AVISS — Automated Verification of Infinite State Systems

(IST-2000-26410)

Deliverable D1.2

Dissemination and Use Plan

1 Introduction

As described in the previous deliverables (D3.1–3), we have begun experimenting with our prototype verification tool and testing it against the protocols of the corpus [3]. This deliverable D1.2 describes the *Dissemination and Use Plan* of the project, which we have finalized during the second official project meeting in Freiburg (20–21.9.01) and during a number of follow-up informal meetings in Dagstuhl (23–28.9.01).

In fact, a major goal of the second half of this assessment phase is the dissemination and use of our approach, techniques and tools within the scientific community, both academic and industrial. To this end, in parallel to the development activities (the remaining tasks of the project, turning our prototype into a successful protocol verification tool), we have initiated communication and collaboration with a number of academic and industrial partners. This will allow us to improve our tool and identify a set of representative case studies coming from the industrial practice on which to apply the results of the project; this will thus pave the way to turning the prototype into a mature technology, whose application in the industrial setting will be ascertained in a follow-up, full RTD project with industry involvement.

The following illustrates the dissemination and use steps we have already realized and the ones we will carry out in the next months.

2 First project half

Representatives of all three project partners were among the academic and industrial participants at the Dagstuhl seminar "Specification and Analysis of Secure Cryptographic Protocols", co-organized by David Basin together with other leading researchers in the field of security protocol verification, namely Grit Denker and Jon Millen from SRI International Menlo Park and Gawin Lowe from Oxford University.[1] There, David Basin and Michaël Rusinowitch gave official seminar talks presenting the work of the different partners and the prototype tool we are developing. Most importantly, during the seminar week, we had the opportunity of giving more in-depth demonstrations of the tools to a number of interested participants. In particular, Grit Denker and Jon Millen from SRI International have expressed their interest in our project and have suggested possible collaborations. So has Jorge Cuellar from Siemens AG. Indeed, as a result of the seminar and of a subsequent visit to Freiburg by Dr. Cuellar, where he held a block-course on computer security ("Standardization of Internet Protocols"), Siemens has expressed their interest in partaking in the full RTD project that will follow this assessment phase.

The project has also been presented on 1.10.01 to Prof. Alan Bundy (University of Edinburgh) and Prof. Jörg Siekmann (Universität des Saarlandes) and on 11.10.01 to Prof. Moshe Vardi (Rice University) during their visits to the Genova group.

Luca Compagna and Enrico Giunchiglia from Genova and David Basin have also participated to the Dagstuhl seminar "Exploration of Large State Spaces" (4–9.11.01) and given project-related talks.

A preliminary version of the lazy intruder approach, which has been implemented in our prototype tool, has been presented by Yannick Chevalier and Laurent Vigneron at the Verification Workshop of the conference IJCAR (VERIFY'01, Siena, Italy, 19.6.01) [2]. They will also present the actual lazy intruder approach and some experiments with the theorem prover daTac at the 16th IEEE International Conference on Automated Software Engineering (ASE'01, San Diego, 26–29.11.01) [1].

Michaël Rusinowitch has given an invited talk presenting the work done by Nancy on this project at the Post-CAV Workshop on Logical Aspects of Cryptographic Protocols, Paris, 23.7.01 [4]. He also presented the project at Journées Systèmes et Logiciels Critiques, Grenoble, 6.11.01

[1] The seminar, which took place 23–28.9.01, that is immediately after the second project meeting (Freiburg, 20–21.9.01), was attended by David Basin, Sebastian Mödersheim and Luca Viganò from Freiburg, Alessandro Armando from Genova, and Michaël Rusinowitch from Nancy. More information on the seminar can be found at `http://www.dagstuhl.de`.

(`http://www.systemes-critiques.org/journees2001.php`). He gave a seminar at TU Vienna on 28.5.01 and will give another one at Kiel University on 6.12.01 on the same topic. A theoretical result that is directly related to the AVISS objectives (namely that protocol insecurity with finite number of sessions is NP–complete) has been presented at the 14th IEEE Computer Security Foundation Workshop, Cape Breton, Canada, on 12.6.01 [5].

3 Second project half

Dissemination and use of our tool will continue both on an informal basis, with presentations and demonstrations to researchers from academia and industry during informal meetings and visits, and on a formal basis, with official conferences and meetings.

More specifically, to further disseminate the results of our project, the different partners have planned to submit both independent papers and a joint project presentation paper at the conferences on security protocol verification that will take place next year, such as the Computer Security Foundations Workshop (CSFW 2002) and the European Symposium on Research in Computer Security (ESORICS 2002).

Further, while participation to the next project meeting (that will take place 12–13.12.01 in Nancy) will be restricted to the project partners, the final meeting (planned for March, in Genova) will be open and we will invite a number of prospective academic and industrial partners for the follow-up RTD project. Jorge Cuellar, Francis Klay (France Télécom R&D), and Juan Ortega (University of Malaga) have already expressed their interest in participating to this meeting, and we will give demonstrations of our verification tool that, we believe, will ensure their collaboration for the full project.

Bibliography

[1] Y. Chevalier and L. Vigneron. A Tool for Lazy Verification of Security Protocols. In *Proceedings of the Automated Software Engineering Conference (ASE'01)*. IEEE Computer Society Press, 2001. Long version available as Technical Report A01-R-140, LORIA, Nancy (France).

[2] Y. Chevalier and L. Vigneron. Towards Efficient Automated Verification of Security Protocols. In *Proceedings of the Verification Workshop (VERIFY'01) (in connection with IJCAR'01), Università degli studi di Siena, TR DII 08/01*, pages 19–33. 2001.

[3] J. Clark and J. Jacob. A survey of authentication protocol literature: Version, 1997.

[4] Michael Rusinowitch. The practice of cryptographic protocols verification. In Jean Goubault-Larrecq, editor, *CAV Workshop on Logical Aspects of Cryptographic Protocols Verification*, Electronic Notes in Theoretical Computer Science ENTCS 55(1). Elsevier Science Publishers, Amsterdam, July 2001. Invited talk.

[5] Michael Rusinowitch and Mathieu Turuani. Protocol Insecurity with Finite Number of Sessions is NP-complete. In *Proceedings of the 14th IEEE Computer Security Foundations Workshop*. 2001.