PhD thesis proposal

Verifying timed cybersecurity properties in the presence of energy constraints

Supervisor: Laure Petrucci and Étienne André (both full professor, Université Sorbonne Paris Nord)
Email: `first.last@univ-paris13.fr`
Laboratory: LIPN, CNRS UMR 7030, Université Sorbonne Paris Nord
Team: SAFER

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; ADL24]).

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]; in addition, the presence of energy constraints will be interesting, to model energy consumption, or costs [Beh+01; Lar+01; ALP04; Bri+22]. That is, the main challenge will be to study the decidability of the following problem: given a system modeled by a priced/cost/energy timed automaton, can the attacker deduce private information by only looking at the execution time and/or the energy consumption?

Different directions will be envisioned during the thesis:

1. Decidability: studying decidability of various notions of opacity with respect to energy.
2. Expiring opacity: studying decidability of *expiring* opacity [Amm+21; ALM23], i.e., when the secret has an expiration date.
3. Parametric verification: parameters (encoding either timing uncertainty or energy uncertainty [AHV93; Bac+21]) 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.
4. Depending on the findings, the algorithms developed during the thesis might be implemented in some open-source software, in order to be validated against benchmarks. A typical software candidate is of course IMITATOR, developed by Étienne André and Laure Petrucci [And21; NPP18].

Keywords

Formal methods, cybersecurity, opacity, energy

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.

[ADL24] Étienne André, Sarah Dépernet, and Engel Lefaucheux. "The Bright Side of Timed Opacity". In: *ICFEM* (Dec. 2–6, 2024). Ed. by Kazuhiro Ogata, Meng Sun, and Dominique Méry. Vol. 15394. Lecture Notes in Computer Science. Hiroshima, Japan: Springer, Dec. 2024, pp. 51–69. DOI: 10.1007/978-981-96-0617-7_4.

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. "Parametric real-time reasoning". In: *STOC* (May 16–18, 1993). Ed. by S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal. San Diego, California, USA: ACM, 1993, pp. 592–601. DOI: 10.1145/167088.167242.

[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.

[ALP04] Rajeev Alur, Salvatore La Torre, and George J. Pappas. "Optimal paths in weighted timed automata". In: *Theoretical Computer Science* 318.3 (2004), pp. 297–322. DOI: 10.1016/j.tcs.2003.10.038.

[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.

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

[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.

[And21] Étienne André. "IMITATOR 3: Synthesis of timing parameters beyond decidability". In: *CAV* (July 18–23, 2021). Ed. by Rustan Leino and Alexandra Silva. Vol. 12759. Lecture Notes in Computer Science. virtual: Springer, 2021, pp. 1–14. DOI: 10.1007/978-3-030-81685-8_26.

[Bac+21] Giovanni Bacci, Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, Nicolas Markey, and Pierre-Alain Reynier. "Optimal and robust controller synthesis using energy timed automata with uncertainty". In: *Formal Aspects of Computing* 33.1 (2021), pp. 3–25. DOI: 10.1007/s00165-020-00521-4.

[Beh+01] Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Kim Guldstrand Larsen, Paul Pettersson, Judi Romijn, and Frits W. Vaandrager. "Minimum-Cost Reachability for Priced Timed Automata". In: *HSCC* (Mar. 28–30, 2001). Ed. by Maria Domenica Di Benedetto and Alberto L. Sangiovanni-Vincentelli. Vol. 2034. Lecture Notes in Computer Science. Rome, Italy: Springer, 2001, pp. 147–161. ISBN: 3-540-41866-0. DOI: 10.1007/3-540-45351-2_15.

[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.

[Bri+22] Thomas Brihaye, Gilles Geeraerts, Axel Haddad, Engel Lefaucheux, and Benjamin Monmege. "One-Clock Priced Timed Games with Negative Weights". In: *Logical Methods in Computer Science* 18.3 (2022). DOI: 10.46298/lmcs-18(3:17)2022.

[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.

[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.

[Lar+01] Kim Guldstrand Larsen, Gerd Behrmann, Ed Brinksma, Ansgar Fehnker, Thomas Hune, Paul Pettersson, and Judi Romijn. "As Cheap as Possible: Efficient Cost-Optimal Reachability for Priced Timed Automata". In: *CAV* (July 18–22, 2001). Ed. by Gérard Berry, Hubert Comon, and Alain Finkel. Vol. 2102. Lecture Notes in Computer Science. Paris, France: Springer, 2001, pp. 493–505. DOI: 10.1007/3-540-44585-4_47.

[NPP18] Hoang Gia Nguyen, Laure Petrucci, and Jaco van de Pol. "Layered and Collecting NDFS with Subsumption for Parametric Timed Automata". In: *ICECCS* (Dec. 12–14, 2018). Ed. by Anthony Widjaja Lin and Jun Sun. Melbourne, Australia: IEEE Computer Society, Dec. 2018, pp. 1–9. DOI: 10.1109/ICECCS2018.2018.00009.

[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.

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

[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/