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.

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

- 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.

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 generate a unique key for each user, which is more suitable for the classroom environment.
- SWE2001: System Programming (Fall 2021)

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.