The High-Level Protocol Specification Language HLPSL developed in the project AVISPA

David von Oheimb*
Siemens AG, Corporate Technology IC Sec, Munich, Germany
David.von.Oheimb@siemens.com

Abstract. The just recently finished EU project AVISPA, *Automated Validation of Internet Security Protocols and Applications*, has aimed at developing a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications.
In this short industrial contribution paper, after giving a very brief overview of the AVISPA project, we introduce HLPSL, the *High-Level Protocol Specification Language* developed and used within the project to model security protocols and to specify their desired properties.
This language enjoys a formal semantics based on Lamport's Temporal Logic of Actions. HLPSL is modular and allows for the specification of control flow patterns, data-structures, alternative intruder models, and complex security properties. It is sufficiently high-level to be accessible to protocol engineers (themselves not necessarily formal methods experts), yet easily translatable into a lower-level term-rewriting based language suited to model-checking tools.

1 AVISPA

The project AVISPA [AH-03] was conducted between January 2003 and June 2005 by the following four project partners:

- the Artificial Intelligence Laboratory at DIST, Università di Genova,
- the CASSIS group at INRIA, Nancy, France
- the Information Security Group at ETHZ, Zürich, Switzerland
- Siemens Corporate Technology, München, Germany

The overall goals of the project were

- to develop a rich specification language for formalising protocols, security goals, and threat models of industrial complexity,
- to advance the state-of-the-art in automated deduction techniques to scale up to this complexity,
- to build a tool based on these techniques that allows industry and standardisation bodies to automatically validate or detect errors in their products,
- to tune this tool and demonstrate proof-of-concept on a large collection of practically relevant, industrial protocols, and

* Research partially funded by the Shared cost RTD (FET open) EU project AVISPA, IST-2001-39252

– to begin the migration of this technology into industry standardisation organisations such as the IETF so that both the scientific and the industrial community can benefit from the advances achieved by this project.

Now, after the successful completion of the project itself, various continuations and extensions are under way.

2 HLPSL

HLPSL [CCC+04] is the language through which protocol modellers and analysers make use of the AVISPA Tool. In order to be be easily usable, HLPSL provides a high level of abstraction and offers many features needed to specify large-scale Internet security protocols: symmetric and asymmetric encryption, non-atomic keys, key tables, Diffie-Hellman key-agreement, hash functions, algebraic functions, typed and untyped data. HLPSL specifications are translated to the so-called *Intermediate Format (IF)*, a language at an accordingly lower abstraction level and is thus more suitable for automated deduction.

Protocol specifications in HLPSL are divided into *roles*. Some roles, the so-called *basic* roles, serve to describe the actions of one single agent in a run of a protocol or sub-protocol. Other roles, namely *composed* roles, instantiate several of these basic roles to model an entire protocol run. The *environment* role define the concrete agents and sessions whose execution is consider, as well as the intruder knowledge and other global entities. Finally, the security goals are stated. Currently, HLPSL supports only different forms of authentication and secrecy goals, but further security objectives, like fairness and non-repudiation properties for contract-signing protocols, are planned for future versions.

3 Conclusion

The very challenging and ambitious aims of the project AVISPA were largely fulfilled. In particular, HLPSL is an expressive language that can be efficiently used by protocol designers even with little training, as our experience with the use by students shows. The technology developed is publicly available [AT-05], including software and extensive documentation. It is already of great help for the analysis of current industrial-strength security protocols and will reduce time-to-market of new protocols and increase trust in the security of the Internet and of advanced, distributed IT applications.

References

AH-03. The AVISPA project homepage. http://www.avispa-project.org/, 2003.

AT-05. The AVISPA Tool. Available at http://www.avispa-project.org/, 2005.

CCC+04. Yannick Chevalier, Luca Compagna, Jorge Cuellar, Paul Hankes Drielsma, Jacopo Mantovani, Sebastian Mödersheim, and Laurent Vigneron. *A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols*, volume 180 of *Automated Software Engineering*, pages 193–205. Austrian Computer Society, Austria, September 2004.