Security analysis of the LoRaWAN protocol using formal symbolic verification tools

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

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. Nowdays several efficient verification tools exist, *e.g.* ProVerif [2], and Tamarin [3]. They can be used to analyse security protocols in a more or less completely automatic way. Of course, this requires to specify the protocol in the input language of the tool. This modelling step has to be done with a lot of care and requires some expertise.

With the arrival of the Internet Of Things (IoT), several communication protocols have been proposed. LoRaWAN is a protocol that aims at securing the Medium Access Control layer of a LoRa network (deployed in more that 50 countries worldwide). The service provided by such a network are numerous. For instance, it allows one to perform various measurements (temperature, humidity, ...), but also to remotely switch on and off an equipment such an alarm, ...

Objectives of the internship. The goal of this internship is to analyse the LoRaWAN security protocol which is a worldwide deployed IoT security protocol. An extensive manual analysis of the version 1.0 (which is the currently deployed version) has been recently done in [1] by G. Avoine and L. Ferreira (members of the EMSEC team), and several weaknesses have been already discovered. To start on this proposal the intern will first study the version 1.0 of the protocol. The aim is to propose a formal model of this protocol in order to retrieve the attacks mentioned above but also to probably discovered new ones. Indeed, relying on automatic verification tools will allow one to analyse more complex scenarios. In a second phase, the version 1.1 of this protocol (which is a bit more complex) will be analysed.

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] Gildas Avoine and Loic Ferreira. Rescuing lorawan 1.0. In *Financial Cryptography and Data Security (FC'18)*, LNCS, 2018.

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

[3] 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.