Verification of security protocols using SAT solvers

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 and Véronique Cortier, cortier@loria.fr

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

Keywords security protocols, formal verification, symbolic model, SAT solvers

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 analysing 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 recognise a previously observed passport, potentially tracing passport holders [1].

Many results exist in literature for analysing reachability properties, such as confidentiality and authentication. Recently, equivalence-based security properties received a lot of attention. This notion is particularly useful to model different flavours of anonymity, strong versions of confidentiality, and specification of security properties as ideal systems. Several tools for checking trace equivalence have been developed. In particular, getting inspiration from an approach originally developed for checking reachability properties and implemented in the tool SATMC [3, 2], we developed a novel algorithm based on graph planning and SAT solving [4]. The resulting implementation, SAT-Equiv, performs quite well and does not suffer from the typical state explosion encountered in other approaches.

`https://projects.lsv.ens-cachan.fr/satequiv/`

Objectives of the internship. The goal of this internship is to enlarge the scope of the algorithm proposed in [4] which is limited to the class of simple processes without else branches. Else branches are often ignored when studying trace properties since most protocols typically abort when a test fails. However, a privacy breach may precisely come from the observation of a failure or from the observation of different error messages. A famous example is the attack mentioned above on the French e-passport. Therefore, it would be interesting to consider protocols with simple else branches, where error messages may be emitted in the else branches.

Another possible extension is to go beyond standard primitives (e.g. encryption, signature, or hash) and to consider more subtle ones such as blind signature or zero-knowledge proofs. From a theoretical point of view, each extension requires to extend the typing result on which this approach is based on. However, a possible approach could be to focus on the development of the verification algorithm itself assuming a typed intruder model.

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] Alessandro Armando, Roberto Carbone, and Luca Compagna. SATMC : A sat-based model checker for security-critical systems. In *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*, pages 31–45, 2014.

[3] Luca Compagna. *SAT-based Model-Checking of Security Protocols*. PhD thesis, Edinburgh University and Genova University.

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