Verification of equivalence properties in security protocols

Laboratory, institution and university LSV, ENS Cachan and LORIA, Nancy universités. The internship will be located at Nancy or at ENS Cachan depending on the choice of the candidate.

Team or project of the Lab Team SecSI at LSV and team Cassis at Loria.

Name and email address of the advisor Stéphanie Delaune, `delaune@lsv.ens-cachan.fr` and Steve Kremer, `Steve.Kremer@inria.fr`

Indemnisation The internship is supported by the European grant ProSecure (ERC Starting Grant) and the ANR grant VIP (Programme JCJC).

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. As properties need to be ensured, even if the protocol is executed over untrusted networks (such as the Internet), these protocols have shown extremely difficult to get right. Formal methods have shown very useful to detect errors and ensure their correctness.

Many results exist in literature for analyzing reachability properties, such as confidentiality and authentication. Recently, *indistinguishability properties*, received a lot of attention. The notion of indistinguishability is particular useful to model different flavors of anonymity, strong versions of confidentiality and specification of security properties as ideal systems. Indistinguishability is conveniently modelled by process equivalences in extended pi calculi that allow the modeling of cryptography by the means of equational theories.

Objectives of the internship. Recently, a new procedure [CCK12] has been proposed for verifying such equivalence properties. The tool is based on a modeling of the protocols as first order Horn clauses, techniques from rewriting theory and a dedicated resolution procedure. The aim of the internship is to extend the scope of this procedure.

The procedure does currently not support else branches in conditionals. We expect that techniques used in the tool ProVerif [BAF08] could be adapted to enable the tool to reason about protocols that require the use of else branches. This extension may also lead to an implementation in the tool AKisS that implements (in OCaml) the procedure described in [CCK12].

Expected skills. We are looking for candidates with good skills in Foundations of Computer Science (logic, automated deduction, concurrency theory...). Some knowledge in security is an asset but is not mandatory. The candidate will assimilate this knowledge during the internship.

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

References

[BAF08] Bruno Blanchet, Martín Abadi, and Cédric Fournet. Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008.

[CCK12] Rohit Chadha, Ştefan Ciobâcă, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. In Helmut Seidl, editor, *Programming Languages and Systems —Proceedings of the 21th European Symposium on Programming (ESOP'12)*, volume 7211 of *Lecture Notes in Computer Science*, pages 108–127, Tallinn, Estonia, March 2012. Springer. Extended version available at `http://hal.inria.fr/inria-00632564/PDF/equivalence.pdf`.