Zhuo Ying Jiang Li

zyj20 [at] cl.cam.ac.uk

Education

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

PhD in Computer Science. 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. Qualification: First Class

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

BSc Computer Science. Qualification: First Degree with Honours

IES Son Pacs, Balearic Islands, Spain 09/2017 – 06/2019

International Baccalaureate. Grade: 45/45, Extended Essay (Maths): A

Selected Projects

Proofs-of-concept of Past Vulnerabilities in the CheriBSD Kernel 02/2024 - Ongoing

- Maintaining a framework of exploit primitives and their preconditions given CHERI-based security mitigations.
- Maintaining a vulnerable fork of the CheriBSD kernel with backpatched real-world vulnerabilities.
- Developed individual *proofs-of-concept* programs to prove the feasibility of exploitation techniques against the CheriBSD kernel given constraints.

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.
- Proposed the concept of *security refinements* and showed its relevance in validating the preservation of security semantics.
- 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.

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 Qualification and Finals CTF, LakeCTF Qualification and Finals, CSAW, HackTheBox University CTF, Country2Country.

Cambridge Cyber Security Society

- 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.