Automatic Verification of Security Protocols*

Laurent Vigneron

LORIA — UN2-CNRS
Campus Scientifique, B.P. 239
54506 Vandœuvre-lès-Nancy Cedex, France
vigneron@loria.fr

Internet is becoming everyday a more widely used medium for electronic commerce. This development is hampered by the natural insecurity of communications, as it is not possible to guarantee that some data exchanged is not listened by someone else, or even that it really originated from the claimed sender. This lack of security leads to the development of *security protocols*, that is small messages sequences, after which the author provides some properties to the user, such as the correct identification of the users (called *agents*) and the privacy of some data pieces.

There has been a significant amount of work toward the specification of security protocols [14, 1, 10, 5, 2, 6] and the search for attacks [12, 15, 13, 16, 11, 2, 9], but much less toward the positive verification of protocol properties [3, 4, 8, 7].

After a quick overview of the main techniques developped for considering these three levels, we will focus on some recent ones that are based on constraint solving and unification. They combine several different problems, such as unification and matching in some theories, reachability problems, deduction, and all this in the context of the properties of cryptographic primitives.

References

1. M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *Proc. of the 4th ACM Conference on Computer and Communications Security*, pages 36–47. ACM Press, 1997.
2. A. Armando, D.A. Basin, M. Bouallagui, Y. Chevalier, L. Compagna, S. Bdersheim, M. Rusinowitch, M. Turuani, L. Viganò, and L. Vigneron. The AVISS security protocol analysis tool. In *Proc. of the 14th International Conference of Computer Aided Verification (CAV 2002)*, volume 2404 of *LNCS*, pages 349–353. Springer, 2002.
3. B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. of the 14th Computer Security Foundations Workshop (CSFW'01)*. IEEE Computer Society Press, June 2001.
4. L. Bozga, Y. Lakhnech, and M. Périn. Pattern-based abstraction for verifying secrecy in protocols. In *Tools and Agorithms for the Construction and Analysis of Sytems (TACAS'03)*, volume 2619 of *LNCS*, 2003.

* This work was partially funded by the Information Society Technologies programme of the European Commission, Future and Emerging Technologies under the IST-2001-39252 AVISPA project, and the RNTL 03V360 Prouvé project.

5. Common Authentication Protocol Specification Language. `http://www.csl.sri.com/~millen/capsl/`.
6. Y. Chevalier and L. Vigneron. 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.
7. V. Cortier. Vérifier les protocoles cryptographiques. *Techniques et Sciences Informatiques*, 2004. À paraître.
8. V. Cortier, J. Millen, and H. Rueß. Proving secrecy is easy enough. In *Proc. of the 14th Computer Security Foundations Workshop (CSFW'01)*, pages 97–108. IEEE Computer Society Press, 2001.
9. T. Genet, Y.-M. Tang-Talpin, and V. Viet Triem Tong. Verification of copy-protection cryptographic protocol using approximations of term rewriting systems. In *Proc. of the Workshop on Issues in the Theory of Security (WITS'03)*, 2003.
10. G. J. Holzmann. The Spin Model Checker. *IEEE Transactions on Software Engineering*, 23(5):279–295, May 1997.
11. F. Jacquemard, M. Rusinowitch, and L. Vigneron. Compiling and verifying security protocols. In *Logic for Programming and Automated Reasoning (LPAR'00)*, volume 1955 of *LNCS*, November 2000.
12. G. Lowe. Casper: A compiler for the analysis of security protocols. In *Proc. of 10th Computer Security Foundations Workshop (CSFW'97)*. IEEE Computer Society Press, 1997. Also in Journal of Computer Security, Volume 6, pages 53-84, 1998.
13. J. Mitchell, M. Mitchell, and U. Stern. Automated analysis of cryptographic protocols using murphi. In *Proc. of the IEEE Symposium on Security and Privacy*, pages 141–151. IEEE Computer Society Press, May 1997.
14. A. W. Roscoe. Modelling and verifying key-exchange protocols using CSP and FDR. In *Proceedings of the 8th IEEE Computer Security Foundations Workshop CSFW'95*, pages 98–107. IEEE Computer Society Press, 1995.
15. P.Y.A. Ryan, S.A. Schneider, M.H. Goldsmith, G. Lowe, and A.W. Roscoe. *The modelling and analysis of security protocols: the CSP approach*. Addison-Wesley, 2000.
16. D. X. Song. Athena: A new efficient automatic checker for security protocol analysis. In *Proc. of the 12th Computer Security Foundations Workshop (CSFW'99)*. IEEE Computer Society Press, June 1999.