Satoshi Okada

Web: https://satoshi-okada.github.io
Email: okada@hal.ipc.i.u-tokyo.ac.jp

EDUCATION

- Ph.D. Information Science and Technology, the University of Tokyo.
  Apr. 2022 - Mar. 2025
- M.S. Information Science and Technology, the University of Tokyo.
  Apr. 2020 – Mar. 2022
- B.S. Mathematical Engineering and Information Physics, the University of Tokyo.
  Apr. 2016 – Mar. 2020

Work experience

- Ph.D. Internship at Télécom SudParis (Apr. 2023 - Sep. 2023)

- Project Researcher at Toyo University (Apr. 2021 - Mar. 2025)

- Research Assistant at Toyo University (Oct. 2020 - Mar. 2021)

- Teaching Assistant at the University of Tokyo (Apr. 2020 - Aug. 2021)

- Research Intern at NTT Laboratory (Summer 2020)

- Research Assistant at the University of Tokyo (Apr. 2016 - Sep. 2020)

Skills

- Computer Skills: C/C++, Python Programming
- Qualifications
  - Applied Information Technology Engineer Examination (Sep. 2018)
  - Registered Information Security Specialist (Sep. 2022)
- Language Skills: Japanese (Native Speaker), English

Scholarships and Grants

- JSPS Overseas Challenge Program for Young Researchers (Apr. 2023 - Sep. 2023)

Awards

- The Dean's Award of the Graduate School of Information Science and Technology, The University of Tokyo 2024 (link), Mar. 2025.
- 辻井重男セキュリティ論文賞 (link), Aug. 2023.
- IEEE International Conference on Computing (ICOCO 2022) Best Paper Award (press, certificate), Nov. 2022.
- The Dean's Award of the Graduate School of Information Science and Technology, The University of Tokyo 2021 (link), Mar. 2022.
- IEEE International Conference on Computing (ICOCO 2021) Best Paper Award (certificate), Nov. 2021.

Research Interests

- Machine Learning
- System Security
- IoT security
- Post-quantum Cryptography
- Low-layer Security (Binary Analysis)

Research Publications

Journals (Peer-reviewed)

[1] **Satoshi Okada**, Houda Jmila, Kunio Akashi, Takuho Mitsunaga, Yuji Sekiya, Hideki Takase, Gregory Blanc, Hiroshi Nakamura, "Xai-driven black-box adversarial attacks on network intrusion detectors," International Journal of Information Security, 24, 2025.

[2] **Satoshi Okada**, Yosuke Katano, Yukihiro Kozai, Takuho Mitsunaga, "Predicting and Visualizing Lateral Movements Based on ATT&CK and Quantification Theory Type 3," Journal of Cases on Information Technology (JCIT), vol.26(1), pp.1-14, 2024

[3] Masaki Kuwano, Momoka Okuma, **Satoshi Okada**, Takuho Mitsunaga, "Predicting What the Attacker Might Do Next: ATT&CK Behavior Forecasting by Attacker-based Collaborative Filtering and Graph Databases," Journal of Information Processing, vol.31, pp.802-811, 2023.

[4] **Satoshi Okada**, Kunio Akashi, Daisuke Miyamoto, Yuji Sekiya, Hideki Takase, Hiroshi Nakamura, "Memory-saving LDoS Attacker Detection Algorithms in Zigbee Network," Journal of Information Processing, vol.31, pp.537-549, 2023.

[5] **Satoshi Okada**, Nobuho Hashimoto, Takuho Mitsunaga, "Efficient Matching Algorithms between Logs and Indicators for Automatic Incident Response System," Journal of Information Processing, vol. 31, pp.279-287, 2023.

International Conferences (Peer-reviewed)

[1] Junichiro Ando, **Satoshi Okada**, Takuho Mitsunaga, "Jailbreak Attack on a Multi-Agent LLM Defense System," International Congress on Information and Communication Technology, to appear, 2025.

[2] Rei Watanabe, **Satoshi Okada**, Koki Watarai, Takuho Mitsunaga, "Cloud SecNavigator: RAG Approach to Bridge Gaps and Strengthen Cloud Security Practices with RAGAS Assessment," Proceedings of International Conference on Engineering and Emerging Technologies (to appear),

[3] Taisei Matsumura, **Satoshi Okada**, Koki Watarai, Takuho Mitsunaga, "Explainable Anomaly Detection Method Using LLM Embeddings Model with SHAP," 2024 7th International Conference on Signal Processing and Information Security (ICSPIS). IEEE, pp. 1-5, 2024.

[4] **Satoshi Okada**, Houda Jmila, Kunio Akashi, Takuho Mitsunaga, Yuji Sekiya, Hideki Takase, Gregory Blanc, Hiroshi Nakamura, "XAI-driven Adversarial Attacks on Network Intrusion Detectors," Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference. EICC 2024, pp. 65-73, 2024.

[5] **Satoshi Okada**, Takuho Mitsunaga, "An Improved Technique for Generating Effective Noises of Adversarial Camera Stickers," Proceedings of Eighth International Congress on Information and Communication Technology. ICICT 2024, pp.289-300, 2024.

[6] Momoka Okuma, Koki Watarai, **Satoshi Okada**, Takuho Mitsunaga, "Automated Mapping Method for Sysmon Logs to ATT&CK Techniques by Leveraging Atomic Red Team", 2022 5th International Conference on Signal Processing and Information Security (ICSPIS). IEEE, pp.104-109, 2023.

[7] Konosuke Tamamura, Shun Sakai, Koki Watarai, **Satoshi Okada**, Takuho Mitsunaga, "Detection of XSS Attacks with One Class SVM Using TF-IDF and Devising a Vectorized Vocabulary," 2023 IEEE International Conference on Computing (ICOCO), IEEE, pp.35-40, 2023.

[8] Koshi Ishide, **Satoshi Okada**, Mariko Fujimoto, Takuho Mitsunaga, "ML Detection Method for Malicious Operation in Hybrid Zero Trust Architecture," 2022 IEEE International Conference on Computing (ICOCO), IEEE, pp.264-269, 2022.

[9] Tomoya Oshio, **Satoshi Okada**, Takuho Mitsunaga, "Machine Learning-based Anomaly Detection in ZigBee Networks," 2022 IEEE International Conference on Computing (ICOCO), IEEE, pp.259-263, 2022.

[10] Yosuke Katano, Yukihiro Kozai, **Satoshi Okada**, Takuho Mitsunaga, "Prediction of Infected Devices Using the Quantification Theory Type 3 Based on MITRE ATT&CK Technique," 2022 IEEE International Conference on Computing (ICOCO), IEEE, pp.198-203, 2022.

[11] Masaki Kuwano, Momoka Okuma, **Satoshi Okada**, Takuho Mitsunaga, "ATT&CK Behavior Forecasting based on Collaborative Filtering and Graph Databases," 2022 IEEE International Conference on Computing (ICOCO), IEEE, pp.191-197, 2022. Best paper award.

[12] **Satoshi Okada**, Daisuke Miyamoto, Yuji Sekiya, Hideki Takase, Hiroshi Nakamura, "LDoS Attacker Detection Algorithms in Zigbee Network," International Conferences on Internet of Things (iThings), IEEE, pp.43-50, 2021.

[13] Takuho Mitsunaga, Yoshiki Fujiwara, **Satoshi Okada**, "Proposal for Realization and Improvement of DX in Municipal Services Based on Digital Business Models," International Conference on Computing (ICOCO), IEEE, pp.158-162, 2021.

[14] **Satoshi Okada**, Mariko Fujimoto, Wataru Matsuda, Takuho Mitsunaga, "Malware Detection Method using Tree-based Machine Learning Algorithms," 2021 IEEE International Conference on Computing (ICOCO), IEEE, pp.103-108, 2021.

[15] **Satoshi Okada**, Yoshiki Fujiwara, Mariko Fujimoto, Wataru Matsuda, Takuho Mitsunaga, "Efficient Incident Response System on Shared Cyber Threat Information Using SDN and STIX," 2021 IEEE International Conference on Computing (ICOCO), IEEE, pp.109-114, 2021. Best paper award.

[16] **Satoshi Okada**, Yuntao Wang, "Recovery Attack on Bob's Reused Randomness in CRYSTALS-KYBER and SABER," The 15th International Conference on Provable and Practical Security (ProvSec 2021), Springer LNCS, Vol. 13059, pp. 155-173, 2021.

[17] **Satoshi Okada**, Daisuke Miyamoto, Yuji Sekiya, Hiroshi Nakamura, "New LDoS Attack in Zigbee Network and its Possible Countermeasures," International Conference on Smart Computing (SMARTCOMP), IEEE, pp.246-251, 2021.

[18] **Satoshi Okada**, Yuntao Wang, Tsuyoshi Takagi, "Improving key mismatch attack on NewHope with fewer queries," The 25th Australasian Conference on Information Security and Privacy (ACISP 2020), Springer LNCS, Vol. 12248, pp. 505-524, 2020.

Books

[1] Saho Kobayashi, **Satoshi Okada**, Yu Asabe, Takuho Mitsunaga "はじめて学ぶバイナリ解析 不正なコードからコンピュータを守るサイバーセキュリティ技術", Impress R&D, ISBN: 9784844378495, 2020.