Youngjoo Shin

Korea University • syoungjoo@korea.ac.kr • 02-3290-4884 • syoungjoo.github.io • github.com/syoungjoo
linkedin.com/in/youngjoo-shin-b8b14a55

Summary

Youngjoo Shin is an Associate Professor in the School of Cybersecurity at Korea University, where he directs the Computer Systems Security Lab. His research investigates the security of modern computer systems — from CPU microarchitecture to operating systems, virtualization platforms, and cloud infrastructure — with a particular focus on side-channel and transient-execution attacks, OS kernel defenses, and practical privacy-preserving system design.

Before joining Korea University in 2020, he was an Assistant Professor at Kwangwoon University (2017–2020), a Senior Researcher at the National Security Research Institute (2008–2017), and a Researcher at LG Electronics' Digital Media Laboratory (2007–2008).

Interests

System Security, Microarchitectural Side-channel Attacks, Transient Execution Attacks, OS & Hypervisor Security, Cloud & Container Security, Network Security, Applied Cryptography

Education

KAIST *Korea*
Ph.D in Computer Science

KAIST *Korea*
M.S in Computer Science

Korea University *Korea*
B.S in Computer Science and Engineering

Experience

Associate Professor *2022.3 – present*
School of Cybersecurity, Korea University

Assistant Professor *2020.9 – 2022.2*
School of Cybersecurity, Korea University

Assistant Professor *2017.3 – 2020.8*
Kwangwoon University

Senior Researcher *2008.4 – 2017.2*
National Security Research Institute (NSR)

Researcher *2007.11 – 2008.3*
Digital Media Laboratory, LG Electronics

Research Assistant *2006.3 – 2007.12*
Mobile Multimedia Platform Center, KAIST

Publications

Input-Agnostic Runtime Metric Based Memory Optimization for Serverless Functions Jan 2026
Seunghun Kim, Youngjoo Shin
(IEEE International Conference on Cloud Computing (CLOUD))

TIMESLICE-SANDWICH: A GPU Side-channel Attack Exploiting Time-Sliced Scheduling Jan 2026
Hodong Kim, Gyeongsup Lim, Seunghee Shin, Youngjoo Shin, Junbeom Hur
(USENIX Security Symposium)

SysDiver: Lightweight and Fast Static Analysis for Windows Kernel Drivers Jan 2026
Chanhee Park, Dongjoo Kim, Youngjoo Shin
(ACM Asia Conference on Computer and Communications Security (ASIACCS))

Empirical Study on BMC Firmware Vulnerabilities: Root Causes and Architectural Insights Jan 2026
Jihye Lee, Chanhee Park, Youngjoo Shin
(International Conference on Information Networking (ICOIN))

PathFault: Automated Exploit Generator for Web Services via HTTP Message Parser Discrepancies Jan 2025
Juryeok Kim, Youngjoo Shin
(International Conference on Information Security and Cryptology (ICISC))

MimicCall: Bypassing System Call Filters via Kernel Function Redundancy Jan 2025
Songah Joo, Minchan Park, Hyerean Jang, Youngjoo Shin
(Annual Computer Security Applications Conference (ACSAC))

A Survey of Speculative Load Prediction Attacks Exploiting Memory Disambiguation Units Jan 2025
Selynn Kim, Taehun Kim, Youngjoo Shin
(World Conference on Information Security Applications (WISA))

PodBeater: Exploiting Multi-Value Affinity for Efficient Co-Location Attacks in Kubernetes Jan 2025
Yiju Jung, Hyerean Jang, Youngjoo Shin
(World Conference on Information Security Applications (WISA))

Maximizing GPU Parallelism for a High-performance Cryptanalysis System Jan 2025
Sangyub Kim, Youngjoo Shin
(International Conference on Information Networking (ICOIN))

T-Time: A Fine-grained Timing-based Controlled-Channel Attack against Intel TDX Jan 2025
Woomin Lee, Taehun Kim, Seunghee Shin, Junbeom Hur, Youngjoo Shin
(European Symposium on Research in Computer Security (ESORICS))

Cache Demote for Fast Eviction Set Construction and Page Table Attribute Leakage Jan 2025
Taehun Kim, Hyerean Jang, Youngjoo Shin
(European Symposium on Research in Computer Security (ESORICS))

Vulnerable Intel GPU Context: Prohibit Complete Context Restore by Modifying Kernel Driver Jan 2025
Wonseok Choi, Youngjoo Shin
(ACM Asia Conference on Computer and Communications Security (ASIACCS))

A Survey of Side-Channel Attacks on Branch Prediction Units Jan 2025
Jihoon Kim, Hyerean Jang, Youngjoo Shin
(ACM Computing Surveys)

BranchCloak: Mitigating Side-Channel Attacks on Directional Branch Predictors Jan 2025
Jihoon Kim, Hyerean Jang, Youngjoo Shin
(Electronics)

FuzzyBin: Enhanced Border Binary Identification by Leveraging Fuzzy Hashing Algorithms Jan 2025
Dongsoo Kim, Hyerean Jang, Youngjoo Shin
(IEEE Access)

SysBumps: Exploiting Speculative Execution in System Calls for Breaking KASLR in macOS for Apple Silicon Jan 2024
Hyerean Jang, Taehun Kim, Youngjoo Shin
(ACM Conference on Computer and Communications Security (CCS))

POSTER: Beyond the Filter: Advanced Mimicry Attack to Bypass System Call Filtering Jan 2024
Songah Joo, Hyerean Jang, Youngjoo Shin
(Annual Computer Security Applications Conference (ACSAC))

HBRA: A History-Based Remote Attestation Approach to Resolve Malicious Verifiers in IoT Jan 2024
Euiseong Moon, Youngjoo Shin
(International Conference on ICT Convergence (ICTC))

POSTER: On the Feasibility of Inferring SGX Execution through PMU Jan 2024
Woomin Lee, Taehun Kim, Youngjoo Shin
(ACM Asia Conference on Computer and Communications Security (ASIACCS))

S-ZAC: Hardening Access Control of Service Mesh using Intel SGX for Zero Trust in Cloud Jan 2024
Changhee Han, Taehun Kim, Woomin Lee, Youngjoo Shin
(Electronics)

Exploiting Memory Page Management in KSM for Remote Memory Deduplication Attack Jan 2023
Seungyeon Bae, Taehun Kim, Woomin Lee, Youngjoo Shin
(World Conference on Information Security Applications (WISA))

DevIOus: Device-Driven Side-Channel Attacks on the IOMMU Jan 2023
Taehun Kim, Hyeongjin Park, Seokmin Lee, Seunghee Shin, Junbeom Hur, Youngjoo Shin
(IEEE Symposium on Security and Privacy (S\&P))

MicroCFI: Microarchitecture-level Control-Flow Restrictions for Spectre Mitigation Jan 2023
Hyerean Jang, Youngjoo Shin
(IEEE Access)

Deep Learning based Detection for Multiple Cache Side-channel Attacks Jan 2023
Hodong Kim, Changhee Hahn, Hyunwoo J. Kim, Youngjoo Shin, Junbeom Hur
(IEEE Transactions on Information Forensics and Security)

GAN-based patient information hiding for an ECG authentication system Jan 2023
Youngshin Kang, Geunbo Yang, Heesang Eom, Seungwoo Han, Suwhan Baek, Seungil Noh, Youngjoo Shin, Cheolsoo Park
(Biomedical Engineering Letters)

Fuzzing of Embedded Systems: A Survey Jan 2023
Joobeom Yun, Fayozbek Rustmov, Juhwan Kim, Youngjoo Shin
(ACM Computing Surveys)

A Performance Evaluation of IPsec with Post-Quantum Cryptography Jan 2022
Seungyeon Bae, Yuseong Chang, Hyeongjin Park, Youngjoo Shin
(International Conference on Information Security and Cryptology (ICISC))

Avengers, Assemble! Survey of WebAssembly Security Solutions Jan 2022
Minseo Kim, Hyerean Jang, Youngjoo Shin
(IEEE International Conference on Cloud Computing (CLOUD))

Broken Heart: Privacy Leakage Analysis on ECG-based Authentication Schemes Jan 2022
Seungil Noh, Jaehan Kim, Seokmin Lee, Youngshin Kang, Cheolsoo Park, Youngjoo Shin
(Security and Communication Networks)

ThermalBleed: A Practical Thermal Side-Channel Attack Jan 2022
Taehun Kim, Youngjoo Shin
(IEEE Access)

Quantitative Analysis on Attack Capacity in Meltdown-type Attacks Jan 2021
Seokmin Lee, Taehun Kim, Youngjoo Shin
(World Conference on Information Security Applications (WISA))

A Secure and Privacy-Preserving ECG-based Personal Authentication Jan 2021
Youngshin Kang, Hyeonbin Lee, Youngjoo Shin, Cheolsoo Park
(IEEE International Conference on Smart Internet of Things (SmartIoT))

(Extended Abstract) DCUIP Poisoning Attack in Intel x86 Processors Jan 2021
Youngjoo Shin
(International Conference on Information Networking (ICOIN))

Constructing Covert Channel on Intel CPU-iGPU Platform Jan 2021
Taehun Kim, Taehyun Kim, Youngjoo Shin
(International Conference on Information Networking (ICOIN))

Breaking KASLR Using Memory Deduplication in Virtualized Environments Jan 2021
Taehun Kim, Jaehan Kim, Youngjoo Shin
(Electronics)

Runtime Randomized Relocation of Crypto Libraries for Mitigating Cache Attacks Jan 2021
Youngjoo Shin, Joobeom Yun
(IEEE Access)

DCUIP Poisoning Attack in Intel x86 Processors Jan 2021
Youngjoo Shin
(IEICE Transactions on Information and Systems)

Multibyte microarchitectural data sampling and its application to session key extraction attacks Jan 2021
Youngjoo Shin
(IEEE Access)

Return of Version Downgrade Attack in the Era of TLS 1.3 Jan 2020
Sangtae Lee, Youngjoo Shin, Junbeom Hur
(ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT))

Software-based Random Number Generators for Resource Constrained Devices Jan 2020
Seungil Noh, Youngjoo Shin
(International Conference on ICT Convergence (ICTC))

(Poster) Mitigating Memory Sharing-based Side-channel Attack by Embedding Random Values in Binary for Cloud Environment Jan 2020
Taehun Kim, Youngjoo Shin
(ACM Asia Conference on Computer and Communications Security (ASIACCS))

GPU Side-channel Attacks are Everywhere: A Survey Jan 2020
Taehun Kim, Youngjoo Shin
(IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia))

Inferring Firewall Rules by Cache Side-channel Analysis in Network Function Virtualization Jan 2020
Youngjoo Shin, Dongyoung Koo, Junbeom Hur
(IEEE International Conference on Computer Communications (INFOCOM))

Cache Side-Channel Attack on Mail User Agent Jan 2020
Hodong Kim, Hyundo Yoon, Youngjoo Shin, Junbeom Hur
(International Conference on Information Networking (ICOIN))

Decentralized Server-aided Encryption for Secure Deduplication in Cloud Storage Jan 2020
Youngjoo Shin, Dongyoung Koo, Joobeom Yun, Junbeom Hur
(IEEE Transactions on Services Computing)

Toward Serverless and Efficient Encrypted Deduplication in Mobile Cloud Computing Environments Jan 2020
Youngjoo Shin, Junbeom Hur, Dongyoung Koo, Joobeom Yun
(Security and Communication Networks)

Lightweight and Seamless Memory Randomization for Mission-Critical Services in Cloud Platform Jan 2020
Joobeom Yun, Ki-Woong Park, Dongyoung Koo, Youngjoo Shin
(Energies)

Real-Time Detection for Cache Side Channel Attack using Performance Counter Monitor Jan 2020
Jonghyeon Cho, Taehun Kim, Soojin Kim, Miok Im, Taehyun Kim, Youngjoo Shin
(Applied Sciences)

FPGA reverse engineering in Vivado design suite based on X-ray project Jan 2019
Hoyoung Yu, Hyung-Min Lee, Youngjoo Shin, Youngmin Kim
(International SoC Design Conference (ISOCC))

Real-Time Detection on Cache Side Channel Attacks using Performance Counter Monitor Jan 2019
JongHyeon Cho, TaeHyun Kim, Youngjoo Shin
(International Conference on ICT Convergence (ICTC))

High efficiency, low-noise Meltdown attack by using a return stack buffer Jan 2019
TaeHyun Kim, Youngjoo Shin
(ACM Asia Conference on Computer and Communications Security (ASIACCS))

Poster: FLUSH+REALOD Cache Side-Channel Attack on Mail User Agent Jan 2019
Hodong Kim, Hyundo Yoon, Youngjoo Shin, Junbeom Hur
(Network and Distributed System Security Symposium (NDSS))

Reinforcing Meltdown Attack By using Return Stack Buffer Jan 2019
TaeHyun Kim, Youngjoo Shin
(IEEE Access)

A VM-Based Detection Framework against Remote Code Execution Attacks for Closed Source Network Devices Jan 2019
Youngjoo Shin
(Applied Sciences)

Cross-VM Cache Timing Attacks on Virtualized Network Functions Jan 2019
Youngjoo Shin
(IEICE Transactions on Information and Systems)

Unveiling Hardware-based Data Prefetcher, a Hidden Source of Information Leakage Jan 2018
Youngjoo Shin, Hyung Chan Kim, Dokeun Kwon, Ji Hoon Jeong, Junbeom Hur
(ACM Conference on Computer and Communications Security (CCS))

Privacy-preserving and Updatable Block-level Data Deduplication in Cloud Storage Services Jan 2018
Hyungjune Shin, Dongyoung Koo, Youngjoo Shin, Junbeom Hur
(IEEE International Conference on Cloud Computing (CLOUD))

Improving Security and Reliability in Merkle Tree-based Online Data Authentication with Leakage Resilience Jan 2018
Dongyoung Koo, Youngjoo Shin, Joobeom Yun, Junbeom Hur
(Applied Sciences)

Fast and Secure Implementation of Modular Exponentiation for Mitigating Fine-grained Cache attacks Jan 2018
Youngjoo Shin
(Applied Sciences)

An Online Data-Oriented Authentication based on Merkle Tree with Improved Reliability Jan 2017
Dongyoung Koo, Youngjoo Shin, Joobeom Yun, Junbeom Hur
(IEEE International Conference on Web Services (ICWS))

Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage (Extended Abstract) Jan 2017
Junbeom Hur, Dongyoung Koo, Youngjoo Shin, Kyungtae Kang
(IEEE International Conference on Data Engineering (ICDE))

Practical Data Outsourcing Framework with Provably Secure Deduplication in Untrusted Remote Storage Jan 2017
Dongyoung Koo, Youngjoo Shin, Junbeom Hur
(International Conference on Platform Technology and Service (PlatCon))

A Survey of Secure Data Deduplication Schemes for Cloud Storage Systems Jan 2017
Youngjoo Shin, Dongyoung Koo, Junbeom Hur
(ACM Computing Surveys)

Decentralized Server-aided Encryption for Secure Deduplication in Cloud Storage Jan 2017
Youngjoo Shin, Dongyoung Koo, Joobeom Yun, Junbeom Hur
(IEEE Transactions on Services Computing)

Secure Proof of Storage with Deduplication for Cloud Storage Systems Jan 2017
Youngjoo Shin, Dongyoung Koo, Junbeom Hur, Joobeom Yun
(Multimedia Tools and Applications)

CLDSafe: An Efficient File Backup System in Cloud Storage against Ransomware Jan 2017
Joobeom Yun, Junbeom Hur, Youngjoo Shin, Dongyoung Koo
(IEICE Transactions on Information and Systems)

Privacy-Preserving Aggregation and Authentication of Multi-source Smart Meters in a Smart Grid System Jan 2017
Dongyoung Koo, Youngjoo Shin, Junbeom Hur
(Applied Sciences)

An efficient stream cipher for resistive RAM Jan 2017
Joobeom Yun, Ki-Woong Park, Youngjoo Shin, Hee-Dong Kim
(IEICE Electronics Express)

invited talks

2026: NetSec-KR 2026, IITP Special Session (invited talk)

2025: WDSC 2025 (invited lecture); Drone Cybersecurity Seminar; Unification & Sharing Policy Research Seminar

2024: NetSec-KR 2024

2023: KAIST Colloquium; KSC 2023; ROK Navy Cybersecurity Seminar; WebAssembly Security Seminar

2022: Hansung University

2021: NSR; Hansung University; Sejong University

2020: Side-Channel Analysis Workshop; NSR; Hoseo University; SeoulTech; Hansung University; Sejong University; Kookmin University

2019: KAIST; Korea University; SeoulTech; Sejong University; Hansung University; Kookmin University; WISC 2019; Side-Channel Analysis Workshop

2018: NetSec-KR 2018; KICS; ETRI; NSR; WISC 2018; Side-Channel Analysis Workshop; Sejong / Kookmin / Hansung / Hannam Universities

2017: KCC 2017; SDN/NFV Forum Security WG; NSR; Korea / Kookmin / Hansung Universities

government & public-sector advisory

- IITP Preliminary Feasibility Study, Intelligent Cyber-Shield Dome Program — Subcommittee Member (2025–)
- Cloud Security Assurance Program (CSAP) Certification Committee (2023–2024)
- National Security Research Institute (NSR) — Digital-Signature Advisory (2022)
- National Intelligence Service — Mid-/Long-Term Security Strategy Advisory (2019)
- IITP Preliminary Feasibility Study on Connected-Device Security — Committee Member (2017)

peer review & evaluation

- Korea Data Agency (KoData) — KOSDAQ Technology Assessment Advisor, ICT Sector
- Korea Internet & Security Agency (KISA) — Evaluation Committee Member (2017, 2018)

program committee

- 2026: PST 2026; SECRYPT 2026; SecureComm 2026 (EAI); IFIP SEC 2026
- 2024: ICISC 2024; SmartSP 2024
- 2023: ICISC 2023
- 2022: WoNEXT 2022; CISC-W 2022
- 2020: KCS 2020
- 2018: Security 2018 (사이버보안 논문 공모전)

standards, guidelines & industry

- Korea Association for Industrial Technology Security (KAITS) — Contribution/Advisory on The Future of Sovereign Cloud
- KISA — Key-Management Guidelines Review Advisory
- IDEC — External Advisor (2024)
- LG U+ — Security Advisory (2019)
- KANI; SDN/NFV Forum Security Working Group (2017)

Academia

- Kwangwoon University — Faculty Recruitment Review Committee (2024)
- Kookmin University — Faculty Review Committee (2018)