TECHNOLOGICAL IMPLEMENTATION PLAN

Description of project

EC PROGRAMME:	**IST**
PROJECT TITLE:	Automated Validation of Internet Security Protocols and Applications
ACRONYM:	**AVISPA**
PROGRAMME TYPE:	5th FWP (Fifth Framework Programme)
CONTRACT NUMBER:	IST-2001-39252
PROJECT WEB SITE (if any):	http://www.avispa-project.org/
START DATE:	01 Jan 2003
END DATE:	30 Jun 2005
COORDINATOR DETAILS:	**Name:** Alessandro Armando **Organisation:** DIST, U. of Genova **Address:** Viale Causa 13, 16145 Genova, Italy **Telephone:** +39 010 3532216 **E-mail:** armando@dist.unige.it

PARTNERS NAME:
Eidgenoessische Technische Hochschule Zuerich, Basin David **Siemens Aktiengesellschaft,** Jorge Cuellar **Institut National de Recherche en Informatique et en Automatique,** Michael Rusinowitch

Commission Officer Name:	Fabrizio Sestini

Executive summary

Original research objectives

This project aims to develop a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. This technology will speed the development of the next generation of network protocols, improve their security, and therefore increase the public acceptance of advanced, distributed IT applications based on them. We will achieve this by advancing specification and deduction technology to the point where industry protocols can be specified and automatically analysed. This technology will be integrated into a robust automated tool, tuned on practical, large-scale problems, and migrated to standardization bodies, whose protocol designers are in dire need of such tools. Objectives: This project aims to develop techniques and tools for the analysis of security-sensitive protocols, required to support the next generation of distributed, Internet applications. The main objectives are five fold. First, to develop a rich specification language for formalizing protocols, security goals, and threat models of industrial complexity. Second, to advance the state-of-the-art in automated deduction techniques to scale up to this complexity. Third, to build a tool based on these techniques that will allow industry and standardization organizations to automatically validate or detect errors in their products. Fourth, to tune this tool and demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols. And finally, to begin the migration of this technology into industry standardization organizations such as the IETF so that both the scientific and the industrial community can benefit from the advances achieved by this project. Work description: The work will be carried out by accomplishing the following tasks: - We will design a high-level language for specifying Internet security protocols, and implement a translator from protocol descriptions to a declarative format amenable to formal analysis. The language will support the description of Internet protocol suites, security goals, and assumptions about the environment; - We will develop a technology for automated protocol error detection based on three automated deduction techniques operating on the translator's output. The first technique, on-the-fly model-checking, uses lazy data-types and specialized algorithms that can automatically handle infinite state spaces; it will be backed up by powerful search heuristics. The second technique, theorem-proving with constraints, provides an efficient way of representing an infinite state-space using a constraint store, and supports the specification of built-in theories for cryptographic operators. The third technique employs model-checking methods based on propositional satisfiability checking that efficiently find errors in protocols by reducing an approximation of the problem to a propositional satisfiability problem. Although each technique can work independently, they will be integrated into a single analysis tool, AVISPA, where they will interact and benefit from each other's strengths; - To verify protocols we will develop

techniques for infinite-state verification, like use of abstractions and infinite-state symbolic model-checking, and integrate them in our tool. To avoid combinatorial blow-up in search, for both verification and falsification, we shall exploit the fact that Internet protocols are often built, compositionally from subprotocols and we will develop compositional reasoning techniques; - A set of representative security problems drawn from IETF drafts will be selected and used to thoroughly evaluate the AVISPA tool according to well-defined and measurable criteria.

Expected deliverables

D1.1 Year 1 Progress Report D1.2 Year 2 Progress Report D1.3 Year 3 Progress Report D1.4 Final Project Report D2.1 The High-Level Protocol Specification Language D2.2 Algebraic properties D2.3 The Intermediate Format D2.4 Interface D3.1 Security Properties D3.2 Assumptions on environment D3.3 Sessions instances D4.1 Compositionality D4.2 Partial-Order Reduction D4.3 Heuristics D4.4 AVISPA Tool v.1 D4.5 AVISPA Tool v.2 D4.6 AVISPA Tool v.3 D5.1 Abstractions D5.2 Infinite-state model checking D5.3 Completeness issue D6.1 List of Selected Problems D6.2 Specification of the Problems in the high-level specification language D7.1 Experimental Setup D7.2 Assessment of the AVISPA Tool v.1 D7.3 Assessment of the AVISPA Tool v.2 D7.4 Assessment of the AVISPA Tool v.3 D8.1 AVISPA website D8.2 Project Presentation D8.3 Dissemination and Use Plan D8.4 Year 1 Project Workshop D8.5 Year 2 Project Workshop D8.6 Year 3 Project Workshop D8.7 Technology Implementation Plan

Project's actual outcome

The outcome of the project can be summarised as follows. 1) We have formalised the High-Level Protocol Specification Language HLPSL and the Intermediate Format IF, and have implemented the automated translator HLPSL2IF from HLPSL to IF. Both the HLPSL and the IF are more expressive than other specification languages used for the same purpose. The HLPSL is a very expressive language supporting the specification of security-sensitive protocols with a formal semantics based on an expressive first-order temporal logic. The IF is a tool-independent, low-level protocol specification language that supports the specification of sophisticated typed protocol models and that is suitable for automated deduction. Specifications of security protocols and properties written in HLPSL are automatically translated into IF specifications, which are then given as input to the different back-ends that constitute the AVISPA Tool. We have also devised and implemented a number of advanced techniques and optimisations that allow users of the AVISPA Tool to formally specify complex protocol analysis contexts, environments, and properties. 2) We have devised a number of heuristics, optimisations, and reduction and abstraction techniques, both general and specific to the individual back-ends. Moreover, we have introduced a verification algorithm for time-sensitive security protocols, and we have investigated the completeness of protocol validation procedures and the compositionality of protocols, obtaining a number of results on the composition of intruder theories, of different protocols, and of different communication channels. These protocol analysis techniques are implemented in the 4 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, * SATMC, a SAT-based model-checker developed and maintained by UNIGE, * TA4SP, a tree automata based protocol analyser developed and maintained by the LIFC group affiliated with INRIA. 3) In order to assess the strength of the back-ends of the AVISPA Tool, and to demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols, we have selected a set of candidate protocols currently being drafted by the IETF, along with the security properties these protocols are expected to enjoy. We have thus identified a set of security problems, where a problem is given by both a protocol and a security property the protocol should satisfy. This set, which we call the AVISPA library, contains a total of 384 security problems and 79 protocols, mostly from the IETF, divided into 33 groups.

Broad dissemination and use intentions for the expected outputs

We plan to continue disseminating the results of the project through the standard scientific channels (e.g. scientific publications, presentation at conferences). We will maintain the AVISPA web site, including the public distribution of the AVISPA Tool, the AVISPA Library, and the AVISPA Users mailing list. We also plan to continue our dialogue with the IETF by presenting new releases of the AVISPA Tool at the IETF Meetings as soon as they become available and by giving protocol designers support in the usage of the AVISPA Tool.

Overview of all your main project results

No.	Self-descriptive title of the result	Category A, B or C*	Partner(s) owning the result(s) (referring in particular to specific patents, copyrights, etc.) & involved in their further use
1	Specification languages for large scale security protocols	A	Institut National de Recherche en Informatique et en Automatique Eidgenoessische Technische Hochschule Zuerich Siemens Aktiengesellschaft DIST, U. of Genova
2	SAT-based model checking of security protocols	A	DIST, U. of Genova
3	On-the-fly model checking of security protocols	A	Eidgenoessische Technische Hochschule Zuerich
4	Library of formally specified industrial scale security protocols	A	Eidgenoessische Technische Hochschule Zuerich Siemens Aktiengesellschaft Institut National de Recherche en Informatique et en Automatique DIST, U. of Genova
5	Environment for the automatic validation of security protocols	A	Eidgenoessische Technische Hochschule Zuerich Siemens Aktiengesellschaft Institut National de Recherche en Informatique et en Automatique DIST, U. of Genova
6	Constraint logic based verification of security protocols	A	Institut National de Recherche en Informatique et en Automatique

7	Tree Automata based verification of security protocols	A	Institut National de Recherche en Informatique et en Automatique

*A: results usable outside the consortium / B: results usable within the consortium / C: non usable results

Quantified Data on the dissemination and use of the project results

Items about the dissemination and use of the project results (consolidated numbers)	Currently achieved quantity	Estimated future* quantity
Product innovations	0	0
Process innovations	1	1
New services (commercial)	0	0
New services (public)	1	1
New methods	7	5
Scientific breakthrought	6	5
Technical standards to which this project has contributed	1	10
EU regulations/directives to which this project has contributed	0	0
International regulations to which this project has contributed	0	0
PhDs generated by the project	2	4
Grantees/trainees including transnational exchange of personnel	1	5

** "Future" means expectations within the next 3 years following the end of the project*

Comment on European Interest

Community added value and contribution to EU policies

European dimension of the problem
The problem of improving the security of Internet protocols and applications is perceived as a critical problem not only at the European level but also internationally. As a matter of fact, standardisation organisations, such as the IETF, guiding the standardisation of new protocols are now full-fledged international entities. The development of the AVISPA project, based on multiple advanced technologies, has required a research effort with a truly European dimension: it would have been very difficult to pursue the technical and socio-economical objectives of the project without the participation of different research groups, from both academia and industry.

Contribution to developing S&T co-operation at international level. European added value
The AVISPA project has a relevant and immediate impact on social and economic development in Europe. In particular, the project contributes to the efforts of the European Commission to bring the Information Society closer to the European citizen. The presentation of the project results in international conferences and workshops has ensured their dissemination to the European (and international) research community, and the dissemination of the results to industry and standardisation and regulation bodies (such as the IETF) contributes to improving the competitiveness of European industry. The technology developed in the AVISPA project contributes to the standardisation and industrial consensus of (security-sensitive) Internet protocols and applications, and thereby improves the reliability and efficiency of protocols and networks, and hence reduces their social and marketing costs. It promotes a cheaper, faster and more secure Internet.

Contribution to policy design or implementation
The AVISPA project fits the objectives of the FET OPEN scheme focused on developing new technologies for significant breakthroughs in industrial and societal terms. The project is also closely related to several other action lines, such as that on computing communications and networks, and to the cross-programme on mobile applications and services, and all those actions and policies where security-sensitive applications are developed or exploited, in areas such as health-care, e-commerce, and e-government. Moreover, the project addresses European policy objectives such as those of the eEurope and eEurope+ action plans, namely to promote a cheaper, faster and more secure Internet. The dissemination of the project results to industry and standardisation and regulation bodies such as the IETF contributes to improving the competitiveness of European industry.

Contribution to Community social objectives

Improving the quality of life in the Community:
By promoting the development of a cheaper, faster and more secure Internet the project also contributes to improving the quality of life in the Community.

Provision of appropriate incentives for monitoring and creating jobs in the Community (including use and development of skills):
Not applicable.

Supporting sustainable development, preserving and/or enhancing the environment (including use/conservation of resources):
Not applicable.

Expected project impact (to be filled in by the project coordinator)

EU Policy Goals	I SCALE OF EXPECTED IMPACT OVER THE NEXT 10 YEARS -1 0 1 2 3	II other

		Not applicable to project	Project Impacttoo difficult to estimate
1. Improved sustainable economic development and growth, competitiveness	1		
2. Improved employment	0	√	
3. Improved quality of life and health and safety	1		
4. Improved education	1		
5. Improved preservation and enhancement of the environment	0	√	
6. Improved scientific and technological quality	3		
7. Regulatory and legislative environment	0		√
8. Other	0	√	

1. Economic development and growth, competitiveness	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Increased Turnover for project participants - national markets	1	1
b) Increased Turnover for project participants - international markets	1	1
c) Increased Productivity for project participants	1	1
d) Reduced costs for project participants	1	1
e) Improved output quality/high technology content	1	1

2. Employment	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Safeguarding of jobs		
b) Net employment growth in projects participants staff		
c) Net employment growth in customer and supply chains		
d) Net employment growth in the European economy at large		

3. Quality of Life and health and safety	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved health care	0	0
b) Improved food, nutrition	0	0
c) Improved safety (incl. consumers and workers safety)	1	1
d) Improved quality of life for the elderly and disabled	0	0
e) Improved life expectancy	0	0
f) Improved working conditions	0	0
g) Improved child care	0	0
h) Improved mobility of persons	0	0

4. Improved education	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved learning processes including lifelong learning	0	0

b) Development of new university curricula	1	1

5. Preservation and enhancement of the environment	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Improved prevention of emissions		
b) Improved treatment of emissions		
c) Improved preservation of natural resources and cultural heritage		
d) Reduced energy consumption		

6. S&T quality	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Production of new knowledge	3	3
b) Safeguarding or development of expertise in a research area	3	3
c) Acceleration of RTD, transfer or uptake	3	3
d) Enhance skills of RTD staff	3	3
e) Transfer expertise/know-how/technology	3	3
f) Improved access to knowledge-based networks	2	2
g) Identifying appropriate partners and expertise	0	0
h) Develop international S&T co-operation	1	1
i) Increased gender equality	0	0

7. Regulatory and legislative environment	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3
a) Contribution to EU policy formulation		
Contribution to EU policy implementation		

8. Other (please specify)	Scale of Expected Impacts over the next 10 years (2)	
	By Project End -1 0 1 2 3	After Project End -1 0 1 2 3

Description of Results

No.	Title
1	Specification languages for large scale security protocols

CONTACT PERSON FOR THIS RESULT

Name	Michael Rusinowitch
Position	Directeur de Recherche
Organisation	Institut National de Recherche en Informatique et en Automatique
Address	615 rue du Jardin Botanique BP 105 54602, Villers les Nancy, Cedex FRANCE
Telephone	+33-38-3593020
Fax	+33-3-83278319
E-mail	Michael.Rusinowitch@loria.fr
URL	
Specific Result URL	

SUMMARY

In the AVISPA project, we have designed the High-Level Protocol Specification Language (HLPSL), with the objective to get a language that is both sufficiently high-level to be accessible to engineers and protocol designers of standardisation bodies (themselves not necessarily experts in the area of formal methods) and also expressive enough to specify modern Internet protocols. It has a formal semantics based on Lamport's Temporal Logic of Actions (TLA) that makes it easily translatable into a declarative lower-level term rewriting based language (the Intermediate Format, IF), well-suited to automated analysis tools. HLPSL thus enjoys significant generality, as other tools can easily be made to employ HLPSL by simply adapting them to accept IF specifications as input. HLPSL is modular and allows for the specification of complex control-flow patterns, data-structures, and different intruder models. Using a formal language with a temporal logic semantics to formalise security properties gives us great generality and expressiveness. Finally, HLPSL is not restricted to logicians, but it is particularly suited for engineers and protocols designers. Indeed, HLPSL has been devised as part of the AVISPA project, with the aim to develop push-button, industrial-strength technology supported by expressive specification languages like HLPSL for the analysis of large-scale Internet security-sensitive protocols and applications. In this context, HLPSL is a good candidate for being use with public domain tools based on formal methods in the design phase at the IETF and other standardisation bodies to hopefully accelerate the standardisation of security protocols and improve their correctness. In more detail, the AVISPA tool takes as input a HLPSL specification that is automatically translated into a corresponding IF specification. The IF is a tool-independent, low-level protocol specification language that supports the specification of sophisticated typed protocol models and that is suitable for automated deduction. IF specifications are then analysed by invoking state-of-the-art back-ends (currently CL-AtSe, OFMC, SATMC and TA4SP are supported) which return attacks (if any) to the user in an intuitive and readable output format. The decision to base HLPSL on TLA affords us a "best of both worlds" situation in which we can take advantage of an existing language with a rich semantics while also augmenting it with constructs specific to protocol modelling that make it a convenient language in practice. The HLPSL language has already proven itself to be an effective language for modelling security protocols: many protocols of varying levels of complexity from the simple NSPK example to more complex industrial-scale protocols such as IKE and TLS have already been formalised in HLPSL. Features like modularity, control flow patterns, the specification of alternative intruder models, and the generality of temporal-logic based goals give the protocol specifier great flexibility both to construct faithful models and to experiment with different assumptions about the environment in which the protocol should be executed. In our experience, we have found that HLPSL is powerful yet readable and intuitive to work with. The fact that users from varied backgrounds, including students, have found HLPSL easy to use testifies to the language s accessibility, which was one of our primary design objectives from the outset.

SUBJECT DESCRIPTORS CODES
149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY 321 INFORMATION TECHNOLOGY/SCIENCE 424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Article	Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Moedersheim, 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.	Public

Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. He?, J. Mantovani, S. Mdersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05). Springer-Verlag, 2005.	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE: Tick a box and give the corresponding details(reference numbers, etc) if appropriate**					**Pre-existing know-how Tick a box and give the corresponding details(reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP[1)]**	**NoI[2)]**	**Details**	**Tick**		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	
Other:	

Quantified data about the result

Items (about the results)	**Actual current quantity**	**Estimated (or future) quantity**
Time to application / market (in months from the end of the research project)		
Number of (public or private) entities potentially involved in the implementation of the result:		
of which: number of SMEs:		
of which: number of entities in third countries (outside EU):		
Targeted user audience: of reachable people		
S&T publications (referenced publications only)		
publications addressing general public (e.g. CD-ROMs, WEB sites)		
publications addressing decision takers / public authorities / etc.		
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development		**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	
Other	(please specify)				

Details:

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

No.	Title
2	SAT-based model checking of security protocols

CONTACT PERSON FOR THIS RESULT

Name	Alessandro Armando
Position	Head of Unit
Organisation	DIST, University of Genova
Address	Viale Causa, 13 16145, Genova Italy
Telephone	+39-0103532216
Fax	+39-0103532948
E-mail	armando@dist.unige.it
URL	http://www.ai.dist.unige.it/armando
Specific Result URL	http://www.avispa-project.org

SUMMARY

The SAT-based Model Checker SATMC developed by UNIGE takes as input a specification of a security problem written in in the AVISPA's Intermediate Format (that is, the IF specification of a security protocol and of a security property that the protocol should satisfy, as generated by the HLPSL2IF translator of the AVISPA Tool from a given security problem specification written in the High-Level Protocol Specification Language HLPSL) and performs both protocol falsification and bounded verification in an automatic way by reducing the input problem to a sequence of invocation to a state-of-the-art SAT-solver. The interface between the SATMC and the SAT solver complies with the DIMACS format (the de facto standard for SAT problems) and therefore SATMC can easy incorporate and exploit new SAT solvers as soon as they will become available. Currently SATMC successfully analyses most protocols in the AVISPA Library whose cryptographic operators do not enjoy any specific algebraic property.

SUBJECT DESCRIPTORS CODES
149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY 321 INFORMATION TECHNOLOGY/SCIENCE 424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. He□, J. Mantovani, S. Mdersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05). Springer-Verlag, 2005.	Public
Article	A. Armando and L. Compagna. Abstraction-driven SAT-based Analysis of Security Protocols. In Proceedings of SAT 2003, LNCS 2919. Springer-Verlag, 2003.	Public
Article	A. Armando and L. Compagna. An optimized intruder model for sat-based model-checking of security protocols. Electronic Notes in Theoretical Computer Science (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004), 125(1):91--108, 2005.	Public
Article	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.	Public
Article	A. Armando, L. Compagna, and P. Ganty. SAT-based Model-Checking of Security Protocols using Planning Graph Analysis. In K. Araki, S. Gnesi, and D. Mandrioli, editors, Proceedings of the 12th International Symposium of Formal Methods Europe (FME), LNCS 2805, pages 875--893. Springer-Verlag, 2003.	Public
SATMC Web Page	http://www.ai.dist.unige.it/satmc	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	KNOWLEDGE: Tick a box and give the corresponding details(reference numbers, etc) if appropriate		Pre-existing know-how Tick a box and give the corresponding details(reference numbers, etc) if appropriate	
	Current	Foreseen	Tick	Details

	Tick	NoP[1)]	NoI[2)]	Details	Tick		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Software code
Other:	prototype

Quantified data about the result

Items (about the results)	**Actual current quantity**	**Estimated (or future) quantity**
Time to application / market (in months from the end of the research project)		
Number of (public or private) entities potentially involved in the implementation of the result:		
of which: number of SMEs:		
of which: number of entities in third countries (outside EU):		
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	6	12
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
publications addressing decision takers / public authorities / etc.	1	2
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	√
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership	√	**CONS**	Available for consultancy	√
Other	(please specify)				
Details:					

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can apply our tool SATMC for the validation of protocols developed by the potential partners, and also information exchange/training in the sense that we can offer tutorial on how to apply SATMC and the AVISPA technology in general to validate protocols and applications. We would also gladly consider extenal collaboration on the fututre development of SATMC.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formal methods and automated reasoning for security protocols and applications, and companies/industry/standardisation organisations working on security protocol development or application.

No.	Title
3	On-the-fly model checking of security protocols

CONTACT PERSON FOR THIS RESULT

Name	Basin David
Position	Professor / Head of unit
Organisation	Eidgenoessische Technische Hochschule Zuerich
Address	Raemistrasse 101 8006, Zuerich SWITZERLAND
Telephone	+41 44 6327245
Fax	+41 44 6321172
E-mail	basin@inf.ethz.ch
URL	http://www.infsec.ethz.ch/~basin
Specific Result URL	

SUMMARY

The On-the-fly Model-Checker OFMC developed by the ETHZ partner takes as input a specification of a security problem written in AVISPA's Intermediate Format (that is, the IF specification of a security protocol and of a security property that the protocol should satisfy, as generated by the HLPSL2IF translator of the AVISPA Tool from a given security problem specification written in the High-Level Protocol Specification Language HLPSL) and performs both protocol falsification and bounded verification in an automatic way. Whenever it terminates, OFMC outputs the result of the analysis in AVISPA's Output Format, so that protocol attacks can then also be represented graphically, in the form of message sequence charts or as postscript files. The experimental results that we have carried out during the project demonstrate that OFMC is an extremely effective, state-of-the-art protocol analysis tool both in terms of coverage and performance: we have successfully applied it to all the protocols in the AVISPA library and have been able to re-discover known attacks as well as find new attacks. OFMC's effectiveness is due to a number of technical results. First of all, OFMC performs both protocol falsification and bounded verification by exploring the transition system described by an IF specification of a protocol analysis problem in a demand-driven way, that is, on-the-fly, hence the name of the back-end. Second, OFMC integrates a number of symbolic techniques and optimisations, which are correct and complete, in the sense that no attacks are lost nor new ones are introduced by them. For instance, the "lazy intruder technique", which significantly reduces the search space without excluding any attacks, represents terms symbolically to avoid explicitly enumerating the possible messages the Dolev-Yao intruder can generate. This is achieved by representing intruder messages using terms with variables, and storing and manipulating constraints about what terms must be generated and which terms may be used to generate them. As another significant example, the "constraint differentiation technique" is a search reduction technique that integrates the lazy intruder with ideas from partial-order reduction, and which can be formally proved to terminate and to be correct and complete, thereby reducing OFMC's search time by a factor of two to several orders of magnitude. Third, OFMC also implements a number of efficient search heuristics. It supports the specification of algebraic properties of cryptographic operators, and typed and untyped protocol models. We plan to continue optimising OFMC by introducing further reduction techniques and strategies, as well as heuristics. Moreover, we have also begun investigating abstraction techniques as a means for automatic protocol verification without bounding the scenario as is done in the case of bounded verification: the idea roughly is to compute an overapproximation of the set of reachable states of the system and if this set does not contain any states representing attacks on the protocol, then the original model also does not contain any attacks and the protocol is verified. We have begun initial experiments with abstraction techniques and have promising preliminary results. Moreover, the abstraction techniques are complementary to the techniques employed in our current tool for falsification. We therefore plan to develop extensions of OFMC that employ the best of both falsification and verification techniques, that is, searching for an attack in the original model while, in parallel, searching for an abstraction of the protocol under which it is safe. We will explore too the possible coupling of these routines, and in particular investigate ways in which the tasks can use each other's partial results as heuristics.

SUBJECT DESCRIPTORS CODES
129 COMPUTER SCIENCE/ENGINEERING, NUMERICAL ANALYSIS, SYSTEMS, CONTROL 321 INFORMATION TECHNOLOGY/SCIENCE 424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Article	David Basin, Sebastian Moedersheim, Luca Vigano': An On-The-Fly Model-Checker for Security Protocol Analysis. In E. Snekkenes and D. Gollmann, editors, Proceedings of ESORICS'03, LNCS 2808, pages 253--270. Springer-Verlag, 2003.	Public
Article	David Basin, Sebastian Moedersheim, Luca Vigano': Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols. In V. Atluri and P. Liu, editors, Proceedings of CCS'03, pages 335--344. ACM Press, 2003.	Public

Article	David Basin, Sebastian Moedersheim, Luca Vigano‘: Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols (Extended Abstract). In Proceedings of SPV’03, 2003.	Public
Article	Carlos Caleiro, Luca Vigano‘, David Basin: Towards a Metalogic for Security Protocol Analysis. In W.A. Carnielli, F.M. Dionisio, 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 Matematica, Instituto Superior Tecnico, Lisbon, Portugal, 2004	Public
Article	Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Moedersheim, 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.	Public
Article	Paul Hankes Drielsma and Sebastian Moedersheim: The ASW Protocol Revisited: A Unified View. In Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004), Electronic Notes in Theoretical Computer Science 125(1): 141--156 (Elsevier Science Direct), 2005.	Public
Article	Carlos Caleiro, Luca Vigano‘, David Basin: Metareasoning about Security Protocols using Distributed Temporal Logic. In Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004), Electronic Notes in Theoretical Computer Science 125(1):67-89 (Elsevier Science Direct), 2005.	Public
Journal	Alessandro Armando, Luca Vigano‘: Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004), Electronic Notes in Theoretical Computer Science 125(1) (Elsevier Science Direct), 2005	Public
Journal	Pierpaolo Degano, Luca Vigano‘: Proceedings of the Second Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2005), Electronic Notes in Theoretical Computer Science 135(1) (Elsevier Science Direct), 2005.	Public
Article	Carlos Caleiro, Luca Vigano‘, David Basin: Deconstructing Alice and Bob. In Electronic Notes in Theoretical Computer Science 135(1):3--22 (Proceedings of the Second Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005), 205	Public
Article	Carlos Caleiro, Luca Vigano‘, David Basin: Relating Strand Spaces and Distributed Temporal Logic for Security Protocol Analysis. Logic Journal of the IGPL, to appear.	Public
Article	David Basin, Sebastian Moedersheim, Luca Vigano‘: OFMC: A symbolic model checker for security protocols. International Journal of Information Security 4(3):181-208, 2005.	Public
Article	Paul Hankes Drielsma, Sebastian Moedersheim, Luca Vigano‘: A Formalization of Off-Line Guessing for Security Protocol Analysis. In Franz Baader and Andrei Voronkov, editors, Proceedings of LPAR’04, LNAI 3452, pages 363-379, Springer, 2005.	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE:** **Tick a box and give the corresponding details(reference numbers, etc) if appropriate**					**Pre-existing know-how** **Tick a box and give the corresponding details(reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP[1)]**	**NoI[2)]**	**Details**	**Tick**		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Scientific and/or Technical knowledge (Basic research)
Other:	Prototype/demonstrator available for testing

Quantified data about the result

Items (about the results)	Actual current quantity	Estimated (or future) quantity
Time to application / market (in months from the end of the research project)	0	0
Number of (public or private) entities potentially involved in the implementation of the result:	20	60
of which: number of SMEs:	3	10
of which: number of entities in third countries (outside EU):	7	20
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	12	20
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
publications addressing decision takers / public authorities / etc.		
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	√
Other	(please specify)				
Details:	We plan to both further develop OFMC and also to apply it to a large number of industrial case studies provided by the project partners but also by potential future partners.				

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can apply our tool OFMC for the validation of protocols developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to apply OFMC and the AVISPA technology in general to validate protocols and applications. We would also gladly consider external collaboration on the future development of OFMC.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formal methods and automated reasoning for security protocols and applications, and companies/industry/standardisation organisations working on protocol development or application.

No.	Title
4	Library of formally specified industrial scale security protocols

CONTACT PERSON FOR THIS RESULT

Name	David von Oheimb
Position	Senior Researcher
Organisation	Siemens Corporate Technology
Address	Otto-Hahn-Ring 6 81739, Munich Germany
Telephone	+49 89 636-41173
Fax	+49 89 636-48000
E-mail	David.von.Oheimb@siemens.com
URL	http://w4.siemens.de/ct/
Specific Result URL	http://www.avispa-project.org/

SUMMARY

The AVISPA Selection is a broad collection of 79 practically-important Internet protocols and 384 security properties related to them. The AVISPA Library is a large subset of these, namely 66 protocols (including variants) and their properties that have been modelled in the HLPSL and checked with the AVISPA Tool. The AVISPA Selectoin identifies, categorises, and briefly describes a large number of protocols as well as their required properties. It has undergone a thorough coverage and relevance assessment: the protocols have been selected in such a way to be representative of the many protocol groups currently being developed by the IETF and other standardisation bodies. The AVISPA Library comprises a significant part of the AVISPA Selection, formalising in HLPSL the original, more or less informal, protocol specifications, typically given in the form of one or more IETF RFCs or drafts. The formalisations have been carefully reviewed and cross-checked to make sure that they faithfully describe the important aspects within the expressiveness of HLPSL, while keeping them easy to read and model checking feasible. The AVISPA Selection and Library are publicly available and can serve the scientific community as a suite of benchmark problems for protocol formalisation and analysis that can be readily used to assess the coverage, effectiveness, correctness and performance of rival approaches. Note that, in contrast to the AVISPA Tool, no other state-of-the-art approach is able to deal with these protocols.

SUBJECT DESCRIPTORS CODES
149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY 321 INFORMATION TECHNOLOGY/SCIENCE 424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Deliverable	AVISPA. Deliverable 6.1: List of selected problems. Available at http://www.avispa-project.org/, 2003	Public
Deliverable	AVISPA. Deliverable 6.2: Specification of the Problems in the High Level Protocol Specification Language. Available at http://www.avispa-project.org/, 2004	Public
Online Publication	AVISPA. The AVISPA Libaray. http://www.avispa-project.org/, 2005	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	KNOWLEDGE: Tick a box and give the corresponding details(reference numbers, etc) if appropriate					Pre-existing know-how Tick a box and give the corresponding details(reference numbers, etc) if appropriate	
	Current				Foreseen	Tick	Details
	Tick	NoP[1)]	NoI[2)]	Details	Tick		
Patent applied for	√	1	1	'Method for securing data traffic in a mobile network environment',International Application Number PCT/DE03/00017, filed Jan 7, 2003			
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							

Copyrights						
Secret know-how						
Other - please specify:						

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Scientific and/or Technical knowledge (Basic research)
Other:	

Quantified data about the result

Items (about the results)	**Actual current quantity**	**Estimated (or future) quantity**
Time to application / market (in months from the end of the research project)	0	0
Number of (public or private) entities potentially involved in the implementation of the result:	20	60
of which: number of SMEs:	3	10
of which: number of entities in third countries (outside EU):	7	20
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	12	20
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
publications addressing decision takers / public authorities / etc.	0	0
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement	√	**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	√
Other	(please specify)				
Details:	The AVISPA Library serves as a suite of benchmark problems for protocol formalisation and analysis that can be readily used to assess the coverage, effectiveness, correctness and performance of rival approaches. We intend to extend it in the course of academic follow-up and industrial application projects.				

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can extend our library by modeling and validating protocols developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to apply the AVISPA technology in general to formalise protocols and applications. We would also gladly consider external collaboration on the future development of the AVISPA Library.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formalising and analysing security protocols and applications, and companies/industry/standardisation organisations working on protocol design or application.

No.	Title
5	Environment for the automatic validation of security protocols

CONTACT PERSON FOR THIS RESULT

Name	Alessandro Armando
Position	Head of Unit
Organisation	DIST, U. of Genova
Address	Viale Causa 13 16145, Genova Italy
Telephone	+39 010 3532216
Fax	+39 010 3532948
E-mail	armando@dist.unige.it
URL	http://www.ai.dist.unige.it/armando/
Specific Result URL	http://www.avispa-project.org/

SUMMARY

The AVISPA Tool is a modular environment for the automatic validation of Internet security protocols and applications. The tool can be employed by external users thanks to the web-interface accessible from the project web-site (URL: http://www.avispa-project.org), and it is also downloadable as a single ''package'' to be installed on the users' local machines. The tool takes as input a specification of a security problem written in AVISPA's High-Level Protocol Specification Language HLPSL (that is, it takes as input the specification of a security protocol and of a security property that the protocol should satisfy) and gives in output the results of the analysis by the four different back-ends of the tool. Users can also select to have only one of the back-ends perform the analysis. More specifically, specifications of security protocols and properties written HLPSL are automatically translated (by the translator HLPSL2IF) into Intermediate Format (IF) specifications, which are then given as input to the different back-ends of the AVISPA Tool: OFMC, CL-AtSe, SATMC, and TA4SP. The back-ends implement a variety of analysis techniques, ranging from falsification (that is, searching for protocol attacks), to bounded verification (that is, proving that the input protocol correctly satisfies the input property in a bounded execution scenario specified by the user), and to unbounded verification. In the latter case, abstraction techniques allow the tool to prove whether protocols satisfy secrecy properties in unbounded execution scenarios, but this comes at the cost of preventing the detection of attacks in some protocols. The IF also provides the interface via which other protocol analysis tools can be connected to the AVISPA environment. 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. The results are output in AVISPA's Output Format, so that protocol attacks can then also be represented graphically, in the form of message sequence charts or as postscript files. In order to assess proof-of-concept the strength of the AVISPA tool, we have defined the AVISPA library, a set of formalised security problems (protocols and security properties) drawn from Internet protocols that have recently been standardised or are currently undergoing standardisation by industry and standardisation organisations. The experiments that we have carried out on the library during the project demonstrate that the AVISPA Tool is a state-of-the-art protocol analysis tool in terms of coverage (number of different security problems that can be specified), effectiveness (number of different security problems that can be analysed), and performance (amount of time required for the analysis). The AVISPA Tool has been able to re-discover all known attacks to protocols in the library as well as find a number of new attacks. All the project partners will continue to develop the AVISPA technologies and tools: we plan to strengthen the current environment (that is, extending the specification languages and the back-ends) and apply it to a wider spectrum of problems. In particular, we plan to scale up AVISPA from the validation of protocols to the modular design and validation of composed security services, focussing in particular on the development of a framework for the formal specification of security requirements, the formal analysis of security services, and their composition in an automated and validated way.

SUBJECT DESCRIPTORS CODES
149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY 321 INFORMATION TECHNOLOGY/SCIENCE 424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. He□, J. Mantovani, S. Mdersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05). Springer-Verlag, 2005.	Public
AVISPA Web Site	http://www.avispa-project.org	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	KNOWLEDGE: Tick a box and give the corresponding	Pre-existing know-how Tick a box and give the

	details(reference numbers, etc) if appropriate					corresponding details(reference numbers, etc) if appropriate	
	Current				Foreseen	Tick	Details
	Tick	NoP[1)]	NoI[2)]	Details	Tick		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Scientific and/or Technical knowledge (Basic research)
Other:	Prototype/demonstrator available for testing

Quantified data about the result

Items (about the results)	Actual current quantity	Estimated (or future) quantity
Time to application / market (in months from the end of the research project)	0	0
Number of (public or private) entities potentially involved in the implementation of the result:	20	60
of which: number of SMEs:	3	10
of which: number of entities in third countries (outside EU):	7	20
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	12	20
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
publications addressing decision takers / public authorities / etc.	0	0
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	√
Other	(please specify)				
Details:	We plan to both further develop OFMC and also to apply it to a large number of industrial case studies provided by the project partners but also by potential future partners.				

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can apply our environment for the validation of protocols developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to apply the AVISPA technology in general to validate protocols and applications. We would also gladly consider external collaboration on the future development of AVISPA.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formal methods and automated reasoning for security protocols and applications, and companies/industry/standardisation organisations working on protocol development or application.

No.	Title
6	Constraint logic based verification of security protocols

CONTACT PERSON FOR THIS RESULT

Name	Michael Rusinowitch
Position	Directeur de Recherche
Organisation	Institut National de Recherche en Informatique et en Automatique
Address	615 rue du Jardin Botanique BP 105 54602, Villers les Nancy, Cedex FRANCE
Telephone	+33-38-3593020
Fax	+33-3-83278319
E-mail	Michael.Rusinowitch@loria.fr
URL	
Specific Result URL	

SUMMARY

The CL-AtSe tool (CL-based Model-Checker), developed by the INRIA-CASSIS Partner from Nancy (FRANCE), provides a translation from any security protocol specification written in the AVISPA's Intermediate format (IF), into a set of constraints which can be effectively used to find attacks to protocols. Both translation and checking are fully automatic and internally performed by CL-AtSe, i.e. no external tool is used. In this approach, each protocol step is modeled by a set of minimal constraints on the adversary's knowledge. For example, a message received by an honest participant is a forgeability constraint for the adversary. Moreover, any conditions like equality, inequality, element or non-element of a list are also constraints. The most important advantages of CL-AtSe are the following: - Input Treatment: First, CL-AtSe reads and interprets the AVISPA's Intermediate Format. That is, each role in the IF file is partially pre-executed to extract an exact and relatively minimal list of constraints modeling it. The participant's states and knowledge are eliminated thanks to the use of global variables, which gives us a very simple and rapidly executable protocol specification. Second, CL-AtSe performs various strong simplifications on this extracted protocol specification. This second treatment of the input is responsible for an important part of the CL-AtSe's outstanding speed. In particular, CL-AtSe can eliminate and merge protocol steps together. It can also decompose sent and received messages, and eliminate parts of them when it can be statically decided if the adversary will be able, or will never be able, to use or create them. In the end, all what remain of the former protocol specification is it's very essence. - Protocol execution: Following the idea of the lazy intruder technique developed for AVISS and extended by the AVISPA group, a protocol state (i.e. both the intruder and honest participant's state) is represented by a set of constraints on the (global) protocol variables. These constraints are not solved immediately, but kept in an appropriate data structure on which only satisfiability is checked. Any protocol step is executed by adding new constraints to the system and reducing/eliminating other constraints accordingly in a lazy way. Finally, at each step the system state is tested against the provided set of security properties. Many optimizations have been included here to be as efficient as possible. For example, a great care was taken to avoid collisions between system states and to avoid useless computations. The analysis algorithm used by CL-AtSe is designed for a bounded number of loops, i.e. a bounded number of protocol steps in any trace. With a bounded number of loop iterations, the search for attacks is correct and complete. - Human-readable output: CL-AtSe tries to produce a very nice attack description (when one is found), in an extension of the output format. It can also produce an output strictly compliant with the official AVISPA's format to be used for the generation of a graphical message sequence chart. - Handling of algebraic properties: CL-AtSe can perform the search for attacks modulo some algebraic properties. While this list is expandable in the future, we have currently a partial associativity of concatenation, some xor and exponential properties. Associativity of concatenation is partial in the sense that all solutions of the unification modulo associativity are found, except those that require the generation of new variable. While incomplete, this already gives many interesting results. For example in the project test suite, CL-AtSe outputs many potential security flaws modulo associativity that other tools don't. CL-AtSe can also validate these protocols without associativity. Recently, a set of properties of algebraic operators has been included in CL-AtSe, namely the ACUN properties of the Xor operator, and some properties of the exponential. Natural extensions of this work is to also implement the intruder deduction rules in a modular way, so that adding a new theory to CL-AtSe only requires adding a new small module to the system. - Tool results: The CL-AtSe tool has proved to be extremely efficient on protocol analysis, especially when the associativity of the concatenation is not required. In such cases, CL-AtSe is usually much faster that all other tools of the test suite. Moreover, CL-AtSe is able to perform verification and validation of security protocols modulo various algebraic properties (partial associativity, xor, exponential). Such theories are intended to be completed by new ones in the future. Also, other decision techniques developed by other groups will be adapted for CL-AtSe, in order to improve the protocol simplification phase or to weaken the restriction of a bounded number of sessions.

SUBJECT DESCRIPTORS CODES
424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT 149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY 321 INFORMATION TECHNOLOGY/SCIENCE

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Thesis	M. Turuani. Sécurité des Protocoles Cryptographiques: Décidabilité et Complexité. Thèse de doctorat, Université Henri Poincaré, Nancy, décembre 2003.	Public

Thesis	Y. Chevalier. Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques. Thèse de doctorat, Université Henri Poincaré, Nancy, décembre 2003.	Public
Article	Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents. In Proceedings of the Foundations of Software Technology and Theoretical Computer Science, FSTTCS'03, Lecture Notes in Computer Science. Springer, December 2003. Long version available as Christian-Albrecht Universität IFI-Report 0305, Kiel (Germany).	Public
Article	Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions. In M. Baaz, editor, Computer Science Logic (CSL 03) and 8th Kurt Gödel Colloquium (8th KCG), volume 2803 of Lecture Notes in Computer Science, Vienna, Austria, August 2003. Springer.	Public
Article	Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. In Proceedings of the Logic In Computer Science Conference LICS'03, pages 261-270, June 2003. Long version available as Technical Report RR-4697, INRIA, France.	Public
Journal	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.	Public
Article	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. In Proceedings of Workshop on Specification and Automated Processing of Security Requirements (SAPS), Linz, Austria, September 2004. (13 pages).	Public
Journal	Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. Theoretical Computer Science, 338(1-3):247-274, June 2005.	Public
Article	Y. Chevalier and M. Rusinowitch. Combining Intruder Theories(2005), International Colloquium on Automata, Languages and Programming 11.07. - 15.07, Lisbon, Portugal. Springer LNCS	Public
Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. He□, J. Mantovani, S. Mdersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05). Springer-Verlag, 2005.	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	**KNOWLEDGE: Tick a box and give the corresponding details(reference numbers, etc) if appropriate**					**Pre-existing know-how Tick a box and give the corresponding details(reference numbers, etc) if appropriate**	
	Current				**Foreseen**	**Tick**	**Details**
	Tick	**NoP[1)]**	**NoI[2)]**	**Details**	**Tick**		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Scientific and/or Technical knowledge (Basic research)
Other:	

Quantified data about the result

Items (about the results)	**Actual current quantity**	**Estimated (or future) quantity**
Time to application / market (in months from the end of the research project)	0	0
Number of (public or private) entities potentially involved in the implementation of the result:	20	60
of which: number of SMEs:	3	20
of which: number of entities in third countries (outside EU):	3	20
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	10	20
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	4
publications addressing decision takers / public authorities / etc.	1	4
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	√
Other	(please specify)				
Details:	We plan to both further develop CLATSE and also to apply it to a large number of industrial case studies provided by the project partner but also by potential future partners				

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can apply our tool CLATSE for the validation of protocols developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to apply CLATSE and the AVISPA technology in general to validate protocols and applications. We would also gladly consider external collaboration on the future development of CLATSE.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formal methods and automated reasoning for security protocols and applications, and companies/industry/standardisation organisations working on protocol development or application.

No.	Title
7	Tree Automata based verification of security protocols

CONTACT PERSON FOR THIS RESULT

Name	Michael Rusinowitch
Position	Directeur de Recherche
Organisation	Institut National de Recherche en Informatique et en Automatique
Address	615 rue du Jardin Botanique BP 105 54602, Villers les Nancy, Cedex FRANCE
Telephone	+33-38-3593020
Fax	+33-3-83278319
E-mail	Michael.Rusinowitch@loria.fr
URL	
Specific Result URL	

SUMMARY

The TA4SP (Tree Automata based Automatic Approximations for the Analysis of Security Protocols) tool developed by the INRIA-CASSIS Partner from Besancon (FRANCE) takes as input a specification of a security problem written in AVISPA's Intermediate format (IF) and performs an unbounded verification in an automatic way. The IF transition system representing the protocol is translated into a rewriting system and the IF initial state is transformed to a regular tree language. This tree language is also considered as the intruder knowledge. By applying the term rewriting system (representing the protocol steps and intruder abilities), TA4SP is able to compute an over-approximation of the intruder knowledge by means of abstractions and automatic approximations. For a given problem, a secrecy property holds when all terms related to this property are not in the language representing the over-approximated knowledge of the intruder. The TA4SP tool uses a tree automata library named Timbuk developed by Thomas Genet (IRISA-Rennes, FRANCE). We have been improving Timbuk in order to support our automatic approximations. To speed up the computation, some optimizations such as the use of coarser abstractions, have also been developed. The counterpart of these coarser abstractions is that the results obtained might be more often inconclusive (a secret is in the over-approximated intruder knowledge). However most of our results have been obtained using this optimization. Not only is TA4SP able to guarantee the secrecy of data for a given set of sessions, but under some assumptions it is also possible to extend the result for any set of sessions. Although TA4SP has been recently integrated into the AVISPA tool, some promising results have been obtained. Furthermore, we have also started investigating attacks detection in collaboration with Thomas Genet. Indeed, due to the approximations done, TA4SP is not able to deduce whether a data, claimed as secret, is in the real knowledge of the intruder or not. These investigations will allow us to reveal the presence of an attack in some cases. We plan to augment TA4SP scope by adding new features like sets and conditions.

SUBJECT DESCRIPTORS CODES
424 NETWORK TECHNOLOGY, NETWORK SECURITY 558 SECURITY SYSTEMS 598 SYSTEMS ANALYSIS AND MODELS DEVELOPMENT 321 INFORMATION TECHNOLOGY/SCIENCE 149 DATA PROTECTION, STORAGE TECHNOLOGY, CRYPTOGRAPHY

DOCUMENTATION AND INFORMATION ON THE RESULT

Documentation type	Details (Title, ref. number, general description, language)	Status: PU=Public CO=Confidential
Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, J. Mantovani, S. Moedersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The Avispa Tool for the automated validation of internet security protocols and applications, Tool presentation, in the proceedings of CAV 2005, Computer Aided Verification.	Public
Article	Y. Boichut, P.-C. Heam, O. Kouchnarenko and F. Oehl, Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols, in Automated Verification of Infinite States Systems AVIS'04 (WS ETAPS'04), 2004.	Public
Report	Boichut, Y. and Heam, P.-C. and Kouchnarenko, O., Automatic Verification of Security Protocols Using Approximations, LIFC - Laboratoire d'{I}nformatique de l'Universite de Franche Comte, Research Report number RR2005-01, http://lifc.univ-fcomte.fr/publis/pub/2005/RR2005-01.pdf, 2005.	Public
Article	A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. He□ , J. Mantovani, S. Mdersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, and L. Vigneron. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05). Springer-Verlag, 2005.	Public

INTELLECTUAL PROPERTY RIGHTS

Type of IPR	KNOWLEDGE: Tick a box and give the corresponding details(reference numbers, etc) if appropriate					Pre-existing know-how Tick a box and give the corresponding details(reference numbers, etc) if appropriate	
	Current				Foreseen	Tick	Details
	Tick	NoP[1)]	NoI[2)]	Details	Tick		
Patent applied for							
Patent granted							
Patent search carried out							
Registered design							
Trademark applications							
Copyrights							
Secret know-how							
Other - please specify:							

1) Number of **P**riority (national) applications/patents
2) Number of **I**nternationally extended applications/patents

MARKET APPLICATION SECTORS

Market application sectors
64 Post and telecommunications 72 Computer and related activities 73 Research and development

CURRENT STAGE OF DEVELOPMENT

Current stage of development	Scientific and/or Technical knowledge (Basic research)
Other:	

Quantified data about the result

Items (about the results)	Actual current quantity	Estimated (or future) quantity
Time to application / market (in months from the end of the research project)	0	0
Number of (public or private) entities potentially involved in the implementation of the result:	20	60
of which: number of SMEs:	3	10
of which: number of entities in third countries (outside EU):	7	20
Targeted user audience: of reachable people	100	1000
S&T publications (referenced publications only)	12	20
publications addressing general public (e.g. CD-ROMs, WEB sites)	1	2
publications addressing decision takers / public authorities / etc.		
Visibility for the general public	YES	

Further collaboration, dissemination and use of the result

COLLABORATIONS SOUGHT

R&D	Further research or development	√	**FIN**	Financial support	
LIC	Licence agreement		**VC**	Venture capital/spin-off funding	
MAN	Manufacturing agreement		**PPP**	Private-public partnership	
MKT	Marketing agreement		**INFO**	Information exchange/training	√
JV	Establish a joint enterprise or partnership		**CONS**	Available for consultancy	√
Other	(please specify)				
Details:					

POTENTIAL OFFERED FOR FURTHER DISSEMINATION AND USE

We offer both consulting, in the sense that we can apply our tool T4SP for the validation of protocols developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to apply T4SP and the AVISPA technology in general to validate protocols and applications. We would also gladly consider external collaboration on the future development of T4SP.

PROFILE OF ADDITIONAL PARTNER(S) FOR FURTHER DISSEMINATION AND USE

Both academic partners working on formal methods and automated reasoning for security protocols and applications,

and companies/industry/standardisation organisations working on protocol development or application.

Exploitation plans

CONFIDENTIAL

I am the Co-ordinator of the above project, and confirm on behalf of the contracted Partners the information contained in this Technological Implementation Plan, and I authorise its public dissemination.

Signature: **Name:**

Date: **Organisation:**

close