Curriculum Vitae - Junseung You

Seoul, South Korea | jsyou@sor.snu.ac.kr | 82 10 6652 5760 | sor.snu.ac.kr | github.com/jsyou-sor

Summary

I am a Ph.D. candidate supervised by Prof. Yunheung Paek in Seoul National University, specializing in systems security, particularly on hardware-assisted security solutions and confidential computing. My research focuses on addressing fundamental security challenges such as memory safety and isolation by leveraging hardware-based security features like ARM's Memory Tagging Extension. Further, I am interested in hardening trusted execution environment technologies for confidential computing across various architectures from various attacks. With hands-on experience in low-level system software, including kernel extensions, compilers, and hypervisors, I am eager to apply my skills to cutting-edge research and contribute to the advancement of secure systems.

Education

Seoul National University, MS/Ph.D. in Electrical and Computer Engineering — Sep 2019 - Feb 2026 (expected)
Seoul National University, BE in Electrical and Computer Engineering — Mar 2014 - Aug 2019

Publications

SECV: Securing Connected Vehicles with Hardware Trust Anchors — to appear
Martin Kayondo*, ***Junseung You****, Eunmin Kim, Jiwon Seo, Yunheung Paek
(: Both authors contributed equally to this work)*
Network and Distributed System Security (NDSS) Symposium

BASTAG: Byte-level Access Control on Shared Memory using ARM Memory Tagging Extension — Oct 2025
Junseung You, Jiwon Seo, Kyeongryong Lee, Yeongpil Cho, and Yunheung Paek
ACM SIGSAC Conference on Computer and Communications Security (CCS)

KVSEV: A Secure In-Memory Key-Value Store with Secure Encrypted Virtualization — Oct 2023
Junseung You, Kyeongryong Lee, Hyungon Moon, Yeongpil Cho, and Yunheung Paek
ACM Symposium on Cloud Computing

ZOMETAG: Zone-based Memory Tagging for Fast, Deterministic Detection of Spatial Memory Violations on ARM — July 2023
Jiwon Seo*, ***Junseung You****, Donghyun Kwon, Yeongpil Cho, and Yunheung Paek
(: Both authors contributed equally to this work)*
IEEE Transactions on Information Forensics and Security

SFITAG: Efficient Software Fault Isolation with Memory Tagging for ARM Kernel Extensions — July 2023
Jiwon Seo, ***Junseung You***, Yungi Cho, Yeongpil Cho, Donghyun Kwon, and Yunheung Paek
ACM Asia Conference on Computer and Communications Security (ASIACCS)

Enhancing a Lock-and-Key Scheme with MTE to Mitigate Use-After-Frees — Dec 2023
Inyoung Bang, Martin Kayondo, ***Junseung You***, Donghyun Kwon, Yeongpil Cho, and Yunheung Paek
IEEE Access

SBGen: A Framework to Efficiently Supply Runtime Information for a Learning-based HIDS for Multiple Virtual Machines — Nov 2020
Jiwon Seo, Inyoung Bang, ***Junseung You***, Yeongpil Cho, and Yunheung Paek
IEEE Access

Projects

ARM Confidential Compute Architecture Module — 2023-2024

- Guest/host kernel and hypervisor extension to support secure memory sharing between ARM confidential VMs
- Tools Used: C, KVM, LKVM, ARM FVP

Security Monitor for Multi-HTA System-on-Chips *funded by IITP, South Korea* 2024

- TrustZone-based security monitor on SoC heterogeneous processors for software-defined vehicles
- Tools Used: C, Rust, assembly, LLVM

Data Flow Tracking Runtime inside Trusted Execution Environment *funded by IITP, South Korea* 2024

- Used-defined policy based data flow analysis runtime for privacy preservation inside Intel SGX enclave
- Tools Used: C, Python, SGX SDK

Key Management Library inside SGX for HE *funded by IITP, South Korea* 2022 - 2023

- Key management service and library targeting homomorphic encryption for privacy-preserving computing
- Tools Used: C, SGX SDK

MQTT Broker Service for SGX Attestation *funded by IITP, South Korea* 2021-2022

- MQTT-based lightweight open, delegated attestation framework for Intel SGX enclaves
- Tools Used: C, SGX SDK, Python

Experience

Visiting Researcher, Arizona State University – Arizona, AZ Jan 2024 - Feb 2024

- Collaborated research with the team at ASU School of Computing and Augmented Intelligence
- Designed a mechanism to securely and efficiently share memory between confidential virtual machines supported by recent ARM Confidential Compute Architecture (CCA)
- Implementation across CCA software stack provided by ARM - guest virtual machine kernel, host kernel, host hypervisor, host firmware, etc.

Research Intern, National University of Singapore, School of Computing Sep 2018 - Feb 2019

- Undergraduate research intern at Network Security and Privacy Lab, NUS
- Implemented the design that safeguards network intrusion detection system (NIDS) in untrusted cloud with trusted execution environment - Intel Software Guard Extensions
- Ported various libraries such as OpenSSL and implemented system calls inside libOS prototype for SGX to run Snort NIDS inside enclave

Teaching (Assistant)

Introduction to Security, Privacy and Blockchain *undergrad course* Mar 2024 - Jun 2024

Topics on System Software (Data Security and Privacy) *grad course, head TA* Sep 2024 - Dec 2024

Awards and Scholarship

A Study on Vulnerabilities and Defense Systems of ARM TrustZone-assisted TEEs 2020
Best paper award from Korea Information Processing Society

A Study on Isolation of Kernel Subsystems and Kernel Modules 2020
Best paper award from Korea Institute of Information Security and Cryptology

Scholarship
BK21+ Scholarship *by the Ministry of Education of Korea* Mar 2020 - Aug 2025

Grants
ACM CCS 2025 Student Travel Grant Oct 2025

Services & Activities

EuroSys 2025 *Shadow Program Committee*

IEEE Transactions on Dependable and Secure Computing *Reviewer* Oct 2025

Secondary-Reviewer

IEEE Transactions on Computers	2025
Silicon Valley Cybersecurity Conference	2025

Talks & Seminars

"*Hardware-Assisted Security on Arm Mobile Platforms - From Memory Safety to Confidential Computing*" *presented at Sejong University, November 2025*

Skills

Programming: C/C++, Rust, Python

Frameworks: LLVM, rustc, ARM FVP, KVM/QEMU, SGX SDK

Platforms: Linux (x86_64, AArch64, AArch32), Android

Language: English (iBT TOEFL: 114), Korean (native)