Zhuo Ying Jiang Li

zyj20 [at] cl.cam.ac.uk GitHub ID: RoundofThree

Education

University of Cambridge, Cambridge, UK 10/2023 – 06/2026 (expected)

PhD in Computer Science, focusing on vulnerability research and adversarial analysis in CHERI software.
Thesis proposal: *The Art of Exploitation in CHERI-Enabled Systems and Applications*

University of Cambridge, Cambridge, UK 10/2022 – 06/2023

MPhil in Advanced Computer Science. Graduated with First Class (Distinction).

King's College London, London, UK 09/2019 – 06/2022

BSc Computer Science. Graduated with First Degree with Honours.

Selected Projects

Syzkaller: Kernel fuzzing for CheriBSD 07/2024 - 09/2024

- Ported syzkaller to fuzz CheriBSD pure-capability kernel in Arm Morello. Arm Morello is a prototype System-on-Chip (SoC) with a CHERI-extended ARMv8-A processor.
- Added support to syzkaller for fuzzing bluetooth, netlink and netgraph kernel subsystems.
- Found several security bugs applicable to FreeBSD, conducted an analysis of them, and wrote proof-of-concept triggers. One bug is pending a security advisory.
- Worked in a dynamic two-person team, contributing ideas and fostering a collaborative environment.

AFL++ for CheriABI 11/2024 - Ongoing

- Ported AFL++ to CheriABI. Specifically, LLVM PCGUARD instrumentation.
- Set up fuzzing harnesses for userspace programs in CheriABI. Work in progress.

CHERI+ASan: AddressSanitizer for CheriABI 09/2024 - 12/2024

- Ported LLVM AddressSanitizer (ASan) runtime to CheriABI in CheriBSD Arm Morello. The goal is to enhance sanitization performance and effectiveness by combining deterministic spatial safety detection of CHERI and redzone-based temporal safety detection of ASan.
- Ported Kernel AddressSanitizer (KASAN) to CheriBSD pure-capability kernel in Arm Morello.
- Improved KASAN memory corruption detection in CheriBSD by implementing kernel allocation quarantining and redzone padding. Also applicable to FreeBSD.

Damn Vulnerable Kernel Module for CheriBSD 04/2024 - Ongoing

- Developed a tool that provides a flexible way to inject exploitation primitives in a controlled adversarial experiment, which serves as a swiss army knife for demonstrating and evaluating exploitation techniques with controlled attacker capabilities.

Open-source Binary Analysis Tools for the Morello Architecture 11/2023 - Ongoing

- Developed Ghidra Software Reverse Engineering suite Arm Morello architecture extension.
- Developed GEF (GDB Enhanced Features) with Morello support: GDB plugins with visualisation commands of the heap state and program states.
- Developed Unicorn Engine with Morello support: scriptable CPU emulation library based on QEMU and with Python bindings.

Validation of CHERI IR Security Properties in LLVM Optimization Passes 11/2022 - 06/2023

- Proposed the CHERI Alive2 IR semantics model, modified from the Alive2 IR semantics model to conform to the CHERI C memory model assuming a purecap CheriABI runtime. The CHERI Alive2 IR semantics model has modified semantics for capability operations and memory accesses through capabilities as well as new undefined behaviour cases related to CHERI exceptions.
- Implemented the CHERI Alive2 fork of Alive2 that adds support for CHERI intrinsics and attributes emitted by the Morello LLVM compiler, replaces the pointer type to the capability type in the underlying SMT encoding and models the proposed CHERI LLVM IR semantics and refinement checks.
- Modified two compiler fuzzers to generate less conservative random programs in C and LLVM IR that cover pointer operations, pointer escaping, memory operations and CHERI-specific intrinsics and builtins.

TASO-TVM: A Multi-Platform Tensor Algebra SuperOptimizer for Deep Learning 11/2022 - 1/2023

- Designed a architecture that integrates the TVM backend to the TASO superoptimizer.
- Implemented the kernels and their cost model using AutoScheduler.
- Evaluated the runtime performance of deep learning networks (BERT, NasRNN) using the autoscheduled kernels on different architectures (Metal, CUDA and CPU).

Experience

CTF competitions

- I mostly solve binary exploitation and reverse engineering challenges with the *cheriPI* team at Cambridge. Some of the CTFs I have attended are PwnEd Qualifiers and Finals CTF, LakeCTF Qualifiers and Finals, CSAW, HackTheBox University CTF, Country2Country.

Cambridge Cyber Security Society committee member

- Organised socials to engage with other university members who are also into systems and security.
- Proposed ideas and organised academic workshops to foster interest into practical adversarial exploration and CHERI.

Skills

Programming Languages: C/C++, Python.
Others: LLVM compiler hacking, UNIX kernel development, vulnerability research, reverse engineering, gdb.