Evaluating web browser robustness against micro-architectural attacks

September 2018

Advisor: Clémentine Maurice (clementine.maurice@irisa.fr, https://cmaurice.fr/)
Lab: IRISA, Rennes, France
Domain: Security
Group: EMSEC (https://www.irisa.fr/emsec/)
Keywords: side-channel attacks, web browser, micro-architecture, countermeasures

Topic: Hardware is often considered as an abstract layer that behaves correctly, just executing instructions and outputing a result. However, the internal state of the hardware leaks information about the programs that are executing, paving the way for covert channels or side-channel attacks. Recent work showed that these attacks can be performed through websites using JavaScript, exploiting micro-architectural components such as the cache [OKSK15, LGS+17] and optimization techniques such as speculative execution in Spectre attacks [KHF+19]. All these attacks have in common the fact that they require a very high-resolution timer.

In reaction, web browser vendors have deployed countermeasures such as reducing timer resolution, however, this countermeasure has been showed to not be effective [SMGM17]. The different attacks each prompted a reaction from the browser vendors who had to adapt rapidly in light of the severity of the vulnerabilities[1]. Different features, such as the `performance.now()` method, and the `SharedArrayBuffer` object are therefore changing rapidly, being enabled and disabled between different browser versions. No systematic evaluation has been performed in order to assess the vulnerability of the different browsers to each class of attack.

During this internship, the student will:

- Implement some known attacks.
- Propose metrics to assess the robustness of browsers against these attacks, and implement them. This can take the form of a security benchmark suite in JavaScript.
- Perform a retrospective longitudinal study on the major browsers on current (and past, when available) versions to evaluate the evolution of the different countermeasures in place.
- Propose new countermeasures in the cases where the ones in place are not efficient.

About the lab: IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires), founded in 1975, is a mixed research center for IT, image, signal processing, and robotics, located in Rennes, France. The institute hosts 750 researchers belonging to 40 teams, and is funded by 8 entities,

[1] https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

namely CentraleSupélec, CNRS, ENS Rennes, Inria, INSA Rennes, Institut Mines-Télécom, University of Southern Brittany (UBS), University of Rennes 1.

References

[KHF+19] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *S&P*, 2019. to appear.

[LGS+17] Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard. Practical keystroke timing attacks in sandboxed javascript. In *ESORICS*, 2017.

[OKSK15] Yossef Oren, Vasileios P. Kemerlis, Simha Sethumadhavan, and Angelos D. Keromytis. The spy in the sandbox: Practical cache attacks in javascript and their implications. In *CCS*, 2015.

[SMGM17] Michael Schwarz, Clémentine Maurice, Daniel Gruss, and Stefan Mangard. Fantastic timers and where to find them: High-resolution microarchitectural attacks in javascript. In *FC*, 2017.