Post-doc Proposal

Detecting timing attacks using formal methods

PI: Étienne André
Email: postdoc.promis@lipn13.fr
Laboratory: LORIA, Université de Lorraine, CNRS, Inria, Nancy, France
Team: MOSEL + VeriDis

1 Context

The Spectre vulnerability in modern processors has been reported in 2018. The key insight is that speculative execution in processors can be misused to access secrets speculatively. Subsequently even though the speculatively executed states are squashed, the secret may linger in micro-architectural data structures such as cache, and hence can be potentially accessed by an attacker via side channels.

The Spectre vulnerability is merely one example of a family of vulnerabilities which could lead to the so-called side channel attacks. In general, side channel attacks use information which is leaked through certain side channel (*e.g.* time, energy (see Fig. 1), cache state and sound wave) in order to reveal system secrets. For instance, a timing side channel attack simply observes variations in how long it takes to perform certain operations, and determines the value of certain secret (*e.g.* an encryption key) in the system. Such attacks involve analysis of timing measurements and have been demonstrated to be effective in attacking a range of systems.

2 Post-doc subject

Timing side channel attacks consist in retrieving some secret by taking advantage of some *timing* information—typically the execution time of a program, or some subfunction. Timing side channel attacks are known to be challenging to detect and mitigate. The goal will be to propose a formal approach so as to verify whether a given system model is free from timing side channel attacks.

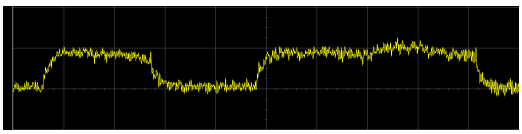

Figure 1: An example of power attack (author: Audriusa, license GNU-GPL)

To this end, the system would be modeled using a formalism close to the popular model of timed automata [AD94], an extension of finite-state automata with real-valued *clocks*. Then, new methods should be proposed to detect whether a given system is free from timing side channel attack or not.

A focus will particularly be made on the case when some of the timing parameters can be configured (*e.g.* using some `Wait` statement in a program). The formalism can then become *parametric timed automata* [AHV93], and the ultimate goal will be to *synthesize* some of these parameter valuations guaranteeing that the system is free from timing side channel attacks.

The work would contain a theoretical part, but also an implementation part; this implementation may reuse the parametric timed model checker IMITATOR [And+12].

As a more open research direction, translating real-world programs to parametric timed automata (or similar formalisms) using only the relevant timing information would also be a possible research perspective, depending on the applicant's wish.

Related works Opacity or non-interference in timed automata was studied in several works, notably [Bar+02; GMR07; Cas09; Ben+15; AS19]. These works all suffer from some limitations and, with the exception of [AS19], were not implemented in dedicated software toolkits.

3 Framework

3.1 Scientific framework: ANR-NRF ProMiS

This post-doc fellowship is in the framework of the French-Singaporean ANR-NRF project *ProMiS* (Provable Mitigation of Side Channel through Parametric Verification) 2020-2023. This project involves LORIA (Nancy, France), LS2N (Nantes, France), Singapore Management University and Singapore University of Technology of Design (Singapore). While the position is based in Nancy, frequent interactions will be conducted with the other partners of the project; this may include short- or medium-length visits to Nantes and/or Singapore partners.

3.2 Location: Nancy

The post-doc position will take place at LORIA (Laboratoire lorrain de recherche en informatique et ses applications) at Université de Lorraine, Nancy. LORIA is an internationally recognized research laboratory comprising over 400 scientists from 48 nationalities.

Université de Lorraine is a dynamic university in the beautiful city of Nancy, 1h30 from Paris by TGV (high-speed train); Nancy is a human-sized city featuring a high quality of life, a UNESCO-world-heritage city center, and very affordable living costs.

Figure 2: Place Stanislas (author: Nicolas Cornet, license CC-by-sa)

4 Keywords

Formal methods, cybersecurity, verification, opacity, cryptography, program analysis

Conditions

Highly motivated applicants with an excellent research record are being sought. Expertise is at least one of the aforementioned keywords is required. The fellowship is research-only: no teaching, no administrative paperwork.

The post-doc fellowship is for 12 months, and can possibly be extended for another 12 months. The successful applicant can start anytime, with a high preference for a starting date before 1st October 2020.

Approximate remuneration: 2,400 € net / month (social security and retirement scheme are also provided). Funding for traveling, notably to Singapore, is also provided.

Application

Applications can be made by email, using a fully developed CV, a complete research record, possible names of referees, and any relevant additional information.

Contact: `postdoc.promis@lipn13.fr`

References

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

[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, United States: ACM, 1993, pp. 592–601. ISBN: 0-89791-591-7. DOI: 10.1145/167088.167242.

[And+12] Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat. “IMITATOR 2.5: A Tool for Analyzing Robustness in Scheduling Problems”. In: *FM*. (Aug. 27–31, 2012). Ed. by Dimitra Giannakopoulou and Dominique Méry. Vol. 7436. Lecture Notes in Computer Science. Paris, France: Springer, Aug. 2012, pp. 33–36. DOI: 10.1007/978-3-642-32759-9_6.

[AS19] Étienne André and Jun Sun. “Parametric Timed Model Checking for Guaranteeing Timed Opacity”. In: *ATVA*. (Oct. 28–31, 2019). Ed. by Yu-Fang Chen, Chih-Hong Cheng, and Javier Esparza. Vol. 11781. Lecture Notes in Computer Science. Taipei, Taiwan: Springer, 2019, pp. 115–130. DOI: 10.1007/978-3-030-31784-3_7.

[Bar+02] Roberto Barbuti, Nicoletta De Francesco, Antonella Santone, and Luca Tesei. “A Notion of Non-Interference for Timed Automata”. In: *Fundamenta Informaticae* 51.1-2 (2002), pp. 1–11.

[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. Lecture Notes in Computer Science. Seoul, Korea: Springer, 2009, pp. 21–30. DOI: 10.1007/978-3-642-02617-1_3.

[GMR07] Guillaume Gardey, John Mullins, and Olivier H. Roux. “Non-Interference Control Synthesis for Security Timed Automata”. In: *Electronic Notes in Theoretical Computer Science* 180.1 (2007), pp. 35–53. DOI: 10.1016/j.entcs.2005.05.046.

Version: January 15, 2020