Dinh Duy Kha

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

Introduction

I am a third-year Ph.D. student at Sungkyunkwan University, working under the guidance of Prof. Hojoon Lee in the System Security Lab. My research focuses on the intersection of system design and security, with specific interests in memory safety, program compartmentalization, operating systems design, trusted execution environments, and side-channel mitigations.

Working 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

- Used gem5 to develop a full-system simulation of the emerging PIM hardware.
- Implemented and evaluated 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 leverages 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 using the proposed capability-based framework.

Accelerating AddressSantizers in Rust

- Participated in designing and formalizing the cross-IR compiler analyses that help classify safe, unsafe, and potentially unsafe memory accesses.

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)

Open Source Contributions

- Unikraft

Publication

[1] **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. DOI: 10.1109/ACCESS.2021.3136889.

[2] Dinh Duy, K., 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, ¡conf-loc¿, ¡city¿Copenhagen¡/city¿, ¡country¿Denmark¡/country¿, ¡/conf-loc¿: Association for Computing Machinery, 2023, pp. 874–888, ISBN: 9798400700507. DOI: 10.1145/3576915.3623079. [Online]. Available: https://doi.org/10.1145/3576915.3623079.

[3] **Duy, K. D.**, Lee, H., "Se-pim: In-memory acceleration of data-intensive confidential computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 2473–2490, 2023. DOI: 10.1109/TCC.2022.3207145.

[4] Cho, K., Kim, J., **Duy, K. D.**, Lee, H., "Rustsan: Retrofitting addresssanitizer for efficient sanitization of rust (to appear)," in *33nd USENIX Security Symposium (USENIX Security 24)*, USENIX Association, 2024.