Dinh Duy Kha

PhD Student @ Sungkyunkwan University, South Korea
kha-dinh | khadinh@skku.edu

Introduction

I am a third-year Ph.D. student advised by Prof. Hojoon Lee at System Security Lab, Sungkyunkwan University. I do research in Systems Security. My research interests include software security, operating systems security, trusted execution environments, and virtualization.

Experiences

System Security Lab, Sungkyunkwan University (SKKU) — Suwon, South Korea
Graduate Student Researcher — 2019 - Present

- Design security mechanisms that utilize modern hardware features.
- Design system-level mitigations against side-channels.

VNG Corporation — Ho Chi Minh City, Vietnam
Software Engineering Intern — Jun 2018 - Jun 2019

- Develop and maintain backend APIs for the TalkTV streaming platform written in C (now discontinued).

Education

Sungyunkwan University — Suwon, South Korea
PhD in System Security — 2019 - present
Ho Chi Minh City University of Technology — Ho Chi Minh City, Vietnam
B.S. in Computer Science — 2014 - 2019

Projects

Similation framework for PIM-based confidential computing

- Use gem5 to perform a full-system simulation of the emerging PIM hardware.
- Implemented security features to allow PIM to be used as an accelerator for confidential computing.

Cryptographic capabilities for program compartmentalization

- Designed an in-process capability-based compartmentalization framework that uses new ARM hardware features and evaluated its security.
- Developed LLVM compiler instrumentation passes to enforce its security policies on memory accesses.
- Developed a kernel module to support the isolation of file-related objects.

Accelerating AddressSantizers in Rust

- Designed and formalized the cross-IR compiler analyses that help classify safe, unsafe, and potentially unsafe memory accesses.

Publications

Duy, Kha Dinh, Taehyun Noh, et al. (2021). "Confidential Machine Learning Computation in Untrusted Environments: A Systems Security Perspective". In: *IEEE Access* 9, pp. 168656–168677. DOI: 10.1109/ACCESS.2021.3136889.

Dinh Duy, Kha et al. (2023). "Capacity: Cryptographically-Enforced In-Process Capabilities for Modern ARM Architectures". In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. CCS '23. ¡conf-loc¿, ¡city¿Copenhagen¡/city¿, ¡country¿Denmark¡/country¿, ¡/conf-loc¿: Association for Computing Machinery, pp. 874–888. ISBN: 9798400700507. DOI: 10.1145/3576915.3623079. URL: https://doi.org/10.1145/3576915.3623079.

Duy, Kha Dinh and Hojoon Lee (2023). "SE-PIM: In-Memory Acceleration of Data-Intensive Confidential Computing". In: *IEEE Transactions on Cloud Computing* 11.3, pp. 2473–2490. DOI: 10.1109/TCC.2022.3207145.

Cho, Kyuwon et al. (2024). "RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust (to appear)". In: *33nd USENIX Security Symposium (USENIX Security 24)*. USENIX Association.

Last updated: December 15, 2023