Project's Achievements Fiche

Questions about project's outcomes	Number	Comments
1. Scientific and technological achievements of the project (and why are they so ?)		
Question 1.1. Which is the 'Breakthrough' or 'real' innovation achieved in the considered period	N/A	Brief description: We have formalised in the HLPSL 112 security problems associated with 33 security protocols that have recently been standardised or are currently undergoing standardisation at IETF or in related standardisation bodies. The techniques for the automatic analysis of security protocols developed by the partners and implemented in the AVISPA Tool have advanced to the point that of the 112 problems considered, 110 are successfully analyses by the AVISPA Tool v.2 in less than 25 minutes each (all 110 problems in 69 minutes).
2. Impact on Science and Technology: Scientific Publications in scientific magazines		
Question 2.1. Scientific or technical publications on reviewed journals and conferences	18	Title and journals/conference and partners involved 1. A. Armando (UNIGE) and L. Compagna (UNIGE). An optimized intruder model for SAT-based model-checking of security protocols. In Proceedings of the IJCAR04 Workshop ARSPA, 2004. To appear in ENTCS, available at http://www.avispa-project.org. 2. A. Armando (UNIGE) and L. Compagna (UNIGE). 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 730733, Lisbon, Portugal, 2004. Springer-Verlag. 3. A. Armando (UNIGE), L. Compagna (UNIGE), and Y. Lierler. Automatic compilation of protocol insecurity problems into logic programming. In Proceedings of the 9th European Conference on Logics in Artificial Intelligence (JELIA'04), volume 3229 of LNAI, pages 617627, Lisbon, Portugal, 2004. Springer-Verlag. 4. A. Armando (UNIGE) and L. Vigano` (ETHZ), editors. Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04). Electronic Notes in Computer Science. Elsevier Science, Amsterdam, The Netherlands, to appear. 5. D. Basin (ETHZ), S. Moedersheim (ETHZ), and L. Vigano` (ETHZ). OFMC: A

Symbolic Model-Checker for Security Protocols. International Journal of Information Security, 2004.

6. Y. Boichut (INRIA), P.-C. Heam (INRIA), O. Kouchnarenko (INRIA), and F. Oehl. Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In Proc. Int. Workshop on Automated Verification of Infinite-State Systems (AVIS'2004), joint to ETAPS'04, pages 111, Barcelona, Spain, 2004. The final version will be published in EN in Theoretical Computer Science, Elsevier.
7. Y. Boichut (INRIA), P.-C. Heam (INRIA), O. Kouchnarenko (INRIA), and F. Oehl. Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In Proceedings of Automated Verification of Infinite States Systems (AVIS'04), ENTCS, 2004. To appear.
8. C. Caleiro, L. Vigano` (ETHZ), and D. Basin (ETHZ). Towards a metalogic for security protocol analysis. In W. A. Carnielli, F. M. Dion´isio, and P. Mateus, editors, Proceedings of the Workshop on the Combination of Logics: Theory and Applications (Comblog'04), pages 187196. Center for Logic and Computation, Departamento de Matema´tica, Instituto Superior Te´cnico, Lisbon, Portugal, 2004.
9. C. Caleiro, L. Vigano` (ETHZ), and D. Basin (ETHZ). Metareasoning about Security Protocols using Distributed Temporal Logic. In Proceedings of the IJCAR'04 Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA'04), Electronic Notes in Computer Science. Elsevier Science, Amsterdam, The Netherlands, to appear.
10. Y. Chevalier (INRIA). A simple constraint combination procedure for cryptographic protocols with xor. In M. Kohlhase, editor, 18th Int. Workshop on Unification, Cork, Ireland, July 2004. Long version available as INRIA Research Report RR-5224.
11. Y. Chevalier (INRIA), L. Compagna (UNIGE), J. Cuellar (Siemens), P. Hankes Drieslma (ETHZ), J. Mantovani (UNIGE), S. Moedersheim (ETHZ), and L. Vigneron (INRIA). A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols, volume 180 of Automated Software Engineering, pages 193205. Austrian Computer Society, Austria, September 2004.

		12. Y. Chevalier (INRIA), R. Ku"sters, M. Rusinowitch (INRIA), and M. Turuani (INRIA). Deciding the Security of Protocols with Commuting Public Key Encryption. In Workshop on Automated Reasoning for Security Protocol Analysis - ARSPA'2004, Electronic Notes in Theoretical Computer Science - ENTCS, Cork, Ireland, Jul 2004. 13. Y. Chevalier (INRIA) and L. Vigneron (INRIA). Rule-based Programs describing Internet Security Protocols. In S. Abdennadher and C. Ringeissen, editors, 5th Int. Workshop on Rule-Based Programming (RULE), Aachen, Germany, June 2004. 14. Y. Chevalier (INRIA) and L. Vigneron (INRIA). Strategy for Verifying Security Protocols with Un- bounded Message Size. Journal of Automated Software Engineering, 11(2):141166, April 2004. 15. G. Delzanno (UNIGE) and P. Ganty (UNIGE). Automatic verification of time sensitive cryptographic protocols. In K. Jensen and A. Podelski, editors, Tools and Algorithms for the Construction and Analysis of Systems, 10th International Conference, TACAS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings, volume 2988 of Lecture Notes in Computer Science, pages 342356. Springer, 2004. 16. P. Hankes Drielsma (ETHZ) and S. Moedersheim (ETHZ). The ASW protocol revisited: A unified view. In Proceedings of the IJCAR04 Workshop ARSPA, 2004. To appear in ENTCS, available at http://www.avispa-project.org. 17. M. Rusinowitch (INRIA). A decidable analysis of security protocols. In J.-J. Le´vy, E. Mayr, and J. Mitchell, editors, 18th IFIP World Computer Congress on Theoretical Computer Science - TCS'2004, Toulouse, France, August 2004. Kluwer Academic Publishers. 18. L. Vigneron (INRIA). Automatic verification of security protocols. In M. Kohlhase, editor, 18th Int. Workshop on Unification, Cork, Ireland, July 2004. Invited talk.
Question 2.2.		

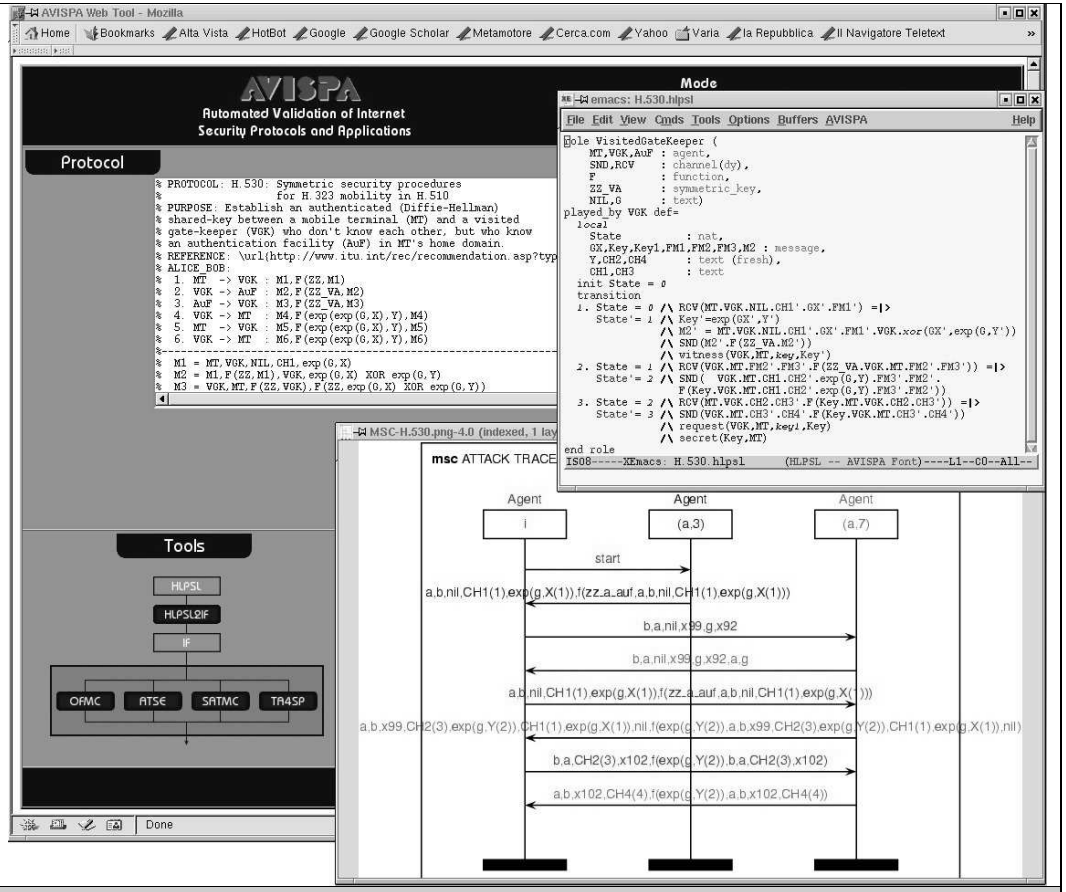
Scientific or technical publications on non-reviewed journals and conferences	0	
Question 2.3. Invited papers published in scientific or technical journal or conference.	0	Title and journals/conference and partners involved 1. M. Rusinowitch. A Decidable Analysis of Security Protocols. In the Proceedings of the 18th IFIP World Computer Congress on Theoretical Computer Science - TCS'2004}, J.-J. Le'vy, E. Mayr, J. Mitchell (editors), Kluwer Academic Publishers, Toulouse, France, August 2004. Invited talk.
3. Impact on Innovation and Micro-economy		
A – Patents		
Question 3.1. Patents filed and pending	0	When and in which country(ies): Brief explanation of the field covered by the patent:
Question 3.2. Patents awarded	0	When and in which country(ies): Brief explanation of the field covered by the patent* (if different from above):
Question 3.3. Patents sold	0	When and in which country(ies): Brief explanation of the field covered by the patent* (if different from above):
Questions about project's outcomes	**Number**	**Comments or suggestions for further investigation**
B - Start-ups		
Question 3.4. Creation of start-up	No	If YES, details: - date of creation: - company name - subject of activity: - location:

		- headcount: - turnover: - profitable : yes / no / when expected - web address:
Question 3.5. Creation of new department of research (ie: organisational change)	No	Name of department and institution/company:
C – Technology transfer of project's results		
Question 3.6. Collaboration/ partnership with a company?	1	Which partner: UNIGE, INRIA, ETHZ Which company : Siemens What kind of collaboration? Siemens AG is partner in the project. The role of Siemens within the project is twofold: • Definition of 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. • Dissemination of the project's results within standardisation bodies and at main international scientific events by means of presentations and tutorials.
4. Other effects		
A - Participation to Conferences/Symposium/Workshops or other dissemination events		
Question 4.1. Active participation[1] to Conferences in EU Member states, Candidate countries / NAS. (specify if one partner or "collaborative" between partners)	2	Names/ Dates/ Subject area / Country: Organisers: Alessandro Armando (UNIGE), David Basin (ETHZ), Jorge Cuellar (Siemens), Michael Rusinowitch (INRIA) and Luca Vigano` (ETHZ) Title: *Workshop on Automated Reasoning for Security Protocols Analysis* (ARSPA'04) Type: Collaborative Number of attendees: about 50 Subject Area: Security Protocol Analysis, Automated Reasoning Country: University College Cork, Ireland

[1] 'Active Participation' in the means of organising a workshop / session / stand / exhibition directly related to the project (apart from events presented in section 2).

		Date: July 4, 2004 URL: http://www.avispa-project.org/arspa Organisers: Jorge Cuellar (Siemens), Sebastian Moerdersheim (ETHZ) and Luca Vigano` (ETHZ) Title: *Full day tutorial on Automated Validation of Security Protocols* (AVASP'04) Type: Collaborative Subject Area: Security Protocol Analysis, Automated Reasoning Country: University College Cork, Ireland Date: July 4, 2004 URL: http://www.avispa-project.org/avasp
Question 4.2. Active participation to Conferences outside the above countries (specify if one partner or "collaborative" between partners)	0	Names/ Dates/ Subject area / Country:
B – Training effect		
Question 4.3. Number of PhD students hired for project's completion	7	In what field: Automatic analysis of security protocols, model-checking of finite and infinite-state systems.
Questions about project's outcomes	**Number**	**Comments or suggestions for further investigation**
C - Public Visibility		
Question 4.4. Media appearances and general publications (articles, press releases, etc.)	0	References:
Question 4.5. Web-pages created or other web-site links	4	References:

related to the project		http://www.avispa-project.org/ http://www.avispa-project.org/avasp http://www.avispa-project.org/arspa http://www.avispa-project.org/software
Question 4.6. Video produced or other dissemination material	0	References: (Please attach relevant material)
Question 4.7. Key pictures of results	0	References: Snapshot of the graphical user interface of the AVISPA Tool v.2

		
D - Spill-over effects		
Question 4.8. Any spill-over to national programs	No	If YES, which national programme(s):

Question 4.9. Any spill-over to another part of EU IST Programme	No	If YES, which IST programme(s):
Question 4.10. Are other team(s) involved in the same type of research as the one in your project?	Yes	If YES, which organisation(s): • The PROUVE Project (Follow up to EVA). It includes all the partners of EVA plus INRIA-Lorraine and France Telecom R&D. • The Project DEGAS (IST-2001-32072, http://www.omnys.it/degas/). Organisations involved: University of Trento, Technical University of Denmark, University of Pisa, and University of Edinburgh. • Bruno Blanchet 's group at the MPI for computer science (Saarbruecken, Germany). • The Eindhoven Computer Science Security Group led by Prof. Sjouke Mauw. • Jonathan Millen's group at SRI International. More information can be found in Section 2.6 of Deliverable D1.2.