YuXin (Myles) Liu

yuxin.liu@uci.edu
https://www.ics.uci.edu/~yuxil11/ | https://www.linkedin.com/in/mylesliu/

EDUCATION

Doctor of Philosophy in Computer Science June 2020 – June 2026 (expected)
Working in Trustworthy Systems Lab (TrussLab) (https://trusslab.github.io/)
Advised by Professor Ardalan Amiri Sani (https://www.ics.uci.edu/~ardalan/)
Recipient of *UCI CS Rising Star Award*
University of California, Irvine

Bachelor of Science in Computer Science; Minor in Japanese September 2016 - March 2020
Specialized in Intelligent Systems
ICS Honors Program
University of California, Irvine

RESEARCH INTEREST & SUMMARY

"Seeing is believing". My thesis research focuses on restoring people's trust towards digital media in this world that is full of AI-generated photos and videos. I architect and build systems that establish verifiable digital provenance, creating a secure "chain of custody" from capture to consumption. I firmly believe that provenance is the key for people to regain trust in the AI era. This principle is also essential beyond media; for instance, it is critical for ensuring the reliability of large language and vision models in high-stakes applications such as autonomous driving. My work spans the full stack, from low-level hardware sensor interfaces to high-level machine learning applications, enabling me to design holistic solutions for all types of trustworthy intelligent systems.

RESEARCH EXPERIENCE

ProvStream: Providing Practical Provenance for Online Conferencing

- A webcam providing practical provenance for both video and audio in real-time online conferencing.
- Project in progress.

Patchlings: Safety-Preserving Persistent Hotpatching of Automotive Microcontrollers via Static Trampolines

- A novel hotpatching system designed specifically for mission-critical real-time embedded devices such as automotive ECUs.
- Maintain both functional and timing safety when applying patches and significantly reduce amount of effort needed for update verification.
- Persistent hotpatching that survives system resets while maintaining robustness and predictability.
- Collaboration project with Bosch Research, with a paper under submission to USENIX Security 2026.

Data Passport: Confidentially Provable Provenance for Onboarding Verifiable ML

- Introduce tamper-proof Data Passports that bind data to verifiable and confidential proofs of authenticity.
- Use zero-knowledge proof to verify the validity of the passports.
- Unlock cryptographic verification of data provenance throughout the ML pipeline.
- Paper to be submitted to CCS 2026.

YuXin (Myles) Liu

yuxin.liu@uci.edu

https://www.ics.uci.edu/~yuxil11/ | https://www.linkedin.com/in/mylesliu/

Scoop: Mitigation of Recapture Attacks on Provenance-Based Media Authentication

- Realize an attack specifically targeting a modern provenance-based camera, where attackers use such a camera to capture fake footage displayed on flat surfaces such as TV, effectively authenticating them with provenance.
- A novel system that points out suspicious surfaces by processing both depth map generated with a depth sensor and depth map generated with monocular depth estimation ML model.
- A comprehensive dataset to be used to evaluate systems like ours.
- Paper accepted to USENIX Security 2025; invited by ACM SIGMOBILE to be featured as a research highlight for ACM *GetMobile*.

Coral: A Physically-Isolated TEE Design with High Performance and Utilization

- A novel TEE that provides much stronger security guarantee while maintaining the same (and sometimes better) level of performance.
- A complete Xilinx FPGA based system prototype with custom IP designs.
- Paper submitted to MobiSys 2026.

UnderRansom: A Robust and Practical Way to Tackle Ransomware in OS Kernel

- Detecting and mitigating ransomware in real time in OS kernel by monitoring I/O related system calls and dynamically scanning process's memory.
- A working Linux loadable kernel module prototype, evaluated against various ransomwares.
- Project done at Bosch Research internship in Summer 2024, with two patents written.

ProvCam: A Camera Module with Self-Contained TCB for Producing Verifiable Videos

- Securing both data and control planes of the camera/video pipeline without having a bloated TCB, where videos' authenticity is protected by cryptographic proof.
- A complete Xilinx FPGA based system prototype with custom IP designs.
- Paper accepted to MobiCom 2024.

Vronicle: A System for Producing Videos with Verifiable Provenance

- A verifiable system flow of both capturing and post-processing videos using TrustZone/SafetyNet and Intel SGX.
- Paper accepted to MobiSys 2022. (Best Poster Award Runner-up)

Tabellion: Secure Legal Contracts on Mobile Devices

- A secure contract signing system specifically designed for mobile devices using TrustZone and Intel SGX.
- Paper accepted to MobiSys 2020.

PUBLICATIONS

Scoop: Mitigation of Recapture Attacks on Provenance-Based Media Authentication
USENIX Security 2025
(Also featured as a research highlight in ACM *GetMobile*)
Yuxin (Myles) Liu, Habiba Farrukh, Ardalan Amiri Sani, Sharad Agarwal, Gene Tsudik

ProvCam: A Camera Module with Self-Contained TCB for Producing Verifiable Videos

YuXin (Myles) Liu

yuxin.liu@uci.edu
https://www.ics.uci.edu/~yuxil11/ | https://www.linkedin.com/in/mylesliu/

ACM MobiCom 2024
Yuxin (Myles) Liu, Zhihao (Zephyr) Yao, Mingyi Chen, Ardalan Amiri Sani, Sharad Agarwal, Gene Tsudik

Vronicle: A System for Producing Videos with Verifiable Provenance
ACM MobiSys 2022 (Best Poster Award Runner-up)
Yuxin (Myles) Liu, Yoshimichi Nakatsuka, Ardalan Amiri Sani, Sharad Agarwal, Gene Tsudik

Tabellion: Secure Legal Contracts on Mobile Devices
ACM MobiSys 2020
Saeed Mirzamohammadi, Yuxin (Myles) Liu, Tianmei Ann Huang, Ardalan Amiri Sani, Sharad Agarwal, Sung Eun (Summer) Kim

WORK & TEACHING EXPERIENCE

Donald Bren School of Information and Computer Sciences June 2020 – Present
Graduate Student Researcher

Robert Bosch LLC June 2025 – Present
Automotive Security Intern

Robert Bosch LLC June 2024 – September 2024
Security Researcher

Donald Bren School of Information and Computer Sciences September 2023 – December 2023
Teaching Assistant
- Responsible for leading discussions and grading projects. (Computer System Architecture)

Donald Bren School of Information and Computer Sciences March 2022 – June 2022
Teaching Assistant
- Responsible for leading discussions, giving office hours, guest lectures, and grading projects. (Database & Web Apps Projects)

Donald Bren School of Information and Computer Sciences March 2021 – June 2021
Teaching Assistant
- Responsible for leading discussion sessions, designing and grading homework/projects/quizzes. (Advanced C++)

UCI ICS Honors Research Program December 2018 – March 2020
Undergraduate Student Researcher

Donald Bren School of Information and Computer Sciences January 2017 – December 2017
Lab Tutor
- Tutoring sessions include homework, project, and quiz help for Python and C++.

SERVICES

◊ ACM SAC 2026 (Program Committee)
◊ ACM MobiSys 2025 (Local Arrangement Chair)

YuXin (Myles) Liu

yuxin.liu@uci.edu

https://www.ics.uci.edu/~yuxil11/ | https://www.linkedin.com/in/mylesliu/

- ◊ ACM SAC 2025 (Program Committee)
- ◊ UCI Security Seminar 2024-2026 (Student Lead)
- ◊ IEEE Transactions on Computers (Reviewer)
- ◊ ACM HotMobile 2023 (Helper)

Honors & Awards

- ◊ UCI CS Rising Star Award (2026)
- ◊ USENIX Security 2025 Student Grant
- ◊ ACM HotMobile 2023 Student Travel Grant
- ◊ ACM MobiSys 2022 Student Travel Grant
- ◊ UCI ICS Honors Program (2018-2020)
- ◊ UCI SURP Fellow (2019)
- ◊ UCI Dean's Honor List (2016-2020)

SKILLS

Technical

Programming: Proficient in C/C++, Java, Python, Verilog.
Experience with Kotlin, Swift, PHP, MySQL, Assembly, HTML, CSS, JavaScript, C#.

Others: Intel SGX, ARM TrustZone, Linux Kernel, Android System (AOSP), FPGA (Xilinx), FreeRTOS, ZephyrOS.

Language

Proficient in Chinese (Native); Professional Japanese (JLPT N1).