Ph.D proposal

Side Channel Analysis for Vulnerabilities Concerning Post-quantum Cryptography

Department: **COMELEC – Telecom Paris**
Director: **Luodvic Apvrille (COMELEC)**
Supervisor: **Maria Mushtaq (COMELEC)**

1. Context and motivation

Security failure in computing systems has become one of today's biggest concerns. The primary threat is that modern computing architectures –from computational optimizations to storage elements and interfaces, from end-user applications to the operating system & hypervisor, and from microarchitecture to underlying hardware– may hide unexpected vulnerabilities. This concern is gaining further momentum with the spectacular aggressiveness of Spectre, Meltdown, and ZombieLoad vulnerabilities. They demonstrate that even hardware, which is often considered an abstract layer that behaves correctly by executing instructions and giving a logically correct output, is leaking critical information as a side effect of software implementation and execution. Even worse, the many undocumented parts of modern architectures open doors for yet undescribed side-channel attacks (SCAs). There are four established categories of side-channel attacks at the microarchitectural level. For instance, software on- software attacks could be an untrusted operating system attacking software that is being protected [1], [2]. A software-on-hardware attack could be untrusted software using cache side-channel attacks to learn secret information from a processor cache's operation [3], [4]. A hardware-on-software attack could be an untrusted memory controller trying to extract information from DRAM memory Rowhammer [5], [6]. A hardware-on-hardware attack could be an untrusted peripheral trying to disable the memory encryption engine [7]. The vulnerability assessment will not be performed for components inside the software or hardware Trusted Computing Base (TCB) as they are never assumed to be sources of attack, and, by definition, they are trusted with ensuring protection for the system.

From the software point of view, hardware is often considered an abstract layer that behaves correctly and can safely keep secret information. This assumption is no longer true when considering the systems relying on connected objects like IoT (Internet of Things) or embedded military equipment that could be physically accessible and analyzed by a potential adversary. Indeed, software execution on the underlying computing hardware can be the target of physical attacks, like side-channels analysis or fault injection attacks. They open doors for critical vulnerabilities and cyber-physical attacks that can impact the microarchitecture in terms of security and privacy. This project aims to propose a framework for the instrumentation such as monitoring, detection, and mitigation of different types of attacks using Artificial Intelligence, both on software and hardware. The implication of this framework will be relative to the assessment and mitigation of cyber threats happening in daily life IoT products which involve computing in general life, i.e., home automation, mobiles, biometric security systems, smart cards, etc.

2. Scope of the Project:

This PhD thesis argues in favor of assessment-based protection. Automated assessment will be our first-line-of-defense against cache and covert timing SCAs. It will help apply mitigation only after a successful automated attack assessment at runtime. This will reduce the all-weather performance degradation of mitigation approaches. The scope of work is limited to microarchitecture analysis and solutions. This Ph.D. is focused on systematizing the discovery of micro architectural weakness in modern architectures, at design-time as well as at runtime, and automatically detecting vulnerabilities both in the software and hardware by training machine and deep learning models [8, 9]. Manual discovery of an attack is not viable when thousands of attack execution traces and attack behaviors are involved [10].

3. Project Description:

The position is funded under BPI X7PQC project with industrial partners of SECURE-IC and HENSOLD and academic partners of Telecom Paris and XLIM. It gives a wonderful playground to the candidate to know the key players of cybersecurity in France and integrate into project meetings, discussions, and seminars to collaborate at a full scale.

Besides the project, the selected candidate will be able to integrate fully with the SSH team, LTCI Laboratory of Telecom Paris, which holds an international reputation for the safety and security of embedded systems. The candidate will be able to integrate and collaborate with other Ph.D. and Postdoc candidates within the team on aligned topics. Furthermore, you may avail the opportunity to teach and assist with your advisors with added salary benefits.

Contact

Director: Luodvic Apvrille: ludovic.apvrille@telecomparis.fr

Supervisor: Maria Mushtaq: maria.mushtaq@telecoinfrm-paris.fr

References:

[1] 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 40th IEEE Symposium on Security and Privacy (S&P'19), 2019.

[2] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading Kernel Memory from User Space. In 27th USENIX Security Symposium (USENIX Security 18), 2018.

[3] Berk GÅNulmezo˘glu, Mehmet Sinan ˙Inci, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar. A faster and more realistic flush+reload attack on AES. In Revised Selected Papers of the 6th International Workshop on Constructive Side-Channel Analysis and Secure Design - Volume 9064, COSADE 2015, pages 111–126, New York, NY, USA, 2015. Springer-Verlag New York, Inc.

[4] Daniel Gruss, ClÅLementine Maurice, Klaus Wagner, and Stefan Mangard. Flush+ flush: a fast and stealthy cache attack. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 279–299. Springer, 2016.

[5] Daniel Gruss, ClÅLementine Maurice, and Stefan Mangard. Rowhammer. js: A remote software-induced fault attack in javascript. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 300–321. Springer, 2016.

[6] Andrew Kwong, Daniel Genkin, Daniel Gruss, and Yuval Yarom. Rambleed: Reading bits in memory without accessing them.

[7] Ilya Kizhvatov. Side channel analysis of avr xmega crypto engine. In Proceedings of the 4th Workshop on Embedded Systems Security, page 8. ACM, 2009.

[8] Mushtaq et al., WHISPER: A tool for runtime detection of side-channel attacks," IEEE Access, 2020.

[9] M. Mushtaq et al., "Machine Learning for Security: The Case of Side channel Attack Detection at Run-Time, InICECS, 2018.

[10] Akram, et al., Meet the Sherlock Holmes' of Side Channel Leakage: A Survey of Cache SCA Detection Techniques, IEEE Access, 2020.

[11] Mushtaq et al., Winter is here! A decade of cache-based side-channel attacks, detection & mitigation for RSA, Elsevier Information Systems, 2020.

[12] France et al., Vulnera bility assessment of the rowhammer attack using machine learning and the gem5 simulator-work in progress," ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2021.

[13] Mushtaq et al., WHISPER: A tool for runtime detection of side-channel attacks," IEEE Access, 2020.

[14] Transit-Guard: An OS-based Defense Mechanism Against Transient Execution Attacks. Maria Mushtaq; David Novo; Florent Bruguier; Pascal Benoit; Muhammad Khurram Bhatti. IEEE European Test Symposium (ETS), 2021.

[15] The Kingsguard OS-level mitigation against cache side-channel attacks using runtime detection. Maria Mushtaq, Muhammad Muneeb Yousaf, Muhammad Khurram Bhatti, Vianney Lapotre & Guy Gogniat. Annals of Telecommunications (2022).