Thomas Rokicki
Postdoctoral application

Paris, France• thomas.rokicki2805@orange.fr • +33 (0) 6 16 63 47 48

PROFESSIONAL EXPERIENCE

Univ Rennes, CNRS, IRISA **Rennes, France**
Ph.D. Candidate **2019-2022**
Microarchitectural Side Channels in Web Browsers

Ph.D. Thesis under the supervision of Clémentine Maurice and Gildas Avoine. My thesis focused on offensive security on micro-architectural side channels, especially in web-based environments.

- Systematization of timing attacks in Web Browsers. Our goal was to provide a clear view of the threats and requirements of such attacks - including microarchitectural side channels, as well as concretely evaluating browsers' countermeasures.
- Implementation of new side channels in JavaScript's sandbox. In particular, we focused on port contention, which brings contention-based side channels to browsers. We also focused on changing the threat models of existing attacks to better suit browsers' constraints, e.g. making them independent of SMT.
- Identification of hardware features from the sandbox. We focused on hardware fingerprinting, as it grants extensive stability compared to more volatile software attributes. This type of application, specific to browser-based environments, required us to adapt existing side channels to be fast and reliable.
- Development of systematic analysis tools. For most of my work, I developed automated tools to enhance and promote portability on different hardware and browsers.

EDUCATION

Insa Rennes **Rennes, France**
Ph.D. Candidate **2019-2022**

- My Research focused on offensive microarchitectural security in web browsers.
- Under the supervision of Clémentine Maurice and Gildas Avoine.
- I Defended in November 2022 with Jan Reineke and Billy Brumley as reporters and Veelasha Moonsamy and Walter Rudametkin as members of the jury.

IMT Atlantique **Rennes/Brest, France**
Cybersecurity Master's Degree **2016-2019**

Generalistic formation in cybersecurity, with a strong focus on network and web security.

Universidad de la Republica (UdelaR) **Montevideo, Uruguay**
Academic semester **2018**

Exchange semester to study in the cybersecurity track. Focus on system security and embedded devices.

Lycée Saint Louis **Paris, France**
Preparatory classes **2014-2016**

Preparatory classes specialized in mathematics, physics, and computer science.

SKILLS

Technologies:

- JavaScript / WebAssembly / WebGPU
- C / x86 Assembly
- Python

Organization:

- Managed Team's seminary
- Organized practical classes for Masters's degree courses.

Spoken Languages:

- French - Native language
- English - Full professional proficiency
- Spanish - Limited Working proficiency

PUBLICATIONS

SoK: In Search Of Lost Time: A Review Of JavaScript Timers In Browsers **EuroS&P21**

Thomas Rokicki, Clémentine Maurice, Pierre Laperdrix

Timing attacks have been greatly explored in web browsers. They include microarchitectural or software side channels as well as transient execution attacks. As browsers are constantly evolving software, it is hard to evaluate their attack surface. In this paper, we provide a clear picture of the threats posed by timing attacks.

- We define an exhaustive classification of timing attacks in the browsers based on their prerequisites. We isolated 4 families of attacks, ranging from low-level microarchitectural side channels to attacks relying entirely on browser resources.
- Based on this classification, we classify existing and theoretical countermeasures. These defenses have been proposed, by academics and browser vendors, at different levels. In particular, we observed a paradigm shift from timing-based countermeasures to isolation-based solutions.
- We developed an automated framework to evaluate the efficiency of timing-based countermeasures. With a longitudinal study on more than 100 versions of Chrome and Firefox, we demonstrate how later versions of browsers were more exposed to timing attacks in general than older versions, due to less restrictive timers.

Article: https://hal.inria.fr/hal-03215569/document Code: http://github.com/thomasrokicki/in-search-of-lost-time

Port Contention Goes Portable: Port Contention Side Channels in the Browser **AsiaCCS22**

Thomas Rokicki, Clémentine Maurice, Marina Botvinnik, Yossi Oren

In this paper, we present the first port contention side channel running entirely in a web browser, despite a highly challenging environment.

- We introduce the first implementation of port-contention side channels inside of the JavaScript sandbox. By repeatedly calling specific WebAssembly instructions, we use CPU ports as bottlenecks to leak information on other processes' port usage.
- We propose an automated black-box framework to evaluate the port usage of WebAssembly instructions. By executing arbitrary pairs of instructions in different processes on the same physical core and measuring their execution times, we can determine their port usage.
- We demonstrate the threat posed by our new side channels by implementing a side-channel artificial example. Its spatial resolution is on par with the best attacks of the state of the art.
- We implemented a covert channel using port contention as a physical layer, allowing an attacker to exchange information outside of the sandbox with a bandwidth of 200 bps.

Article: https://inria.hal.science/hal-03708833/document Code: https://github.com/MIAOUS-group/web-port-contention

Port Contention Without SMT **Esorics 2022**

Thomas Rokicki, Clémentine Maurice, Michael Schwarz

Port contention side channels rely heavily on SMT or HyperThreading. This prevents the implementation of these attacks on systems without SMT (RedHat OS, ChromeOS) or virtualized environments where the attacker cannot control the cores.

- We introduced a new side-channel, sequential port contention, where the attacker can create contention even without SMT. Our side channel works both in native and web environments.
- We developed our black-box framework to automatically detect sequences of instructions triggering sequential port contention.
- We used this side channel to automatically detect the CPU generation of the victim from the JavaScript sandbox with 96% accuracy.

Article: https://cmaurice.fr/pdf/esorics22_rokicki.pdf Code: https://github.com/MIAOUS-group/port-contention-without-smt

The Finger in the Power: How to Fingerprint PCs by Monitoring their Power Consumption **DIMVA 2023**

Marina Botvinnik, Tomer Laor, Thomas Rokicki, Clémentine Maurice, Yossi Oren

Power analysis has long been used to tell apart different instructions running on the same machine. In this work, we introduce a power-analysis-based fingerprinting technique.

- We show that it is also possible to use power consumption to tell apart different machines running the same instructions, even if these machines have entirely identical hardware and software configurations.
- We collect an extended dataset of power consumption traces from 291 desktop and server systems, spanning multiple processor generations and vendors (Intel and AMD), and use the differences in power consumption to create fingerprints. We also developed a proof-of-concept evaluation in WebAssembly, showing our method can still be applied without the need for native instructions.
- Due to restrictions on power measurement, our method is only applicable with ring-0 access, reserving it for defense-only applications.

Article: https://orenlab.sise.bgu.ac.il/p/FingerInThePower.pdf Code: https://github.com/FingerInThePower/Finger_In_The_Power

TEACHING

Microarchitectural Security — **2021 and 2022**
Insa Rennes — **Master's level**
Created and managed practical classes and student projects on side channels. The labs were introducing students to primary microarchitectural side channels (Prime+Probe, Flush+Reload) and other microarchitectural attacks (Rowhammer, Spectre). In a project, the students had to implement a Flush+Reload-based covert channel.

Network Security — **2022**
Université De Rennes 1 — **Master's level**
Practical classes on the introduction to network and network security. I helped on designing the final exam.

Introduction to Programming — **2019,2020**
Université De Rennes 1 — **Bachelor's level**
Practical classes on the fundamentals of programming (variables, loops, arrays) in Java for students who never programmed before. I also managed students on a programming project, generally consisting of developing a simple game.

Functional Programming — **2019**
Université De Rennes 1 — **Bachelor's level**
Tutorials and labs in Scala to introduce second-year students to functional programming.

MANAGEMENT

Leo Cosseron — **2021**
ENS Rennes, Master's degree (M1) — **6 Months Internship**

Julius Wenzel — **2020**
Insa Rennes — **3 Months Internship**

PRESENTATIONS

Ph.D. Defense — **18/11/2022**
Microarchitectural side channels in Web Browsers: Applications to Security and Privacy — **45 minutes + 2 hours questions**
Video: https://www.youtube.com/watch?v=C55s7kY_2eY

Esorics 2022 — **28/09/2022**
CPU Port Contention Without SMT — **15 minutes + questions**

AsiaCCS 2022 — **02/06/2022**
Port Contention Goes Portable — **15 minutes + questions**
Video: https://dl.acm.org/doi/10.1145/3488932.3517411

SoSySec Seminar (Irisa's security seminar) — **2022**
Port Contention Goes Portable — **45 Minutes + questions**
Video: https://videos-rennes.inria.fr/video/UksGngEVE

EuroS&P 2021 — **09/09/2021**
In Search of Lost Time: A Review of JavaScript Timers in Browsers — **10 Minutes**
Video: https://www.youtube.com/watch?v=ivZInlRXS-k

Pass The Salt Conference — **05/07/2021**
In Search of Lost Time: A Review of JavaScript Timers in Browsers — **35 Minutes**
Video: https://passthesalt.ubicast.tv/videos/2021-in-search-of-lost-time-a-review-of-javascript-timers-in-browsers/