Yoshiaki Sato

Student Researcher | Confidential Computing & Trusted Execution

Tokyo, Japan • yoshisato@kasahara.cs.waseda.ac.jp • +81 90-5282-6969 • https://yoshisato.io

Education

WASEDA UNIVERSITY **Tokyo, Japan**

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

Experience

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

- Conducting research on confidential computing under the supervision of Professor Keiji Kimura.
- Analyzing and benchmarking performance characteristics of I/O peripherals within VM-based Trusted Execution Environments (TEEs).

Research Assistant, IIJ Research Laboratory **Feb 2025 - Present**

- Researching confidential computing applications under the supervision of Dr. Pierre-Louis Aublin.
- Collaborating with Imperial College London's Large-Scale Data & Systems (LSDS) Group, investigating serverless confidential computing and the security of distributed systems.

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

- Performed penetration tests on simulated IoT devices using real-world cybersecurity tools.
- Presented findings and remediation strategies to experienced security engineers, learning how to clearly communicate technical results to both specialist and non-specialist stakeholders.

Personal Projects

ICS Security Simulation Lab (**Network Security Lab, Waseda**) **Dec 2024 - Jan 2025**

- Developed and orchestrated a VirtualBox ICS environment with 5 VMs (Ubuntu, Windows, Kali Linux).
- Integrated OpenPLC, Factory I/O, and pfSense to create an ICS-specific intrusion detection system.
- Simulated real-world industrial cyber threats (network scanning, phishing, logic injection) to evaluate detection efficacy and improve network segmentation strategies.

Pre-Training Pipeline for Decoder Transformer **Mar - Apr 2024**

- Managed and optimized a large-scale ML workflow, improving loss by 40% from initial training rounds.
- Utilized over 35 hours of A100 GPU compute on Google Colab to train and refine model architectures.

Skills

- Research: Intel TDX, AMD SEV-SNP, Kubernetes, Knative, Docker, Linux
- Cybersecurity Tools: Nmap, Wireshark, Metasploit, Ghidra, x64dbg, Exploit-DB
- AI/ML: PyTorch, WandB, AWS (EC2, Lambda, RDS, S3, etc.)
- Programming Languages: C, Python

Extracurricular Activities

Cofounder of Kuma Lab **Apr 2024 - Present**

- Founded a student community of ~30 members to advance robotics and AI research, fostering collaboration and knowledge-sharing in STEM. Organized events and monthly workshops with 10–15 University students.

Backend Developer, Google Developers Student Club **Nov 2023 - Feb 2024**

- Collaborated on the Google Solution Challenge, developing a tool to improve navigation for university labs.