Automatic Security Analysis in the Symbolic Model using Tamarin-Prover

Eike Stadtländer
University Bonn

Michael Nüsken
b-it, University Bonn

29th Crypto Day, 6/7 September 2018

Modern mathematical statements and proofs become increasingly difficult to review, that is to verify or falsify. The problem is that for humans the verification of a proof is often more difficult to do than the creation of the proof in the first place. The reasons for that are manifold: complexity, length and the sheer number of new proposed proofs cast time constraints and cognitive strain on whoever is doing the review. Therefore, the human factor seems to be a significant bottle neck and source of error in this process. Indeed there are already some prominent examples of proposed proofs which turned out to be incorrect or intangible to verify due to their length (Opfer, 2011; Blum, 2017; Mochizuki, 2018). This problem is especially relevant for security analysis of cryptographic protocols where properties like confidentiality, authenticity and integrity are formulated as mathematical statements. If a cryptographic protocol is falsely assumed to be secure, severe damage may be the consequence: Leakage of sensitive data, mass surveillance and corporate espionage are possible examples.

Therefore, automatic provers, verifiers and proof assistants are current subjects of research and investigated as a solution to this problem. Such tools automate the process of finding a proof or verifying statements to improve the trustworthiness of stated results. Tamarin-Prover is one of these verifiers which was developed by Schmidt (2012); Meier (2013) in their dissertations at ETH Zurich. This tool operates in a symbolic model which means that cryptographic messages are viewed as terms instead of bit strings and cryptographic primitives are modelled as function symbols which are applicable to terms.

Inspired by related work on TLS 1.3 (Cremers, Horvat, Hoyland, Scott & van der Merwe, 2017), we report on the experiences and insights gained from working towards an automatic analysis of the IPSec protocol using Tamarin-Prover. We focus in particular on the initialization process before the authentication part of the IPSec protocol. Many cryptographic primitives used in IPSec such as generating nonces, Diffie-Hellman exponentiation and signatures are built into Tamarin-Prover and are easy to use. However, others turn out to be more complicated to implement or they induce an idealization, which may reduce the expressiveness of the results. For instance, pseudo-random functions when modelled as function symbols are collision-free. We discuss the strengths and weaknesses of the symbolic model and propose some building blocks for use in automatic security analyses in Tamarin-Prover as an initial step towards a reference implementation of IPSec.

References

Norbert Blum (2017). A Solution of the P versus NP Problem. *CoRR* **abs/1708.03486**. URL `http://arxiv.org/abs/1708.03486`. Withdrawn.

Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott & Thyla van der Merwe (2017). A Comprehensive Symbolic Analysis of TLS 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, 1773–1788. ACM. URL `http://doi.acm.org/10.1145/3133956.3134063`.

Simon Meier (2013). *Advancing automated security protocol verification*. Dissertation, ETH Zürich.

Sinichi Mochizuki (2018). Inter-universal Teichmüller Theory I-IV. URL `http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html`.

Gerhard Opfer (2011). An Analytic Approach to the Collatz 3n+1 Problem. *Hamburger Beiträge zur Angewandten Mathematik* **9**.

Benedikt Schmidt (2012). *Formal analysis of key exchange protocols and physical protocols*. Dissertation, ETH Zürich.

Complete Work: `https://crypto.bit.uni-bonn.de/teaching/18ss/lab/`

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-21