

Ryutaro Nishizaka

Security Researcher · Ricerca Security, Inc.

Email: ryutaro.nishizaka@gmail.com · LinkedIn: www.linkedin.com/in/ryutaro-nishizaka · GitHub: github.com/KuonRuri · Google Scholar: scholar.google.com/citations?user=ZKCKiloAAAAJ · ORCID: orcid.org/0009-0007-9166-8848

Curriculum Vitae

CAREER & EDUCATION

2026/07 – present	Member, 10th Cohort Masason Foundation
2025/04 – present	Organizing Committee SECCON Beginners
2024/07 – present	Part-time Security Researcher Ricerca Security, Inc.
2024/04 – present	Rikkyo Niiza Senior High School
2024/03	Rikkyo Niiza Junior High School Graduated — Honors Award

PUBLICATIONS

Peer-reviewed

DeMeSSAI @ EuroS&P '26 July 2026	How Far Can LLM Agents Go in Binary Exploitation? A CTF-Based Evaluation Ryutaro Nishizaka , Yudai Fujiwara, Yuichi Sugiyama 5th International Workshop on Designing and Measuring Security in Systems with AI, co-located with EuroS&P 2026
IEEE S&P '26 Poster Session May 2026	Poster: Where Do LLM Agents Fail in Binary Exploitation? Yudai Fujiwara, Ryutaro Nishizaka , Yuichi Sugiyama 47th IEEE Symposium on Security and Privacy <u>PDF</u>

SBFT
@ ICSE '26
April 2026

IPSM-Based Test Case Minimization for Network Protocol Implementations

Ryutaro Nishizaka, Kazushi Kato, Yuichi Sugiyama

19th International Workshop on Search-Based and Fuzz Testing (SBFT), co-located with ICSE 2026

[doi:10.1145/3786155.3788580](https://doi.org/10.1145/3786155.3788580)

BAR
@ NDSS '26
February 2026

Towards LLM-Resistant Software Protection: Agent Failure Patterns in CTF Reverse Engineering

Ryutaro Nishizaka, Yudai Fujiwara, Takuya Shimizu, Kazushi Kato, Yuichi Sugiyama

Workshop on Binary Analysis Research (BAR) 2026, co-located with NDSS Symposium 2026

Domestic conferences

CSS 2025
October 2025

Privilege Escalation Attack to RISC-V Keystone TEE via RowHammer

Ryutaro Nishizaka, Hidemasa Kawasaki, Shinya Takamaeda, Soramichi Akiyama

Computer Security Symposium 2025 (CSS) · pp. 1875-1882

CSS Outstanding Paper Award

[IPSJ Library](#)

[CiNii](#)

CSS 2025
October 2025

State-Aware Test Case Minimization for Network Protocol Implementations

Ryutaro Nishizaka, Kazushi Kato, Yuichi Sugiyama

Computer Security Symposium 2025 (CSS) · pp. 937-944

[IPSJ Library](#)

[CiNii](#)

2026

★ Masason Foundation 33 selected nationwide

Selected for the 10th cohort, open to ages 10 to 20.

★ IPSJ 88th National Convention

Received the Best Poster Presentation Award.

BAR 2026

Presented a first-author paper at the Workshop on Binary Analysis Research, co-located with NDSS 2026.

- Towards LLM-Resistant Software Protection: Agent Failure Patterns in CTF Reverse Engineering

SBFT 2026

Presented a first-author paper at the International Workshop on Search-Based and Fuzz Testing, co-located with ICSE 2026.

- IPSM-Based Test Case Minimization for Network Protocol Implementations

DeMeSSAI 2026

Presented a first-author paper at the International Workshop on Designing and Measuring Security in Systems with AI, co-located with EuroS&P 2026.

- How Far Can LLM Agents Go in Binary Exploitation? A CTF-Based Evaluation

2025

★ Computer Security Symposium 2025 (CSS2025) 13 of 270+ papers

Presented two first-author papers. One received the Outstanding Paper Award, as the youngest recipient to date.

- Privilege Escalation Attack to RISC-V Keystone TEE via RowHammer — CSS Outstanding Paper Award
- State-Aware Test Case Minimization for Network Protocol Implementations

★ SecHack365 6 of 30 works

Accepted into the Learning Course (Sakai seminar) and named an Outstanding Graduate.

- Hisame — a fuzzing framework for RISC-V machine-mode firmware

IPSJ 87th National Convention

Poster presentation.

- Evaluating the Feasibility of RowHammer Attacks against Keystone

SECCON Beginners CTF 2025 (CTF4b)

Served on the organizing team and authored three pwn challenges (pivot4b / pivot4b++ / TimeOfControl).

JST GSC Experts in Information Science

Completed the second stage.

Media coverage

A second interview featured on the school website.

- A School that Fosters the Power to Pioneer: High School Student × Teacher Dialogue — Learning at Rikkyo Niiza

2024

★ CognitiveHack Japan 2024

Champion in both the Junior Division and the Junior School Division.

JST GSC Experts in Information Science

~40 selected nationwide

Selected for the 5th cohort; completed the first stage.

Japanese Olympiad in Informatics

Qualified for the final round.

Machine Learning Specialization

Completed.

UK-Japan Young Scientists Workshop

Completed.

2023

★ Registered Information Security Specialist

Passed the examination at the youngest age on record and registered as a specialist.

Security Camp National Convention

Completed Class C (Threat Analysis).

Security Mini Camp in Tokyo

Completed Track C (Malware Analysis).

Media coverage

Featured on the school website.

- Youngest to Pass the Information Processing Security Support Specialist Examination — Aiming to Contribute to Society through Cybersecurity

CERTIFICATIONS

- Registered Information Security Specialist — Registration No. 026794
- Applied Information Technology Engineer