Zhuo Ying Jiang Li

zyj20 [at] cam.ac.uk

Education

University of Cambridge, Cambridge, UK 10/2022 – 06/2023 (expected)

MPhil in Advanced Computer Science: *Advanced Topics in Computer Architecture, Advanced Operating Systems, Computer Security: Principles and Foundations, Principles of Machine Learning Systems, Mobile Health*

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

Qualification: First Degree with Honours
BSc Computer Science: *Information Security, Cryptography, Operating Systems, Internet Systems, Compilers, Foundations of Computing (Maths), C++ for algorithms and data structures, Optimization Methods, Artificial Intelligence*

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

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

Selected Projects

Security implications on CHERI semantics of LLVM optimization passes 11/2022 - Ongoing

- Define CHERI C semantics and identify the CHERI-related invariants/properties.
- Provide a thorough analysis and testing of LLVM optimization passes in the current CHERI LLVM fork, focusing on functional and security semantics preservation. In case CHERI security guarantees are violated, propose a proof of concept and workarounds if it is feasible.
- Propose and test new optimization passes and/or modify existing optimization passes which exploit CHERI invariants to improve performance.
- Evaluate performance and code size of each optimization pass and evaluate on real-world applications (Nginx, maybe OpenSSL) under different optimization levels.

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).

Targeted and targeted backdoor poisoning attacks against Drebin under problem-space derived constraints 11/2021 - 04/2022

- Presented and implemented a custom gradient-based attack algorithm in Python to perform targeted attacks under previously identified feature-space constraints for Drebin.
- Adapted the *watermarking* targeted backdoor attack method, proposed in a paper about image classification backdoor attacks, to Drebin. Implemented the backdoor attack using the genetic algorithm with greedy heuristics.
- Evaluated and compared the different poisoning attack approaches, both targeted and targeted backdoor attacks, using the presented algorithms, to attack Drebin.

Regular expression matcher, lexer, parser and LLVM compiler front-end 09/2021

- Derived and proved the correctness of the Brzozowski derivatives for extended regular expression operations.
- Implemented the Brzozowski algorithm in a functional language (Scala).
- Implemented the Sulzmann & Lu algorithm as an extension for regular expression lexing (Scala).
- Implemented a parser and a compiler front-end that emits code in SSA form (LLVM-IR).

Experience

CTF competitions

- Solved mostly reverse engineering challenges and some pwn challenges. Some of the CTFs I have attended are PwnEd CTF Quals and Finals 2022, LakeCTF Quals and Finals 2022, CSAW Quals 2022, Maple CTF 2022, HackTheBox University CTF 2021.

GIAC Hacker tools, techniques, exploits and incident handling training, SANS Institute Remote

- Studied in detail defensive and offensive operations in internal networks

Student Representative King's College London

- Co-chaired the Student Staff Liaison Committee (SSLC)
- Collected student feedback and discussed solutions with university staff
- Proposed ideas and organised events to improve the learning environment of the student community

Selected Awards

- Alan Fairbourn Memorial Prize (most meritorious Final Year Project in the Department of Informatics) 2022
- Undergraduate Informatics BSc Finalist Prize (best performance during the final year of the BSc Computer Science programmes) 2022
- Undergraduate Informatics Top-Performing Graduate (best overall performance over the duration of study in the Department of Informatics for an undergraduate finalist) 2022
- GIAC Advisory Board member (top performance) 2020
- Undergraduate Informatics Year 1 or Year 2 Prize (best performance) 2020
- Silver Prize, Iberoamerican Olympiad in Chemistry 2019
- Silver Prize, National Olympiad in Chemistry 2019
- Silver Prize, National Olympiad in Physics 2019

Skills

Programming Languages: Python, C++, C, Golang, Rust, Scala, JavaScript, Java, Ruby.
Others: LLVM, binary exploitation, reverse engineering, program analysis