JUNSEUNG YOU (유준승)

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 at Seoul National University advised by Prof. Yunheung Paek, working in systems security. My research agenda develops ***hardware-assisted mechanisms that efficiently address fundamental systems security challenges*** such as memory safety and isolation, leveraging architectural primitives including Arm Memory Tagging Extension (MTE) and trusted execution environments (TEEs). My work is grounded in low-level systems development across the compiler/toolchain, operating system kernel, and hypervisor.

RESEARCH INTERESTS

- Systems Security
- Hardware-assisted Security
- Confidential Computing
- Autonomous Systems Security

EDUCATION

Seoul National University, Ph.D. in Electrical and Computer Engineering — Sep 2019 - Feb 2026 (expected)

Advisor: Yunheung Paek
Dissertation Title (tentative): Hardware-Assisted Memory Protection on ARM with Memory Tagging Extension

Seoul National University, B.E. in Electrical and Computer Engineering — Mar 2014 - Aug 2019

EXPERIENCE

Seoul National University, Seoul, Korea — Mar 2026 - Aug 2027

Military Service
Serving as Expert Research Personnel (전문연구요원)

Seoul National University, Seoul, Korea — Sep 2019 - Feb 2026

Research Assistant
Advisor: Yunheung Paek

Arizona State University, Tempe, AZ, USA — Jan 2024 - Feb 2024

Visiting Researcher
Advisor: Gail-Joon Ahn, Hokeun Kim
Topic: Hardening Arm trusted execution environment (confidential compute architecture)

National University of Singapore, Singapore, Singapore — Sep 2018 - Feb 2019

Research Intern
Advisor: Min Suk Kang
Topic: Securing network intrusion detection system with trusted execution environment

PUBLICATIONS

Refereed Conference Publications

[1] **SECV: Securing Connected Vehicles with Hardware Trust Anchors** — Feb 2026
Martin Kayondo*, ***Junseung You****, Eunmin Kim, Jiwon Seo, and Yunheung Paek
(**: Both authors contributed equally to this work*)
Network and Distributed System Security (NDSS) Symposium

[2] **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)

[3] **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 (SoCC)

[4] **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)

Refereed Journal Publications

[5] **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 (TIFS)

[6] **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

[7] **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 INVOLVED

with fundings, Principal Investigator : Yunheung Paek

On-device AI Protection *funded by MCST and KOCCA, RS-2025-02221620* Apr 2025 - Current
- Role: Designing on-device AI model protection protocol with TEEs.

Side-channel Resistant SoC IP *funded by Samsung Electronics, South Korea* Sep 2024 - Sep 2025
- Role: Designing mask/parity-based side-channel protection mechanism on RISC-V SoC.

Preserving Privacy using Confidential Computing *funded by IITP, RS-2024-00438729* Jun 2024 - Current
- Role: Designing user-defined policy-based data flow analysis runtime for privacy preservation inside TEEs.

Autonomous Vehicle Security Monitor *funded by MOTIE, RS-2024-00406121* Apr 2024 - Current
- Role: Design ECU protection framework with multiple hardware trust anchors.

HW-centric Secure Data Box *funded by IITP, 2021-0-00528* Apr 2021 - Current
- Role: Designing and implementing secure protocol for using multiple privacy-preserving techniques.

Data Tracking and Protection in Cloud Edge *funded by IITP* Apr 2020 - Dec 2021
- Role: Designing lightweight attestation framework for TEEs.

TEACHING EXPERIENCE

Seoul National University (TA)

Topics on System Software (Data Security and Privacy)
- Period : 2024-2, 2025-2
- Role : Head teaching assistant. Authored lecture materials for system security and TEEs. Lecturer for several system security related topics. Authored, administered, and graded presentations and lab projects.

Introduction to Security, Privacy and Blockchain
- Period : 2024-1, 2025-1
- Role: Authored course materials for system security and confidential computing. Lecturer for introduction to computer systems and security. Authored, administered, and graded course quizzes.

Creative Design Project (Graduation Project)

- Period : 2022-1 to Current
- Role : Guided undergraduates on their final-year graduation projects from topic selection to thesis writeup.

HONORS & AWARDS

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

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

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

[1] *"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)