Verification of security protocols: are the usual encodings safe when considering equivalence-based properties?

Laboratory, institution and university The internship will be located at IRISA (Rennes).

Team or project of the Lab Team EMSEC at IRISA.

Name and email address of the advisor Stéphanie Delaune, Stephanie.Delaune@irisa.fr

Indemnisation The internship is supported by **POPSTAR** (ERC Starting Grant).

Keywords security protocols, formal verification, symbolic model, privacy-type properties

Context. Security protocols are distributed programs that aim at ensuring security properties, such as confidentiality, authentication or anonymity, by means of cryptographic primitives. 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, in passports — which are no longer pure paper documents but 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. Many results exist in the literature for analyzing reachability properties, such as confidentiality and authentication. Recently, *indistinguishability properties* have received a lot of attention, and several procedures and tools have been developed (*e.g.* ProVerif [1], Tamarin [4], Sat-Equiv [2]). 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.

Each tool has its own specificities and some of them do not offer the possibility to use some cryptographic primitives. In such a case, very often, some « simple » encodings are performed to circumvent the lack of some primitives. Tuples of arbitrary size are usually encoded through nested pairs, randomized encryption and signature schemes are modeled relying on non-randomized schemes with possibly explicit randomness. Another primitive, usually encoded through a simple hash function and pairs, is the keyed-hash message authentication code primitive. In [3], for a large class of security properties (that includes rather standard formulations for secrecy and authenticity properties), it has been shown that security of protocols relying on non-randomized primitives (e.g. encryption and signature) implies security in the randomised setting.

Objectives of the internship. The goal of this internship is to pursue this investigation and to precisely state the conditions under which a particular encoding can be used. We will be particularly interested in equivalence-based security properties (out of scope of the result mentioned above).

To start on this proposal the intern will first study the specific case of static equivalence that corresponds to the verification problem in presence of a passive adversary. In a second phase, the more involved case of trace equivalence (the case of an active adversary) will be considered.

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

Références

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

[2] Véronique Cortier, Stéphanie Delaune, and Antoine Dallon. Sat-equiv : an efficient tool for equivalence properties. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*, pages 481–494. IEEE Computer Society Press, August 2017.

[3] Véronique Cortier, Heinrich Hördegen, and Bogdan Warinschi. Explicit randomness is not necessary when modeling probabilistic encryption. In *Workshop on Information and Computer Security (ICS 2006)*, volume 186 of *Electronic Notes Theoretical Computer Science*, pages 49–65, Timisoara, Romania, September 2007.

[4] S. Meier, B. Schmidt, C. Cremers, and D. Basin. The Tamarin Prover for the Symbolic Analysis of Security Protocols. In *Proc. 25th International Conference on Computer Aided Verification (CAV'13)*, volume 8044 of *LNCS*, pages 696–701. Springer, 2013.