Verification of security protocols
— reducing the number of agents —

Laboratory, institution and university LSV, ENS Cachan and LORIA, Nancy universités
The internship will be located at Nancy and/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 Véronique Cortier, cortier@loria.fr and Stéphanie Delaune, delaune@lsv.ens-cachan.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.

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. For example, passports are no longer pure paper documents and they contain a chip that stores the personal data of its holder. It has been shown that the *Basic Access Control* protocol used to protect the data stored inside the chip is flawed. It is actually possible to recognize a previously observed passport, potentially tracing passport holders [1].

Many results exist in literature for analyzing reachability properties, such as confidentiality and authentication. Recently, *indistinguishability properties*, received a lot of attention, and several procedures/tools have been developed (*e.g.* ProVerif [2], Apte [3]). The notion of indistinguishability is particularly useful to model different flavors of anonymity, strong versions of confidentiality, and specification of security properties as ideal systems.

Though security protocols are often described in a concise way, the verification problem is difficult due to several sources of unboundedness :

1. the number of agents potentially using the protocol is unbounded, as well as the number of protocol sessions ;
2. the size of messages which can be forged by an attacker is also unbounded.

Actually, even for a simple notion of secrecy, the verification problem is undecidable.

Objectives of the internship. We would like to investigate the unboundedness issue due to the number of agents that are potentially using the protocol. For reachability properties (*e.g.* secrecy, authentication), it has been shown that it is always sufficient to consider a bounded

number of agents (actually 2 agents are sufficient) [4]. More precisely, it has been shown that : *if there is an attack involving n agents then there is an attack involving at most 2 agents.* Such a result has been established in a model based on Horn clauses that allows one to express many security protocols as soon as they rely on standard cryptographic primitives (*e.g.* symmetric and asymnetric encryptions) and they do not use else branch.

The goal of this internship is to develop a similar reduction result for indistinguishability properties. Such a reduction result will be useful to forget about the universal quantifications over agent identifiers and consider finitely many instances of the different protocol roles. This will allow us to get rid of one source of unboundedness when considering the verification problem.

Expected skills. We are looking for candidates with good skills in Foundations of Computer Science (logic, automatic deduction, ...). 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.

Références

[1] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proc. 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 107–121. IEEE Computer Society Press, 2010.

[2] Bruno Blanchet, Martín Abadi, and Cédric Fournet. Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 2008.

[3] Vincent Cheval. Apte : an algorithm for proving trace equivalence. In Erika Ábrahám and JKlaus Havelund, editors, *Proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14)*, Lecture Notes in Computer Science, Grenoble, France, April 2014. Springer. to appear.

[4] Hubert Comon-Lundh and Véronique Cortier. Security properties : two agents are sufficient. In Pierpaolo Degano, editor, *Proceedings of the 12th European Symposium on Programming (ESOP'03)*, volume 2618 of *Lecture Notes in Computer Science*, pages 99–113, Warsaw, Poland, April 2003. Springer.