties and goals, and intruder/threat models.

Such a standard and precise protocol notation will allow for easy validation and reuse of modules by industrial partners. The promotion of HLPSL will be supported by tutorials given at conferences, industrial meetings, thematic schools, and presentations and courses at engineering schools. Two of them are already planned:

1. Full day tutorial, led by Jorge Cuellar (Siemens AG), at the *International Conference on Software Engineering And Formal Methods* (SEFM 2003, Brisbane, Australia, 22nd - 27th September, 2003)

   http://www.svrc.uq.edu.au/Events/SEFM03

2. Invited talk by Jorge Cuellar (Siemens AG) at *Formal Methods Europe* (FME 2003): *Specifying and Verifying real-world Security Protocols*

   http://fme03.isti.cnr.it/iday-progr.htm

On the practical side, the formalisation of the syntax and semantics of the IF will provide a *programmer's manual* to developers who plan to connect their own protocol analysis back-ends (possibly implementing deduction techniques different than ours) with the IF and our analysis tool. We plan to promote the use of the IF at a number of academic and industrial meetings, stressing the two kinds of contributions. That is, we will promote its use both as the interface of the AVISPA Tool and as a tool-independent language providing a formal model for the investigation of different protocol and intruder models.

4.3. Automated Deduction Techniques

On the theoretical side, the foamlisation of the syntax and semantics of IF will allow us to formalise a number of alternative protocol and intruder models (e.g. where cryptography is not perfect or where the intruder has limited capabilities). It will also allow us to formalise a number of automated deduction techniques, in particular symbolic techniques, which will provide the basis of our back-ends.

In particular, we will also formalise optimisations of protocol models in order to speed up search and thus improve the efficiency of the AVISPA Tool, and prove

properties of these optimisations, e.g. prove that no protocol attacks are lost or introduced by a particular optimisation, or show the decidability of some sub-problem.

4.4. The AVISPA Protocol Library

To assess the coverage, effectiveness and performance of the AVISPA Tool, we will collect a set of representative security problems drawn mainly from IETF drafts, as illustrated above, and thoroughly evaluate the AVISPA Tool on these problems according to well-defined and measurable criteria. This set of problems, specified in our proposed language, will be also available to the scientific community.

Thus, one of the goals of the project is to build and make publicly available a library of formalised Internet protocols and associated security problems. The protocols will be selected in such a way to be representative of the many protocol groups currently being developed by the IETF and other standardisation bodies. The library will be proposed to the scientific community as a suite of benchmark problems for automatic protocol analysis that can be readily used to assess the performance of rival approaches. At the end of the project we expect at least 80 problems to be in the database.

For the initial round the following protocols have been selected: SHARE, UMTS-AKA, ISO Public Key Protocols without T3 Party, ChapV2, EKE, SRP, EKE2, SPEKE, ASW, AAA-MIP, IKEv2, Two-Party-Signature, CMS with Symmetric Key-Management, TLS, Kerberos, HIP, Mutual Authentication for low power devices, sucv, BU-IPv6, SSH, Key-Privacy in Public Key, Payment in UMTS, and TESLA.