Ping-Jui Liao

(541) 829-2714 pingjuiliao@gmail.com
Website: **www.ping-jui.com**
LinkedIn: www.linkedin.com/in/ping-jui-liao-73636b195

Education

M.S in Computer Science, School of Electrical Engineering and Computer Science
Oregon State University, Corvallis, Oregon — Jan 2018 - Present (Expected Completion: Mar 2024)

- Research: Automated vulnerability discovery, building Software Defense mechanism
- Coursework: System Security, Operating System

Ph.D. in Computer Science, School of Electrical Engineering and Computer Science
Oregon State University, Corvallis, Oregon — Jan 2018 - Present (Not Pursuing Completion)

Bachelor of Science in Computer Science, Department of Science
National Chengchi University, Taipei, Taiwan — Sep 2011 - Jun 2016

Work Experience

Oregon State University — **Corvallis, Oregon**
Graduate Research Assistant — Sep 2019 - Present

- Led the development of advanced memory corruption attack mitigation techniques, bolstering system security and resilience
- Conducted a comprehensive evaluation of the fuzzing outcomes from the Cyber Grand Challenge (CGC), an extensive set of binary benchmarks designed to emulate real-world common errors

Sony Interactive Entertainment — **San Mateo, California**
Software Development Engineer Intern — Jun 2022 - Sep 2022

- Engineered the script for continuous operation, automating vulnerability discovery and ensuring uninterrupted security testing within software libraries
- This proactive approach led to the early detection and mitigation of potential vulnerabilities, strengthening the organization's cybersecurity defenses
- Established a reporting system that generated detailed reports and real-time alerts upon identifying vulnerabilities, facilitating rapid response and remediation

Projects

Sensitive Pointer Integrity Sanitizer — Jul 2023 - Sep 2023

- Constructed an LLVM sanitizer designed to mitigate control-flow hijacking attacks by maintaining shadow copies of sensitive pointers in both C and C++
- Achieved a low overhead performance on the SPEC CINT2006 benchmark, all while maintaining compatibility with contemporary security measures like Address Space Layout Randomization (ASLR)

Showcase Dynamic Website — Mar 2023 - Jun 2023

- Established a Python Flask-based markdown service with Nginx, adhering to RESTful API principles and the Model-View-Controller (MVC) framework
- Incorporated database interface abstraction and Docker-compose into the service to enhance flexibility and portability

Fuzz Testing Integration Framework — Sep 2022 - Jan 2023

- Created a versatile fuzzing framework that optimizes workflow by seamlessly integrating diverse research prototype fuzzers and maximizing efficiency through the reuse of partial algorithms
- Designed and implemented a user-friendly interface for the fuzzing framework, utilizing object-oriented programming design patterns to enhance code reusability, flexibility, and maintainability

State-aware Fuzzer — Jul 2020 - Sep 2021

- Engineered a low-level mechanism to instrument test programs, enabling comprehensive state reporting and thereby improving test coverage
- Adapted the C-based American Fuzzy Lop (AFL) fuzzer to extract feedback from the previously instrumented code, guiding AFL's genetic algorithm towards exploring deeper program paths

Shadow Stack — Jun 2020 - Sep 2020

- Developed a compiler extension utilizing the LLVM framework to enhance memory safety in a low-level programming language by creating isolated memory regions to protect return addresses

Multi-architecture and Multi-OS Shellcode — May 2018 - Jun 2018

- Created a unified program capable of launching shells on various operating systems, including MacOS and Linux, across both x86_64 and ARM64 computer architectures
- Crafted a portable exploit in Sigreturn Oriented Programming (SROP) utilizing the previously mentioned shellcode

Skills

Programming Language: C, C++, Python, Swift, Solidity, Rust, R, Objective-C, C#, Javascript, Java, Go, X86, ARM
Web development: Node.js, Django, Express.js, Flask, MySQL, MariaDB, MongoDB, SQLite, SQLAlchemy, AWS, DynamoDB, AWS EC2, AWS S3, HTML, CSS, jQuery, Bootstrap
Operating Systems: Linux, Kernel Debugging, QEMU
Open Sources: LLVM, CodeQL, CMake, OpenMP, OpenGL, CUDA, Google Test, z3, Docker, Docker-compose, Jenkins
CTF: DamCTF2023 8th place (Team OSUSEC), Pwnable.tw Rank 452
Online Courses: Advanced Compilers (Cornell University), Software Analysis (University of Pennsylvania), Cryptography I (Stanford University, Coursera)