Yaxuan(Alice) Wen

370 Jay St. 10th Floor, Brooklyn NY, 11201

(+1)917-834-5595 | yaxuan.w@nyu.edu | alicewyx.me | Yaxuan-w

Research Interest

Compilation Security, Software Supply Chain Security, System Security

Education

New York University *Brooklyn, NY*
Ph.D. in Computer Science *Aug 2024 – Present*

- Advisor: Prof. Justin Cappos
- Research Interest: Compilation Security, Supply Chain Security, Operating Systems

New York University *Brooklyn, NY*
M.Sc. in Cybersecurity *Aug 2022 – May 2024*

- Advisor: Prof. Justin Cappos
- Research Interest: Supply Chain Security, Reproducible Build, System Security

Pennsylvania State University *State College, PA*
B.Sc. in Computer Science *Aug 2017 – May 2021*

Projects

TriSeal: A Verifiable Compilation System
Research Lead

- Designing and implementing *TriSeal*, a secure build system that minimizes the horizontal trusted computing base to three auditable components: Intel SGX, a minimal syscall-less runtime, and a user-specified compiler.
- Enclosing the entire build process within a non-interactive, confined SGX environment that allows only controlled input/output syscalls, achieving full runtime isolation from the host.
- Addressing the limitations of reproducible builds by enforcing deterministic behavior within an enclave-confined environment, resilient to adversarial influence.

3i: An Inter-Cage Interposition Interface for System Call Routing
Research Lead

- Designed and implemented 3i, a modular interposition framework in the Lind project for routing system calls and inter-cage communication by controlling syscall jump targets.
- Integrated with existing "cage" abstractions, lightweight, memory-isolated compartments within a process that enable secure execution of legacy code (with with minimal source code changes if needed).
- Introduced *Grate* abstraction to encapsulate and monitor cages externally, enabling syscall filtering and introspection without modifying the kernel or microvisor.
- Converted file system and RPC-related syscalls into lightweight user-space function calls, reducing context switches and performance overhead, and reducing the attack surface of system call routing.

Lind-Project
Research Assistant

- Designed and implemented *RawPOSIX*, a full Linux system call interface in Rust for the Lind runtime, an intra-process communication platform which runs on existing hardware as an unprivileged Linux process that executes legacy applications.
- Evaluated system performance across three configurations: native Linux, Lind with full runtime, and RawPOSIX-only syscall interface, by developing and running automated microbenchmarks and LAMP workloads.

Academic & Professional Experience

Secure Systems Lab, New York University *Brooklyn, New York*
Research Assistant *May 2023 – Present*

- Working on compilation security, software supply chain security, and operating systems. All projects are open source projects.

Institute of Software, Chinese Academy of Science and Technology *Beijing, China*
Research Assistant *June 2021 – Feb 2022*

- Implemented a network simulation environment to model Software-Defined Networking (SDN) behavior under multi-user conditions.

Teaching Experience

Feb 2024 **Guest Lecture,** Advanced CS Topic: Supply Chain Security *NYU*

Invited Talks

Feb 2025 - Caging: An Abstraction For Finer-grained Isolation *NESysDay*