Verification of security protocols: how to check verifiability of voting protocols

Laboratory, institution and university The internship will be located at LORIA (Nancy), University of Lorraine.

Team or project of the Lab Team Pesto at Loria

Name and email address of the advisor Véronique Cortier, veronique.cortier@loria.fr and Vincent Cheval, vincent.cheval@loria.fr

Indemnisation Interns may receive a stipend.

Context. Security protocols are distributed programs that aim at ensuring security properties, such as confidentiality, authentication or anonymity, by the means of cryptography. Such protocols are widely deployed, *e.g.*, for electronic commerce on the Internet, in banking networks, mobile phones and more recently electronic elections.

Formal methods have demonstrated their usefulness when designing and analyzing security protocols. They indeed provide rigorous frameworks and techniques that have allowed to discover new flaws. In particular, ProVerif [1] is a state-of-the-art tool dedicated to the security analysis of protocols. It has been successfully applied to numerous protocols of the literature, providing security proofs or discovering new attacks.

However, ProVerif fails short when it comes to analyse voting protocols. Indeed, voting protocols should achieve vote privacy (no one knows my vote) and verifiability (the result corresponds to the votes cast by voters). This last part requires to *count* the votes, which is beyond ProVerif's capabilities. Instead, current analyses devise sufficient conditions that imply verifiability and that are easier to prove. However, this means that part of the analysis has to be done by hand (on paper).

Objectives of the internship. The goal of the internship is to enhance ProVerif with counting operations. This would allow to analyse voting protocols but also any protocol with counting operations. This work has a practical impact but requires first to develop theoretical results in the area of automated deduction. Namely, ProVerif actually abstracts protocols by Horn clauses. The success of ProVerif lies in the development of a very efficient resolution strategy for Horn clauses.

Very recently, ProVerif has been enhanced with natural numbers together with a + operation [2]. The first goal of the internship is to develop a resolution procedure for clauses that contain a + operation on integers, especially when the + operator is applied between two variables. This is necessary to deal with verifiability in voting. The new resolution procedure will be integrated into ProVerif and tested on voting protocols of the literature.

On a medium-term, the goal is to devise decision procedures for operators with arithmetic properties like the exclusive or and the modular exponentiation. One direction is to split the properties into properties that can be handled directly by ProVerif and properties that require a dedicated resolution procedure.

One interesting aspect of the internship is that it mixes foundational work together with the study of practical protocols (in evoting).

This internship may lead to a PhD thesis on similar topics.

Expected skills. We are looking for candidates with a solid background in Foundations of Computer Science (for example logic, automatic deduction, ...). Some knowledge in security is an asset but is not mandatory. The candidate will learn security aspects during the internship.

Références

[1] Bruno Blanchet. Modeling and verifying security protocols with the applied pi calculus and proverif. *Foundations and Trends in Privacy and Security*, pages 1–135, 2016.

[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.