Verification of Security Protocols

Véronique Cortier
LORIA - CNRS, INRIA, Université de Lorraine, Nancy, France
https://members.loria.fr/VCortier/
veronique.cortier@loria.fr

Abstract

Cryptographic protocols aim at securing communications over insecure networks like the Internet. Over the past decades, numerous decision procedures and tools have been developed to automatically analyse the security of protocols. The field has now reached a good level of maturity with efficient techniques for the automatic security analysis of protocols

After an overview of some famous protocols and flaws, we will describe the current techniques for security protocols analysis, often based on logic, and review the key challenges towards a fully automated verification.

2012 ACM Subject Classification Security and privacy → Formal security models

Keywords and phrases Security protocols, automated deduction, security

Digital Object Identifier 10.4230/LIPIcs.CSL.2020.1

Category Invited Talk

Funding This work has been partially supported by the European Research Council (ERC) under the European Union's Horizon 2020 research (grant agreement No 645865-SPOOC).

1 Description of the talk

Cryptographic protocols aim at securing communications over insecure networks like the Internet. Over the past decades, numerous decision procedures and tools have been developed to automatically analyse the security of protocols. The field has now reached a good level of maturity with efficient techniques for the automatic security analysis of protocols

After an overview of some famous protocols and flaws, we will describe the current techniques for security protocols analysis, often based on logic, and review the key challenges towards a fully automated verification. For example, one well-established tool for analyzing protocols is ProVerif [1], that internally relies on resolution of Horn clauses. ProVerif performs very well in practice but due to this abstraction, it cannot handle protocols with long term states such counters or tables. We have recently realized [2] that these limitations can be overcome with subtle encodings as well as the integration of mature techniques for integers.

Another major challenge is the coverage of privacy properties (e.g. anonymity, untraceability, ballot secrecy) that are typically expressed as equivalence properties. Such properties require novel verification techniques and many tools have been recently developed, such as SPEC [5], DeepSec [3], SatEquiv [4], with different scope and efficiency compromise.

References

1 Bruno Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *14th IEEE Computer Security Foundations Workshop (CSFW-14)*, pages 82–96. IEEE Computer Society, June 2001.

2 Vincent Cheval, Véronique Cortier, and Mathieu Turuani. A little more conversation, a little less action, a lot more satisfaction: Global states in ProVerif. In *Proceedings of the 31st IEEE Computer Security Foundations Symposium (CSF'18)*, pages 344–358, 2018.

28th EACSL Annual Conference on Computer Science Logic (CSL 2020).
Editors: Maribel Fernández and Anca Muscholl; Article No. 1; pp. 1:1–1:2
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

3 Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. The DEEPSEC prover. In *Proceedings of the 30th International Conference on Computer Aided Verification (CAV'18)*. Springer, July 2018.

4 Véronique Cortier, Stéphanie Delaune, and Antoine Dallon. SAT-Equiv: an efficient tool for equivalence properties. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*. IEEE Computer Society Press, August 2017.

5 Jeremy Dawson and Alwen Tiu. Automating open bisimulation checking for the spi-calculus. In *IEEE Computer Security Foundations Symposium (CSF 2010)*, 2010.