PhD thesis proposal

Verifying timed cybersecurity properties using formal methods

Supervisor: Étienne André (full professor, Université Sorbonne Paris Nord)
Co-supervisor: Engel Lefaucheux (Inria, LORIA)
Email: etienne.andre@univ-paris13.fr
engel.lefaucheux@inria.fr
Laboratory: LIPN, CNRS UMR 7030, Université Sorbonne Paris Nord
Team: LoVe (Logic and Verification)

Context

The pervasiveness of cyber-physical systems is highly increasing, raising many safety and security concerns. For instance, the observation of a 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 behaviors of the system (the correct password) give the same observations to an attacker as some public behaviors of the system. These observations may include timing delays, energy consumption, etc.

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* [AD94], 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., [Cas09; Ben+15; WZ18; WZA18; Amm+21; And+22; KSA22; ALM23]).

Subject

The objective of the thesis will be to study opacity properties for timed automata, with a strong focus on timing information as was done in [And+22]. 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 behaviors. This restriction can be aimed for example at making a system more opaque, or at satisfying additional conditions such as energy constraints.

A focus on *expiring* opacity can also be made [Amm+21; ALM23].

The algorithms developed during the thesis shall be implemented in some software, in order to be validated against benchmarks.

Keywords

Formal methods, cybersecurity, opacity

Conditions

Highly motivated applicants are being sought. The thesis will take place at LIPN (Laboratoire d'Informatique de Paris Nord) within Université Sorbonne Paris Nord. LIPN is an internationally recognized research laboratory comprising over 150 scientists.

References

[AD94] Rajeev Alur and David L. Dill. "A theory of timed automata". In: *TCS* 126.2 (Apr. 1994), pp. 183–235. DOI: 10.1016/0304-3975(94)90010-8.

[ALM23] Étienne André, Engel Lefaucheux, and Dylan Marinho. "Expiring opacity problems in parametric timed automata". In: *ICECCS* (June 14–16, 2023). Ed. by Yamine Ait-Ameur and Ferhat Khendek. Toulouse, France, 2023, pp. 89–98. DOI: 10.1109/ICECCS59891.2023.00020.

[Amm+21] Ikhlass Ammar, Yamen El Touati, Moez Yeddes, and John Mullins. "Bounded opacity for timed systems". In: *Journal of Information Security and Applications* 61 (Sept. 2021), pp. 1–13. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2021.102926.

[And+22] Étienne André, Didier Lime, Dylan Marinho, and Jun Sun. "Guaranteeing timed opacity using parametric timed model checking". In: *ACM Transactions on Software Engineering and Methodology* 31.4 (Oct. 2022), pp. 1–36. DOI: 10.1145/3502851.

[Ben+15] Gilles Benattar, Franck Cassez, Didier Lime, and Olivier H. Roux. "Control and synthesis of non-interferent timed systems". In: *International Journal of Control* 88.2 (2015), pp. 217–236. DOI: 10.1080/00207179.2014.944356.

[Cas09] Franck Cassez. "The Dark Side of Timed Opacity". In: *ISA* (June 25–27, 2009). Ed. by Jong Hyuk Park, Hsiao-Hwa Chen, Mohammed Atiquzzaman, Changhoon Lee, Tai-Hoon Kim, and Sang-Soo Yeo. Vol. 5576. LNCS. Seoul, Korea: Springer, 2009, pp. 21–30. DOI: 10.1007/978-3-642-02617-1_3.

LIPN • Institut Galilée • Université Sorbonne Paris Nord • 93 430 Villetaneuse, France
Etienne.Andre@univ-paris13.fr
https://lipn.univ-paris13.fr/~andre/

[KSA22] Aqsa Kashaf, Vyas Sekar, and Yuvraj Agarwal. “Protecting Smart Homes from Unintended Application Actions”. In: *ICCPS* (May 4–Apr. 6, 2022). Milano, Italy: IEEE, 2022, pp. 270–281. DOI: 10.1109/ICCPS54341.2022.00031.

[WZ18] Lingtai Wang and Naijun Zhan. “Decidability of the Initial-State Opacity of Real-Time Automata”. In: *Symposium on Real-Time and Hybrid Systems - Essays Dedicated to Professor Chaochen Zhou on the Occasion of His 80th Birthday*. Ed. by Cliff B. Jones, Ji Wang, and Naijun Zhan. Vol. 11180. Lecture Notes in Computer Science. Springer, 2018, pp. 44–60. DOI: 10.1007/978-3-030-01461-2_3.

[WZA18] Lingtai Wang, Naijun Zhan, and Jie An. “The Opacity of Real-Time Automata”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37.11 (2018), pp. 2845–2856. DOI: 10.1109/TCAD.2018.2857363.

LIPN • Institut Galilée • Université Sorbonne Paris Nord • 93 430 Villetaneuse, France
Etienne.Andre@univ-paris13.fr
https://lipn.univ-paris13.fr/~andre/