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 215 security problems associated with 48 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 all the 215 problems considered are successfully analysed by the AVISPA Tool in less than 24 minutes each (all 215 problems in 87 minutes). All the prototype tools developed by the partners have been integrated in the AVISPA Tool. The results of the project have been widely disseminated and the AVISPA Tool (now publicly available on the project web-site) has been officially presented at the 62nd Meeting of the IETF and at the 17th International Conference on Computer Aided Verification (CAV'05).
2. Impact on Science and Technology: Scientific Publications in scientific magazines		
Question 2.1. Scientific or technical publications on reviewed journals and conferences	20	1. 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 , 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. Available at www.avispa-project.org. 2. A. Armando, C. Castellini, E. Giunchiglia, and M. Maratea. The SAT-based Approach to Separation Logic. Technical report, UNIGE, 2005. To be published in the Journal of Automated Reasoning, 2005. 3. A. Armando and L. Compagna. An Optimized Intruder Model for SAT-based ModelChecking of Security Protocols. In Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2004), pages 91-108. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct), July 2005. 4. A. Armando and L. Viganò. Preface (editorial). Electronic Notes in Theoretical Computer Science (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004), 125(1):1, 2005. 5. A. Armando and L. Viganò, editors. Proceedings of the Workshop on Automated Reasoning for

Security Protocol Analysis (ARSPA 2004), Amsterdam, The Netherlands, 2005. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct).

6. D. Basin, S. Moedersheim, and L. Viganò. OFMC: A symbolic model checker for security protocols. International Journal of Information Security, 4(3):181-208, June 2005. Published online December 2004.
7. C. Caleiro, L. Viganò, and D. Basin. Deconstructing Alice and Bob. Electronic Notes in Theoretical Computer Science 135(1):3-22 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005), 2005.
8. C. Caleiro, L. Viganò, and D. Basin. Metareasoning about security protocols using distributed temporal logic. Electronic Notes in Theoretical Computer Science (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2004), 125(1):67-89, 2005.
9. C. Caleiro, L. Viganò, and D. Basin. Relating strand spaces and distributed temporal logic for security protocol analysis. Logic Journal of the IGPL, to appear.
10. Y. Chevalier, R. Kuesters, M. Rusinowitch, and M. Turuani. An NP Decision Procedure for Protocol Insecurity with XOR. Theoretical Computer Science, 338(1-3):247- 274, June 2005.
11. Y. Chevalier and M. Rusinowitch. Combining Intruder Theories. Technical report, INRIA -- extended abstract to appear in the proceedings of ICALP'05, 2005. http://www.inria.fr/rrrt/rr-5495.html.
12. Y. Chevalier and M. Rusinowitch. Combining Intruder Theories. In L. Vigneron, editor, Proceedings of the 19th International Workshop on Unification, pages 63-76, Nara, Japan, April 2005.
13. V. Cortier, R. M., and E. Zalinescu. A resolution strategy for verifying cryptographic protocols with cbc encryption and blind signatures. In Proceedings of the 7th ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'05), Lisboa, Portugal. ACM press, July 2005.
14. V. Cortier and B. Warinschi. Computationally Sound, Automated Proofs for Security Protocols. In Proc. 14th European Symposium on Programming (ESOP'05), volume 3444 of Lecture Notes in Computer Science, pages 157-171, Edinburgh, U.K, April 2005. Springer.
15. P. Degano and L. Viganò. Preface (editorial). Electronic Notes in Theoretical Computer Science 135(1):1-2 (Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA 2005), 2005.
16. P. Degano and L. Viganò, editors. Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2005). Electronic Notes in Theoretical Computer Science (Elsevier Science Direct), to appear.
17. P. Hankes Drielsma and S. Moedersheim. The ASW Protocol Revisited: A Unified View. In Proceedings of the Workshop on Automated Reasoning for Security Protocol Analysis (ARSPA

		2004), pages 141-156. Electronic Notes in Theoretical Computer Science 125 (Elsevier Science Direct), July 2005. 18. P. Hankes Drielsma, S. Moedersheim, and L. Viganò. A formalization of off-line guessing for security protocol analysis. In F. Baader and A. Voronkov, editors, Proceedings of LPAR'04, volume 3452 of LNAI, pages 363-379. Springer, 2005. 19. L. Vigneron. A Tool helping to Design Cryptographic Protocols (tutorial). In 4th Conference on Security and Network Architectures (SAR'05), Batz sur Mer, France, June 2005. 20. L. Vigneron, editor. Proceedings of the 19th International Workshop on Unification, Nara, Japan, April 2005. Available as LORIA Research Report A05-R-022, Nancy, France.
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
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):

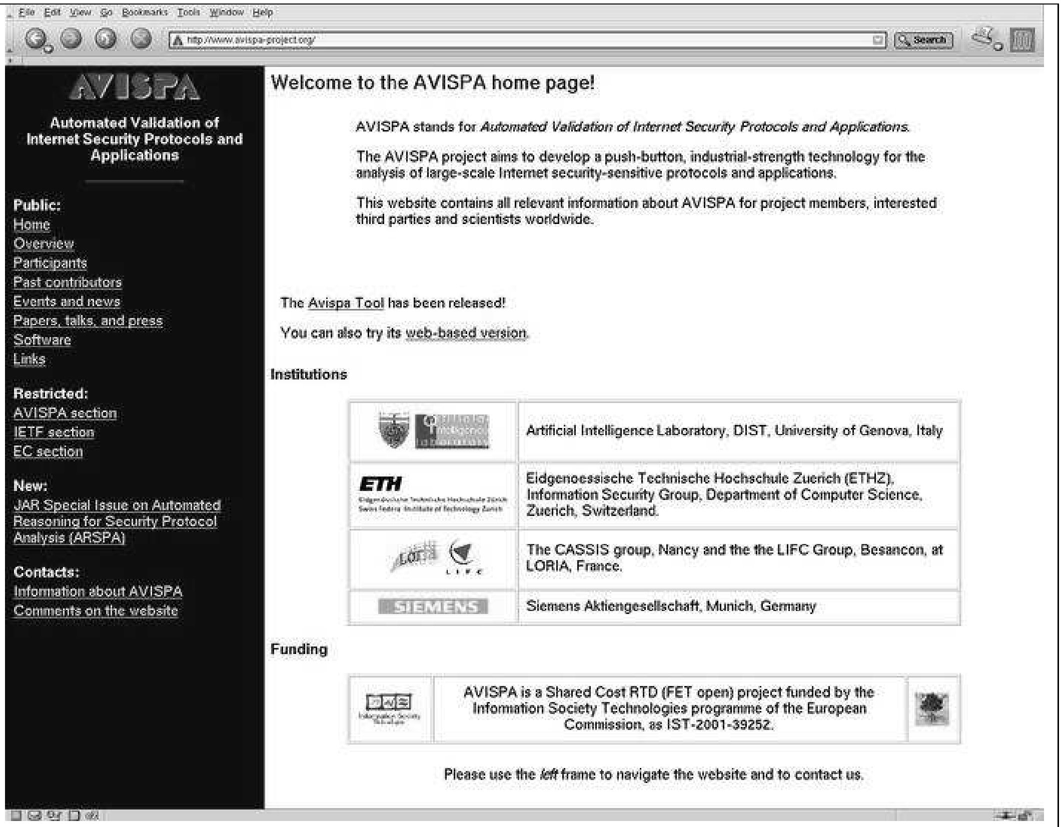
Question 3.3. Patents sold	0	When and in which country(ies): Brief explanation of the field covered by the patent* (if different from above):
Questions about project’s outcomes	**Number**	**Comments or suggestions for further investigation**
B - Start-ups		
Question 3.4. Creation of start-up	No	If YES, 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.

		Which partner: INRIA Which company : LEIRIOS and AXALTO What kind of collaboration? Joint national research project RNTL submitted in June 2005.
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)	4	Names/ Dates/ Subject area / Country: Organisers: Pierpaolo Degano (University of Pisa, Italy) and Luca Viganò (ETHZ) Title: *Workshop on Automated Reasoning for Security Protocols Analysis* (ARSPA'05) Type: Collaborative Number of attendees: about 40 Subject Area: Security Protocol Analysis, Automated Reasoning Country: Portugal Date: July 16, 2005 URL: http://www.avispa-project.org/arspa Organisers: Sebastian Moerdersheim (ETHZ), David von Oheimb (Siemens), and Luca Viganò (ETHZ) Title: *Full day tutorial on Automated Validation of Security Protocols* (AVASP'05) Type: Collaborative Subject Area: Security Protocol Analysis, Automated Reasoning Country: UK Date: April 3, 2005 URL: http://www.avispa-project.org/avasp Organisers: Bruno Blanchet and Veronique Cortier and Yassine Laknech Title: Workshop on the link between formal and computational models Type: INRIA Number of attendees: about 70 Subject Area: Security Proofs Country: France Date: 23-24 June 2005.

[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).

		Organisers: Laurent Vigneron (INRIA) Title: 19th International Workshop on Unification (UNIF'05) Type: INRIA Number of attendees: about 50 Subject Area: Automated Reasoning, Applications to Security Country: Japan Date: April 22, 2005 URL: http://www.loria.fr/
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: Laurent Vigneron (INRIA), April 22, 2005. 19th International Workshop on Unification (UNIF'05), Nara, Japan.
B – Training effect		
Question 4.3. Number of PhD students hired for project's completion	7	• 2 PhD Students have developed their PhD in the context of the project • 4 PhD Students have developed a significant part of their thesis in the context of the project.
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 related to the project	4	References: http://www.avispa-project.org/

		http://www.avispa-project.org/avasp http://www.avispa-project.org/arspa http://www.avispa-project.org/software http://www.avispa-project.org/web-interface
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 AVISPA Project web site.

		 File Edit View Go Bookmarks Tools Window Help http://www.avispa-project.org/ Search **AVISPA** **Automated Validation of Internet Security Protocols and Applications** **Public:** Home Overview Participants Past contributors Events and news Papers, talks, and press Software Links **Restricted:** AVISPA section IETF section EC section **New:** JAR Special Issue on Automated Reasoning for Security Protocol Analysis (ARSPA) **Contacts:** Information about AVISPA Comments on the website Welcome to the AVISPA home page! AVISPA stands for *Automated Validation of Internet Security Protocols and Applications*. The AVISPA project aims to develop a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. This website contains all relevant information about AVISPA for project members, interested third parties and scientists worldwide. The Avispa Tool has been released! You can also try its web-based version. **Institutions** Artificial Intelligence Laboratory, DIST, University of Genova, Italy Eidgenoessische Technische Hochschule Zuerich (ETHZ), Information Security Group, Department of Computer Science, Zuerich, Switzerland. The CASSIS group, Nancy and the the LIFC Group, Besancon, at LORIA, France. Siemens Aktiengesellschaft, Munich, Germany **Funding** AVISPA is a Shared Cost RTD (FET open) project funded by the Information Society Technologies programme of the European Commission, as IST-2001-39252. Please use the *left* frame to navigate the website and to contact us.
D - Spill-over effects		
Question 4.8. Any spill-over to national programs	No	If YES, which national programme(s): • Italian national project on the verification of security protocols funded by the Italian Ministry for Research and Education in the context of the FIRB programme (Project No.

		RBAU01P5SS). Institutions involved: University of Genova, University of Trento and University of Naples. The project is using and extending the HLPSL specification language of AVISPA to specify special classes of security protocols and properties. • Swiss National Project "Verifiably Secure Protocols for Wireless Networks" (VerSePro) funded by the Swiss National Science Foundation, starting October 2005. Institutions involved: ETHZ Zurich and EPFL Lausanne. The goals of the project are to design security protocols for specific tasks in wireless networks, to develop verification methods to ensure their correctness, and to implement the verification methods within the OFMC protocol analysis tool (one of the back-ends of the AVISPA tool) in order to support the automated analysis of security properties of a wide class of mobility protocols.
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. • MyThS, Models and Types for Security in Mobile Distributed Systems, funded by the Global Computing pro-active initiative (GC) of the Future and Emerging Technologies (FET). (Contract IST-2001-32617). • Bruno Blanchet’s groups at the MPI for computer science (Saarbruecken, Germany) and at the ENS (France). • 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 D1.3.