

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
<i>Graduate Student Researcher</i>	2019 - Present

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

VNG CORPORATION	Ho Chi Minh City, Vietnam
<i>Software Engineering Intern</i>	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
<i>PhD in System Security</i>	2019 - present

HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY	Ho Chi Minh City, Vietnam
<i>B.S. in Computer Science</i>	2014 - 2019

PROJECTS

SIMULATION 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.

PUBLICATION

- 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.
- Duy, Kha Dinh and Hojoon Lee (2022). “SE-PIM: In-Memory Acceleration of Data-Intensive Confidential Computing”. In: *IEEE Transactions on Cloud Computing*, pp. 1–18.
- 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. Copenhagen, Denmark: Association for Computing Machinery, pp. 874–888. DOI: [10.1145/3576915.3623079](https://doi.org/10.1145/3576915.3623079). URL: <https://doi.org/10.1145/3576915.3623079>.
- Cho, Kyuwon et al. (2024). “RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust (to appear)”. In: *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association.