Verifying the Security of Enclaved Execution Against Interrupt-based Side-channel Attacks

Frank Piessens

KU Leuven

Belgium

Frank.Piessens@cs.kuleuven.be

ABSTRACT

Computing platforms sometimes provide hardware support for enclaves or trusted execution environments. On such platforms, security critical code can execute in an enclave or secure world, isolated from all other software on the platform.

But the past few years, several successful side-channel attacks have been developed that break, or at least significantly weaken the isolation that these mechanisms offer [1,2,3]. Particularly dangerous are software-based side-channels, as they can be launched even without physical access to the computing platform. These attacks often exploit architectural or micro-architectural features of the platform, like caches, paging, speculative execution, or interrupts. Extending a platform with new features, brings a risk of introducing new such side-channel attacks.

In this talk, we will discuss an approach to formally prove the security of platform extensions against these side-channel attacks, and instantiate that approach in a simple setting. More specifically, we will consider the concrete case of extending a microprocessor that supports enclaved execution with support for securely interrupting these enclaves. The base platform we start from is the Sancus system [4]. We show how making enclaves interruptible can lead to new side-channel attacks that weaken the isolation properties of enclaves. We then discuss how to formalize security against such attacks, and discuss the design and implementation of an interrupt handling mechanism for Sancus that is provably secure in the sense that it does not introduce new side-channel attacks.

Acknowledgments

The research reported on in this talk is joint work with Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, and Jan Tobias Mühlberg, and was

financially supported by a gift from Intel Corporation.

Author Keywords

Computer security; trusted execution environments; enclaves; interrupts; side-channel attacks

BIOGRAPHY

Frank Piessens is a full professor in the Department of Computer Science at the Katholieke Universiteit Leuven, Belgium. His research field is software security, where he focuses on the development of high-assurance techniques to deal with implementation-level software vulnerabilities and bugs, including techniques such as software verification, run-time monitoring, hardware security architectures, type systems and programming language design. He has served on the program committee of numerous security and software conferences including ACM CCS, Usenix Security, IEEE Security & Privacy, and ACM POPL. He acted as program chair for the International symposium on Engineering Secure Software and Systems (ESSOS 2014 & 2015), for the International Conference on Principles of Security and Trust (POST 2016) and for the IEEE European Symposium on Security & Privacy (Euro S&P 2018 & 2019).

REFERENCES

- [1] Y. Xu, et al., "Controlled-channel attacks: Deterministic side channels for untrusted operating systems," in IEEE S&P 2015
- [2] J. Van Bulck, et al., "Foreshadow: Extracting the keys to the Intel SGX kingdom with transient out-of-order execution," in USENIX Security 2018
- [3] J. Van Bulck, et al., "Nemesis: Studying microarchitectural timing leaks in rudimentary CPU interrupt logic," in ACM CCS 2018
- [4] J. Noorman, et al., "Sancus 2.0: A low-cost security architecture for IoT devices", ACM TOPS 20(3), 2017

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

TIS '19, November 11, 2019, London, United Kingdom.

© 2019 Copyright is held by the owner/author(s).

ACM ISBN 978-1-4503-6827-8/19/11.

DOI: <https://doi.org/10.1145/3338467.3358952>