Dinh Duy Kha

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

Introduction

I am a fifth-year Ph.D. candidate at Sungkyunkwan University, where I work with Prof. Hojoon Lee at the System Security Lab. My research sits at the intersection of operating system design and software security, with a current focus on software compartmentalization, practical defenses against side-channel attacks, and automated program analysis for software security. I'm particularly interested in how thoughtful architectural design can make systems inherently more secure.

Working Experiences

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

- Work on the development security of mechanisms that utilize modern hardware features.

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

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

Education

Sungyunkwan University — Suwon, South Korea
Ph.D. Candidate 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

Practical OS-Level Obfuscation of Confidential VMs Against Side-channel Attacks

- Developed an OS-level memory page randomization technique that protects unmodified CVM workloads from side-channel attacks.
- Developed an adaptive randomization strategy that reacts to the attacker's temporal resolution.
- Ported the Unikraft unikernel to work inside AMD SEV-SNP confidential virtual machines, which is contributed to the open-sourced core Unikraft kernel.

Cryptographic Capabilities for Program Compartmentalization

- Designed an in-process cryptographic capability compartmentalization framework that leverages new ARM hardware features and evaluated its security.
- Developed LLVM compiler instrumentation to enforce its security policies on memory accesses.
- Developed a Linux kernel module to enforce capability-based fine-grained isolation on file objects.

Accelerating AddressSantizer in Rust

- Co-designed and formalized compiler analyses that identify potentially unsafe instructions in Rust.

Similation Framework for Processing-in-Memory (PIM)-Based Confidential Computing

- Used gem5 to develop a full-system simulation of the emerging PIM hardware.
- Implemented and evaluated security features that allow PIM to be used as an accelerator for confidential computing.

Teaching

Graduate Teaching Assistant

- ESW4010: Special Topics on System Security (Fall 2021, Spring 2022, Fall 2022)
  - Developed an automated framework to deploy CTF challenges to docker containers.
  - Adapted the CTFd framework to make it more suitable for the classroom environment.
  - The framework is currently used to teach subsequence courses at https://ctf.skku.edu/.
- SWE2001: System Programming (Fall 2021)

Publication

[1] **Duy, K. D.**, Kim, J., Lim, H., Lee, H., " IncognitOS: A Practical Unikernel Design for Full-System Obfuscation in Confidential Virtual Machines," in *2025 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA: IEEE Computer Society, May 2025, pp. 3860–3877. DOI: 10.1109/SP61157.2025.00222. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP61157.2025.00222.

[2] Cho, K., Kim, J., **Duy, K. D.**, Lim, H., Lee, H., "RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust," in *33rd USENIX Security Symposium (USENIX Security 24)*, Philadelphia, PA: USENIX Association, Aug. 2024, pp. 3729–3746, ISBN: 978-1-939133-44-1. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/cho-kyuwon.

[3] **Duy, K. D.**, Cho, K., Noh, T., Lee, H., "Capacity: Cryptographically-Enforced In-Process Capabilities for Modern ARM Architectures," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '23, Copenhagen, Denmark: Association for Computing Machinery, 2023, pp. 874–888. DOI: 10.1145/3576915.3623079. [Online]. Available: https://doi.org/10.1145/3576915.3623079.

[4] **Duy, K. D.**, Lee, H., "SE-PIM: In-Memory Acceleration of Data-Intensive Confidential Computing," *IEEE Transactions on Cloud Computing*, pp. 1–18, 2022.

[5] **Duy, K. D.**, Noh, T., Huh, S., Lee, H., "Confidential Machine Learning Computation in Untrusted Environments: A Systems Security Perspective," *IEEE Access*, vol. 9, pp. 168 656–168 677, 2021.