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 advanced the specification and deduction technologies towards the point where industrial-scale security-sensitive protocols can be specified and automatically analysed. We have started the integration of this technology into a robust automated tool, tuned on practical, large-scale problems.
2. Impact on Science and Technology: Scientific Publications in scientific magazines		
Question 2.1. Scientific or technical publications on reviewed journals and conferences	13	Title and journals/conference and partners involved 1. P. Ammirati (UNIGE) and G. Delzanno (UNIGE). Constraint-based Automatic Verification of Time Dependent Security Properties. In Proceedings of SPV'03. 2. A. Armando (UNIGE) and L. Compagna (UNIGE). Abstraction-driven SAT-based Analysis of Security Protocols. In Proceedings of SAT 2003, LNCS 2919. Springer-Verlag, 2003. 3. A. Armando (UNIGE), L. Compagna (UNIGE), and P. Ganty (UNIGE). 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. 4. D. Basin (ETHZ), S. Mödersheim (ETHZ), and L. Viganò (ETHZ). 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. 5. D. Basin (ETHZ), S. Mödersheim (ETHZ), and L. Viganò (ETHZ). 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. 6. D. Basin (ETHZ), S. Mödersheim (ETHZ), and L. Viganò (ETHZ). Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of

		Security Protocols (Extended Abstract). In Proceedings of SPV'03, 2003. 7. Y. Chevalier (INRIA), R. Küsters, M. Rusinowitch (INRIA), and M. Turuani (INRIA). An NP Decision Procedure for Protocol Insecurity with XOR. In Proceedings of the Logic In Computer Science Conference, LICS'03, pages 261--270, 2003. 8. Y. Chevalier (INRIA), R. Küsters, M. Rusinowitch (INRIA), and M. Turuani (INRIA). 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, FST TCS'03, LNCS 2914. Springer-Verlag, 2003. 9. Y. Chevalier (INRIA), R. Küsters, M. Rusinowitch (INRIA), M. Turuani (INRIA), and L. Vigneron (INRIA). Extending the Dolev-Yao Intruder for Analyzing an Unbounded Number of Sessions. In M. Baaz, editor, Proceedings of CSL'2003, LNCS 2803. Springer-Verlag, 2003. 10. G. Delzanno (UNIGE) and P. Ganty (UNIGE). Symbolic Methods for Automatically Proving Secrecy and Authentication in Infinite-state Models of Cryptographic Protocols. In Proceedings of the Workshop on Issues in Security and Petri Nets (WISP'03), 2003. 11. G. Delzanno (UNIGE) and P. Ganty (UNIGE). Automatic Verification of Time Sensitive Cryptographic Protocols. In Proceedings of TACAS'04, 2004. 12. M. Rusinowitch (INRIA). Automated Analysis of Security Protocols. In G. Vidal, editor, Proceedings of the 12th International Workshop on Functional and (Constraint) Logic Programming, WFLP'03, volume 86(3). Electronic Notes in Theoretical Computer Science, 2003. 13. M. Rusinowitch (INRIA) and M. Turuani (INRIA). Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete. Theoretical Computer Science, 299:451--475, 2003.
Question 2.2. Scientific or technical publications on non-reviewed journals and conferences	2	Title and journals/conference and partners involved 14. Y. Chevalier (INRIA). Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques. Phd, Université Henri Poincaré, Nancy,

		December 2003. 15. M. Turuani (INRIA). Sécurité des Protocoles Cryptographiques: Décidabilité et Complexité. Phd, Université Henri Poincaré, Nancy, December 2003.
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

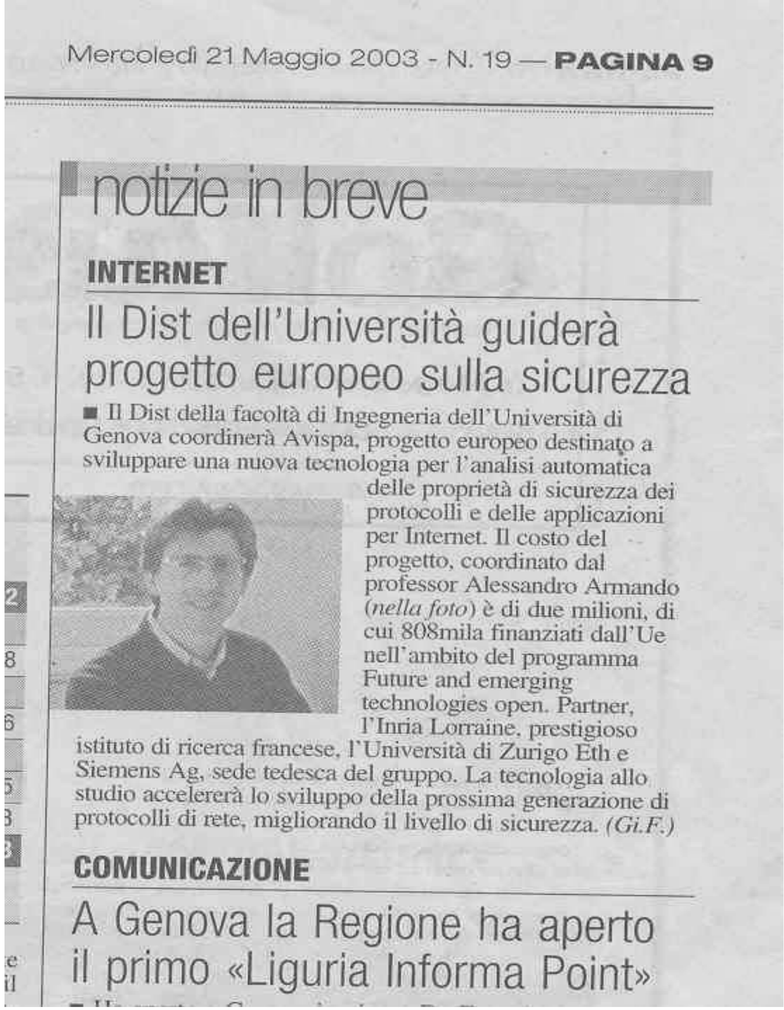
		- subject of activity: - location: - headcount: - turnover: - profitable : yes / no / when expected - web address:
Question 3.5. Creation of new department of research (ie: organisational change)	No	Name of department and institution/company:
C – Technology transfer of project's results		
Question 3.6. Collaboration/ partnership with a company ?	0	Which partner : Which company : What kind of collaboration ?
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)	1	Names/ Dates/ Subject area / Country: Roberto Amadio, Hubert Comon, Michael Rusinowitch (INRIA), Andre Scedrov. *SPV -- Workshop on Security Protocols Verification*, 06.09.2003, Marseille, France. (Workshop Web-Site: http://www.loria.fr/~rusi/spv.html
Question 4.2. Active participation to Conferences outside the above countries	1	Names/ Dates/ Subject area / Country: Jorge Cuellar (Siemens). Full day tutorial at the International Conference on Software Engineering

[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).

(specify if one partner or "collaborative" between partners)		And Formal Methods (SEFM 2003, Brisbane, Australia, 22nd - 27th September, 2003). Available at www.svrc.uq.edu.au/Events/SEFM03 and www.avispa-project.org.
B – Training effect		
Question 4.3. Number of PhD students hired for project's completion	8	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.)	1	References: Article in the "Il Sole 24 Ore, no. 19" published on May 21, 2003 (see Appendix)
Question 4.5. Web-pages created or other web-site links related to the project	1	References: http://www.avispa-project.org
Question 4.6. Video produced or other dissemination material	0	References: (Please attach relevant material)
Question 4.7. Key pictures of results	0	References: (Please attach relevant material .jpeg or .gif)
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 ?	No	If YES, which organisation(s):

Appendix: Media Appearance



Mercoledì 21 Maggio 2003 - N. 19 — **PAGINA 9**

notizie in breve

INTERNET

Il Dist dell'Università guiderà progetto europeo sulla sicurezza

■ Il Dist della facoltà di Ingegneria dell'Università di Genova coordinerà Avispa, progetto europeo destinato a sviluppare una nuova tecnologia per l'analisi automatica delle proprietà di sicurezza dei protocolli e delle applicazioni per Internet. Il costo del progetto, coordinato dal professor Alessandro Armando (*nella foto*) è di due milioni, di cui 808mila finanziati dall'Ue nell'ambito del programma Future and emerging technologies open. Partner, l'Inria Lorraine, prestigioso istituto di ricerca francese, l'Università di Zurigo Eth e Siemens Ag, sede tedesca del gruppo. La tecnologia allo studio accelererà lo sviluppo della prossima generazione di protocolli di rete, migliorando il livello di sicurezza. *(Gi.F.)*

COMUNICAZIONE

A Genova la Regione ha aperto il primo «Liguria Informa Point»