AUTOMATIC PROVING OF THE CORRECTNESS OF CRYPTOGRAPHIC PROTOCOLS

Peter Rajský

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology
Ilkovičova 3, 81219 Bratislava, Slovak Republic
peter.rajsky@elline.sk

Ongoing discoveries of security-related flaws persuade us that informal arguments about security of cryptographic protocols are not sufficient. In this paper we present a method by which it is possible to prove that by fulfilling of certain assumptions a protocol really do that it is supposed to. A big advantage of the presented method is it's possibility of automatization. It's disadvantage is that it is not complete, hence there are correct protocols that cannot be proved by it. However we believe that the possibility of automatic verification - even in interaction of multiple protocols - makes it attractive for future practical exploitation.

References

[1] C. Meadows: *The NRL Protocol Analyzer: An Overview*, Journal of logic programming, 1994.

[2] G. Lowe: *SPLICE/AS: A case study in using CSP to detect errors in security protocols*, Technical report, Oxford University Computing Laboratory, 1996.

[3] J. C. Mitchell, M. Mitchell, U. Stern: *Automated analysis of cryptographic protocols using Murphi*, IEEE Symposium on Security and Privacy, 141-151, 1997.

[4] B. B. Nieh, Tavares Stafford E.: *Modelling and Analyzing Cryptographic Protocols Using Petri Nets*, AUSCRYPT'92, 1992.

[5] L. C. Paulson: *The inductive approach to verifying cryptographic protocols*, Journal of Computer Security, 85-128, 1998.

[6] M. Burrows, M. Abadi, R. Needham: *A Logic of Authentication*, Digital Equipment Corporation, 1989.

[7] M.Debbabi, M.Mejri, N.Tawbi, I.Yahmadi: *A New Algorithm for the Automatic Verification of Authentication Protocols: From Specifications to Flaws and Attack Scenarios.*