Verifying timed cybersecurity properties using formal methods

Engel Lefaucheux and Étienne André

1 General information

Supervisors Étienne André, Engel Lefaucheux
Address LORIA, Campus Scientifique - BP 239, 54506 Vandœuvre-lès-Nancy
Email `Etienne.Andre@loria.fr` `Engel.Lefaucheux@loria.fr`
Office B 210 B235
The PhD will be realised in the VeriDis Inria team at Loria (Université de Lorraine, Nancy, France).

2 Context

The pervasiveness of cyber-physical systems is highly increasing, raising many safety and security concerns. For instance, the observation of an user's interactions with a system should not give secret information to an attacker. Take the example of an attacker trying to guess a password by writing down a random input. If the system follows a naive algorithm to check the correctness of the password (*i.e.* checking if every letter is correct one by one and returning $false$ as soon as a wrong letter is detected), the attacker can guess how many of the first letters of their input are correct. In order to deal with this kind of issue, we request systems to be *opaque*, meaning that secret behaviours of the system (the correct password) give the same observations to an attacker as some public behaviours of the system. These observations may include timing delays, energy consumption,...

Formal methods aim at tackling problems such as opacity through the verification of formal properties on a model abstracting the real system. A well-known formal model to reason about timed systems is *timed automata* [1], an extension of finite-state automata with continuous clocks measuring time. Timed automata have been extensively used to verify safety properties, but not so much security properties, with some exceptions (*e.g.* [4,3,2]).

3 Objectives

The objective of the PhD will be to study opacity properties for timed automata, with a strong focus on timing information as was done in [2]. This line of research will be pushed mainly in two directions:

- Parametric systems: parameters can be used in the model to represent a partial knowledge of the real system or some freedom of choice one has during its design. We are then interested in identifying for which values of the parameters the system is opaque.
- Controllable systems: a control of a model is used to restrain some of the system's possible behaviours. This restriction can be aimed for example at making a system more opaque, or at satisfying additional conditions such as energy constraints.

This research has theoretical aspects, as well as some more concrete applications to cybersecurity.

References

1. Rajeev Alur and David L. Dill. A theory of timed automata. *TCS*, 126(2):183–235, April 1994.
2. Étienne André and Jun Sun. Parametric timed model checking for guaranteeing timed opacity. In Yu-Fang Chen, Chih-Hong Cheng, and Javier Esparza, editors, *ATVA*, volume 11781 of *LNCS*, pages 115–130. Springer, 2019.
3. Gilles Benattar, Franck Cassez, Didier Lime, and Olivier H. Roux. Control and synthesis of non-interferent timed systems. *International Journal of Control*, 88(2):217–236, 2015.
4. Franck Cassez. The dark side of timed opacity. In Jong Hyuk Park, Hsiao-Hwa Chen, Mohammed Atiquzzaman, Changhoon Lee, Tai-Hoon Kim, and Sang-Soo Yeo, editors, *ISA*, volume 5576 of *LNCS*, pages 21–30. Springer, 2009.