Yoshi Sato

Undergraduate Researcher | Computer Security

Tokyo, Japan • yoshi.sato@fuji.waseda.jp • yoshisato.io • github • linkedin

Education

WASEDA UNIVERSITY **Tokyo, Japan**

Bachelor of Science in Computer Science and Communications Engineering **Oct 2022 - Jul 2026**

Research Interests: Microarchitectural Security, Systems Security, Trusted Execution Environments (TEEs)

Publications

[Conference Paper] **Y. Sato**, H. Uranami, A. Saiki, K. Kimura. "Towards GPU Passthrough in Intel TDX: Design Challenges and Early Baselines." In *Proceedings of the IEEE 23rd International Conference on Dependable, Autonomic and Secure Computing (DASC),* 2025. (Best Poster Award)

[Submitted / Under Review] M. Barbaraci, S. Ma, H. Malvai, M. Mouallem, S. Ren, **Y. Sato**, S. Yang, F. Zhang. "DeadDrop: Responsible Disclosure of Smart Contract Bugs." Submitted to *Proceedings on Privacy Enhancing Technologies* (PoPETS), 2026. (Author order alphabetical)

Research Experience

Research Intern, Decentralized Systems Group, Yale University **Jul 2025 - Present**

Advisor: Prof. Fan Zhang

- Architected the core cryptographic primitive for DeadDrop using Oblivious Message Retrieval (OMR) to produce the first functional prototype for oblivious bug reporting.
- Identified a critical “database jumbling” vulnerability where implementation deviated from the theoretical binding of payloads and clues; led discussions to redefine the system’s threat model.
- Designed and executed performance evaluations to quantify clue processing, achieving a throughput of 32,768 payloads in 108s (single-core) and scaling to 524,288 payloads in 110s (16-core).
- Parallelized the precomputation phase of OMR to **reduce initialization latency by 65%**, significantly improving the prototype's practicality for real-world deployment.
- Leading a Systematization of Knowledge (SoK) project on TEEs with researchers from Yale and UIUC to define a new taxonomy and evaluation framework for confidential containers.

Student Researcher, Kasahara-Kimura Lab, Waseda University **Apr 2025 - Present**

Advisor: Prof. Keiji Kimura & Prof. Hironori Kasahara

- Initiated an independent research project on GPU passthrough in Intel TDX, culminating in a paper accepted to IEEE DASC 2025 that won the Best Poster Award.
- Dissected microarchitectural I/O bottlenecks by comparing shared memory buffers in AMD SEV-SNP and Intel TDX.
- Identified that while AMD's `PVALIDATE` incurs zero VM Exits, Intel TDX’s `TDG.MEM.PAGE.ACCEPT` triggers mandatory VM Exits, creating a structural latency bottleneck.
- Quantified memory overheads, establishing a baseline revealing that pageable memory throughput degrades by ~53% compared to pinned memory in confidential environments.

Research Intern, IIJ Research Laboratory **Mar 2025 - Present**

Advisor: Dr. Pierre-Louis Aublin

- Collaborated with the LSDS Group at Imperial College London on Serverless Confidential Containers (SC2) to analyze performance overheads in secure serverless computing.
- Transformed a research prototype into a fully reproducible testbed, enabling the first performance evaluation of the SC2 system on Intel TDX hardware.
- Engineered custom network proxy support for the Knative control plane to resolve critical deployment failures in restricted network environments.
- Analyzing confidential VM cold-start execution paths using Ftrace to identify and quantify dominant latency sources in the boot process.

Professional Service

Artifact Evaluation Committee (AEC) Member **Feb 2026**

The 21st European Conference on Computer Systems (EuroSys 2026)

Student Volunteer **Jun 2025**

The 52nd Annual International Symposium on Computer Architecture (ISCA 2025)

Awards

Best Poster Award, IEEE DASC 2025

Professional Experience

IoT Penetration Testing Intern, FFRI Security **Jan - Feb 2025**

- Conducted static and dynamic binary analysis on IoT firmware and malware executables using Ghidra and GDB, identifying critical vulnerabilities in legacy software components.
- Executed penetration tests on simulated IoT environments to simulate real-world attack vectors against embedded devices, using Nmap, Metasploit, and Wireshark.

Leadership

Secretary, IEEE-HKN, Mu Tau Chapter **Jul 2025 - Present**

Nominated by 2018 IEEE Computer Society President

Co-founder, Kuma Lab **Apr 2024 - Present**

- Founded a student research community of ~30 members to foster peer learning in AI and robotics.
- Organized a flagship technical workshop hosted at Google Shibuya for 25 attendees to bridge the gap between advanced research and non-STEM audiences.

Skills

- TEEs: Intel TDX, AMD SEV-SNP
- Systems: QEMU, Kubernetes, Knative, Docker, Arch Linux
- Applied Cryptography: Microsoft SEAL, PALISADE
- Programming Languages: Python, C++, Rust