Verification of security protocols
— decidability results —

Laboratory, institution and university The internship will be located at IRISA (Rennes) and/or LORIA (Nancy) depending on the choice of the candidate.

Team or project of the Lab Team EMSEC at IRISA and team Pesto at Loria

Name and email address of the advisor Stéphanie Delaune, Stephanie.Delaune@irisa.fr and Véronique Cortier, cortier@loria.fr

Indemnisation The internship is supported by the European grant **POPSTAR** (ERC Starting Grant) and the ANR grant **Sequoia**.

Keywords security protocols, formal verification, symbolic model

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 size of messages which can be forged by an attacker is unbounded ;
2. the number of fresh nonces is unbounded, as well as the number of protocol sessions.

Actually, even for a simple notion of secrecy, the verification problem is undecidable. Recenlty, we start investigating the unboundedness issue due to the number of protocol sessions. We obtained the first decidability result regarding indistinguishability expressed through the notion of trace equivalence, for an unbounded number of sessions and unlimited fresh nonces. This result, published at CSF'15 [5], is based on a simplification result published at Concur'14 [4], that reduces the search space for attacks by bounding the size of messages involved in a « minimal » attack. This decidability result applies only to protocols with concatenation and symmetric encryption.

Objectives of the internship. The goal of this internship is to enlarge the scope of the decidability result given in [5] :

1. We would like to consider other standard primitives, e.g. asymmetric encryption, hash function, and signature, and therefore obtain a decidability result for a larger class of protocols. We expect the conditions of type-compliance, as well as acyclicity of dependency graph to be still useful, but some adjustements will be needed to cope with these new primitives. Lastly, since checking these conditions are rather cumbersome, devising a script to perform these steps automatically would be beneficial for this approach. It would allow one to consider more protocols, and therefore to get a better understanding of the scope of our decidable class.
2. The results, described in [4, 5], have been developed for trace equivalence, but it should be possible to derive similar results for more classical security properties (e.g. secrecy, authentication), and therefore give an answer to a problem that has been left often for a long time and that has received some attention also recently [6].

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.

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] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. Typing messages for free in security protocols : the case of equivalence properties. In Paolo Baldan and Daniele Gorla, editors, *Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)*, volume 8704 of *Lecture Notes in Computer Science*, pages 372–386, Rome, Italy, September 2014. Springer.

[5] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. Decidability of trace equivalence for protocols with nonces. In *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF'15)*, pages 170–184, Verona, Italy, July 2015. IEEE Computer Society Press.

[6] Sibylle Fröschle. Leakiness is decidable for well-founded protocols ? In *Proceedings of the 4th Conference on Principles of Security and Trust (POST'15)*, Lecture Notes in Computer Science, London, UK, April 2015. Springer.