Verification of equivalence-based properties: the case of stateful protocols

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

Team or project of the Lab Team EMSEC at IRISA and team SECSI at LSV

Name and email address of the advisor David Baelde, David.Baelde@lsv.ens-cachan.fr and Stéphanie Delaune, Stephanie.Delaune@irisa.fr

Indemnisation The internship is supported by the European grant **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 [2], Tamarin [5]). 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 (e.g. the size of messages, the number of fresh nonces, the number of protocol sessions, . . .) Actually, even for a simple notion of secrecy, the verification problem is undecidable, and it is even harder when considering indistinguishability properties expressed through the notion of equivalence. We recently investigated a new approach to tackle the challenging problem of unbounded verification for indistinguishability properties. The idea is to design reasonable and checkable conditions on protocols, under which the security property under study holds. This approach has been applied to anonymity and unlinkability property, as described in a publication at S&P'16 [4]. It has been applied on various case studies such as some protocols coming from the e-passport application (BAC and PACE protocols). However, this result suffers from some limitations. In particular, it does not allow one to consider protocols that require to maintain a global, non-monotonic state, e.g., in the form of a database or register.

Objectives of the internship. The goal of this internship is to enlarge the scope of the result presented in [4] in order to be able to analyse indistinguishability properties on stateful protocols. Many modern protocols involve a notion of state. This is the case for instance of many RFID protocols as those presented in [3] and in the survey [6]. Several protocols proposed by the 3rd Generation Partnership Project (3GPP) as a standard for 3G and 4G mobile-network communications are also stateful. For instance, the AKA protocol relies on a state to store a counter across different sessions, and a state is also used in a crucial way to store temporary identifiers (namely TMSI) in the TMSI reallocation procedure. These protocols are supposed to guarantee unlinkability, and are therefore good candidates for guiding the development of our new methodology. Existing results regarding the formal verification of such protocols model states in a very abstract way, considering for instance that the client and the server already (magically) share a fresh name [1] instead of modelling the sequence number mechanism.

To start on this proposal the intern will first have to design new conditions in the spirit of those that have been proposed in [4]. Then, the objective will be to establish a theorem showing that these conditions are indeed sufficient for the purpose of establishing some privacy-type properties (e.g. unlinkability). In parallel, these conditions will have to be confronted to one or two case studies in order to guarantee that they are not too strong in practice. If time allows, it will be possible to implement this technique on top of existing verification tools to automate further case studies. The idea will be to reuse existing verification tools and in no way to design a new verification algorithm from scratch. Therefore, we anticipate that this implementation task will be light and doable during the internship.

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, Loretta Ilaria Mancini, Eike Ritter, and Mark Dermot Ryan. Analysis of privacy in mobile telephony systems. *Int. J. Inf. Sec.*, 16(5) :491–523, 2017.

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

[3] Mayla Bruso, K. Chatzikokolakis, and J. den Hartog. Formal verification of privacy for RFID systems. In *Proceedings of CSF'10*, 2010.

[4] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for verifying privacy-type properties : the unbounded case. In Michael Locasto, Vitaly Shmatikov, and Úlfar Erlingsson, editors, *Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P'16)*, San Jose, California, USA, May 2016. IEEE Computer Society Press.

[5] 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.

[6] Ton van Deursen and Sasa Radomirovic. Attacks on RFID protocols. *IACR Cryptology ePrint Archive*, 2008 :310, 2008.