KU LEUVEN

FACULTY OF ENGINEERING SCIENCE

Jo Van Bulck

Department	Computer Science
PhD defence	14 September 2020
Supervisor	Frank Piessens
Funding	FWO
Website	https://jovanbulck.github.io/
E-mail	jo.vanbulck@cs.kuleuven.be

Microarchitectural Side-Channel Attacks for Privileged Software Adversaries

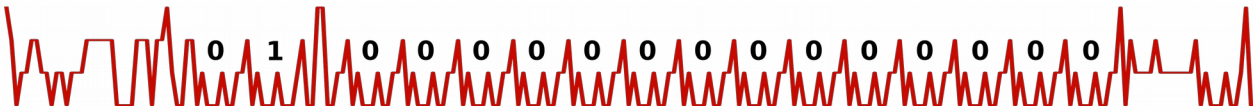


Figure 1: Interrupt latency trace reveals enclave-private memory accesses in secret-dependent code paths.

Introduction / Objective

Recent developments on hardware-based trusted execution environments, such as the Software Guard Extensions (SGX) included in recent Intel x86 processors, hold the promise of securely outsourcing sensitive computations to untrusted remote platforms. The compelling aspect of these architectures is that they aim to protect small software components, called *enclaves*, even against a very powerful type of root adversaries that have full control over the operating system on the target device. However, this thesis developed several innovative attack techniques that nuance the protection offered by today's trusted execution environments in general and Intel SGX in particular.

Research Methodology

While enclaves are strictly isolated at the architectural level, we found that this does not always hold at the lower levels of the processor's implementation. This observation gives rise to a line of *microarchitectural attacks*, which exploit unconstrained optimizations in the processor to reconstruct subtle traces about the enclave software running on top (cf. Figure 2).

In the first part of this dissertation, we develop novel techniques to derive private memory access patterns performed in a victim enclave with very high accuracy (cf. Figure 1). In the second part of this dissertation, we move from metadata exposure to direct data extraction in a critical new line of transient-execution attacks.

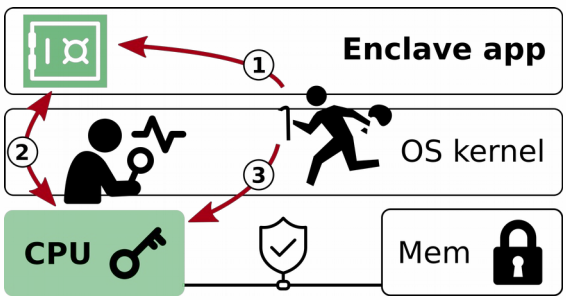
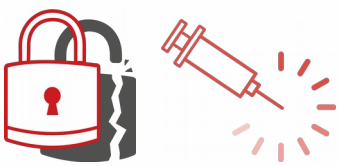


Figure 2: Privileged adversaries exploit interactions between the victim enclave and the CPU.



Results & Conclusions

Our results include several high-impact attacks that led to a full collapse of the Intel SGX ecosystem, affecting millions of devices and necessitating lengthy responsible-disclosure embargoes. The attacks presented in this dissertation were addressed through extensive hardware and software security updates in major processors, compilers, and operating systems.

Major Publications

- J. Van Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 27th USENIX Security Symposium, Aug. 2018, pp. 991–1008. https://foreshadowattack.eu/
- J. Van Bulck, D. Moghimi, M. Schwarz, M. Lipp, M. Minkin, D. Genkin, Y. Yuval, B. Sunar, D. Gruss, and F. Piessens. "LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection", 41st IEEE Symposium on Security and Privacy (S&P), May 2020, pp. 54–72. https://lviattack.eu/
- J. Van Bulck, F. Piessens, and R. Strackx. Microarchitectural Timing Leaks in Rudimentary CPU Interrupt Logic", 25th ACM Conference on Computer and Communications Security (CCS), Oct. 2018, pp. 178–195.