

KAIXUAN LUO

✉ kaixuan@ie.cuhk.edu.hk · 🏠 <https://kaixuanluo.me>

Research Interests: My research focuses on **web security** and its intersection with **digital identities**. Lately, I have been investigating authorization issues in emerging ecosystems and architectural patterns such as Agentic AI. Grounded in my research on OAuth security, I lead standardization efforts to update OAuth security best practices in the IETF.

🎓 EDUCATION

The Chinese University of Hong Kong (CUHK), Hong Kong SAR, China 2022 – 2027

PhD Candidate, Department of Information Engineering (IE)

- GPA: 3.91/4.00
- Supervisor: Prof. Wing Cheong LAU

Huazhong University of Science and Technology (HUST), Wuhan, China 2018 – 2022

BEng in Information Security, School of Cyber Science and Engineering (CSE)

- GPA: 3.92/4.00; TOEFL: 114/120; Graduation with Honorary Degree (Top 3%)
- Supervisor: Prof. Ming WEN

📖 PUBLICATIONS

[1] Demystifying the (In)Security of OAuth-based Account Linking in Connector Ecosystems

📌 Acknowledgments from MICROSOFT, AMAZON, BYTEDANCE, N8N
[Kaixuan Luo](#), Xianbo Wang, Pui Ho Adonis Fung, Wing Cheong Lau
To appear in the 47th IEEE Symposium on Security and Privacy (S&P), May 2026
Acceptance Rate: 253/1,995 = 12.7%.

[2] Universal Cross-app Attacks: Exploiting and Securing OAuth 2.0 in Integration Platforms

📌 Acknowledgments from MICROSOFT, GOOGLE, AMAZON, OPENAI; CVE-2023-36019 (CVSS: 9.6)
[Kaixuan Luo](#), Xianbo Wang, Pui Ho Adonis Fung, Wing Cheong Lau, Julien Lecomte
In the 34th USENIX Security Symposium, August 2025.
Acceptance Rate: 407/2,385 = 17.1%.

[3] SWIDE: A Semantic-aware Detection Engine for Successful Web Injection Attacks

Ronghai Yang, Xianbo Wang, [Kaixuan Luo](#), Xin Lei, Ke Li, Jiayuan Lin, Wing Cheong Lau
In Procs. of ACM Conference on Computer and Communications Security (CCS), October 2024.
Acceptance Rate: 328/1,964 = 16.7%.

[4] Living a Lie: Security Analysis of Facial Liveness Detection Systems in Mobile Apps

Xianbo Wang, [Kaixuan Luo](#), Wing Cheong Lau
In International Conference on Applied Cryptography and Network Security (ACNS), March 2024.
Acceptance Rate: 54/230 = 23.5%.

[5] Effective Isolation of Fault-Related Variables via Statistical and Mutation Analysis

Ming Wen, Zifan Xie, [Kaixuan Luo](#), Xiao Chen, Yibiao Yang, and Hai Jin
In Transactions on Software Engineering (TSE), 2023.

📖 STANDARDIZATION

Updates to OAuth 2.0 Security Best Current Practice

Tim Würtele, Pedram Hosseyni, [Kaixuan Luo](#), and Adonis Fung
draft-ietf-oauth-security-topics-update-01, **IETF Internet-Draft**. Work in Progress, March 2026.

INDUSTRY TALKS

IETF 125 Updates to OAuth 2.0 Security Best Current Practice	March 2026 Shenzhen, China
Black Hat USA 2025 Back to the Future: Hacking and Securing Connection-based OAuth Architectures in Agentic AI and Integration Platforms	August 2025 Las Vegas, USA
Black Hat USA 2024 One Hack to Rule Them All: Pervasive Account Takeovers in Integration Platforms for Workflow Automation, Virtual Voice Assistant, IoT, & LLM Services	August 2024 Las Vegas, USA
Black Hat USA 2023 (Co-speaker) The Living Dead: Hacking Mobile Face Recognition SDKs with Non-Deepfake Attacks	August 2023 Las Vegas, USA
OAuth Security Workshop 2026 Understanding OAuth Session Fixation in Connector Ecosystems	May 2026 Leipzig, Germany
OAuth Security Workshop 2025 Cross-app OAuth Attacks in Integration Platforms: Mix-up Attacks Reloaded	February 2025 Reykjavík, Iceland

INTERN EXPERIENCE

Samsung Research America Security Analysis and Engineering of Samsung's AI Assistant, Bixby	Summer 2023 & 2024 Mountain View, USA
Sangfor Technologies Symbolic Execution for Web Shell Detection	December 2021 - April 2022 Shenzhen, China

SERVICES

ACM CCS, Artifact Evaluation Committee	2025
USENIX Security, Artifact Evaluation Committee	2025, 2026

AWARDS

• IEEE S&P Student Travel Grant	2026
• ACM CCS Top Artifact Reviewers Award	2025
• USENIX Security Distinguished Artifact Reviewer Award	2025
• HKSAR Reaching Out Award	2025
• National Scholarship (Top 0.2% Nationwide)	2021
• National College Student Information Security Contest – Capture the Flag (CTF)	2nd Prize, 2019 & 2020

TEACHING ASSISTANT

FTEC5640	Decentralized Finance	Spring 2026
IERG2080	Introduction to Systems Programming	Spring 2025
IERG4130	Introduction to Cyber Security	Fall 2024
IERG4004	E-payment Systems and Cryptocurrency Technologies	Spring 2024
IERG4300	Web-Scale Information Analytics	Spring & Fall 2023, Fall 2025
ENGG1110	Problem Solving By Programming	Fall 2022