Formal verification of a messaging protocol

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 takes as input the description of a protocol in the applied-pi calculus, a variat of the pi-calculus with a term algebra. It has been successfully applied to numerous protocols of the literature, providing security proofs or discovering new attacks.

While ProVerif has been successfully applied to complex large-scale protocols (e.g. TLS 1.3), there are still limitations when protocols have a complex datastructure and/or large-term shared memories. The goal of the internship is to evaluate the possibilities of ProVerif on a recent and challenging protocol : Asynchronous Ratcheting Trees (ART) [3], designed for asynchronous group messaging systems. It allows members to securely chat in groups while not being all online and support users to add and leave the group. Interestingly this protocol achieves post-compromise security : the key of a group remains secure even *after* compromission, provided that the attacker does not actively and continously interfere with the protocol.

Objectives of the internship. The goal of the internship is to analyse the ART protocol in ProVerif. While this will start as a « standard » case study, we expect several challenges :

— the ART protocol relies on trees, for which ProVerif offers no support ;
— in the ART protocol, a new group key is built using previously generated keys, hence the protocol requires to model long-term states, for which ProVerif offers few support ;
— the property of post-compromise security is a new property that has never been formalised in ProVerif. This requires to define a new attacker model.

Therefore, the intern will need to develop sound (and clever ;-)) encodings to model such a protocol in the language of ProVerif. Alternatively, the intern may need to enhance ProVerif

with new features, with the help of one of the developpers (Vincent Cheval). In particular, it should be possible to build upon recent developments of ProVerif, that include the treatment of stateful protocols and natural numbers [2].

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

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 *31st IEEE Computer Security Foundations Symposium (CSF'18)*, pages 344–358, 2018.

[3] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican, and Kevin Milner. On ends-to-ends encryption : Asynchronous group messaging with strong security guarantees. In *25th ACM Conference on Computer and Communications Securit (CCS'18)*, 2018.