JUNZHEN LOU

CS Master student at ETH Zürich – EPFL

Vesper_Lou@outlook.com 41-765358162

EDUCATION

M.S. Computer Science Major in Cyber Security, joint degree **ETH Zürich - EPFL** 09/2021 - present

✓ **GPA**: 5.3/6.0

Postgrad. Computer Vision, **Institute of Artificial Intelligence and Robotics**, XJTU 09/2020 - 06/2021

B.E. Automation, **School of Electronic and Information Engineering**, XJTU 09/2016 - 06/2020

Honors Youth Program, Qian Xuesen Honors College, XJTU 08/2014 - 06/2020

SKILLS

- Data structures and algorithms;
- Programming languages: **C++/C**, **Golang**, **Python**, SQL, Rust, Move;
- Data and systems: distributed systems, distributed storage/computing, database systems, microarchitecture;
- Security and privacy: network security, cryptography, Multi-Party Computation, confidential computing;
- Frameworks/tools and others: **Linux**, **Git**, **Docker**, **Kubernetes**, Azure, Jupyter, PostgreSQL, NoSQL, REST API, Clang, GCC, XML, JSON, Matlab, Sage, PyTorch, TensorFlow.

PATENTS

A Fast Similarity Detection and Evidence Generation Method for Large-scale Programs Based on Code Mapping and Lexical Analysis, *China National Intellectual Property Administration*, ID: ZL 2018 1 1237212. 6, 08/18/2018.

EXPERIENCE

CYSEC: Software Engineer Intern, Full-stack 02/2023 - present

- Optimize/implement workflow and control panel of vulnerability aggregator, and product lifetime tracker.

PROJECTS & RESEARCH

Peerster: A Distributed Gossip-Based Peer-to-Peer Network Application (Go) 09/2022 - 01/2023

- Implemented basic architecture: UDP-based socket, routing scheme, unicast, and messaging mechanism;
- Implemented **broadcast** functionality, with rumor-mongering and anti-entropy mechanism;
- Implemented data sharing scheme: data upload/download, **asynchronous notification**, and file searching;
- Implemented **Multi-Paxos** protocol: Paxos consensus, state machine, and blockchain storage;
- Designed and implemented **Secure Multi-Party Computation** (MPC) with **permissioned blockchain**.

A Fast Implementation of Data Valuation with Shapley Value and KNN (C++) 03/2022 - 06/2022

- Conducted cost analysis and **cache miss analysis** of original and improved algorithms;
- Implemented scalar optimizations and **SIMD optimizations** to reach an **8x** speedup;
- Created and analyzed performance plots, and evaluated the tighter roofline based on instruction mix.

Cryptography Attacks: "Capture the Flag" (Python) 03/2022 - 06/2022, 09/2022 - 12/2022

- Implemented padding oracle attacks against AES in different modes;
- Studied and implemented Lattice-based attacks against RSA encryption;
- Devised Key Overwriting attack against given system with public-key encryption.

Prof. Ting Liu, Ministry of Education Key Lab for Intelligent Networks and Network Security *2017 - 2019*

Software Target Code Plagiarism Detection and Visualization of Evidence Generation 2017 - 2019

- Contributed to the improvement of DYKIS algorithm, and analyzed key instructions with data flow;
- Conducted experiments on different compilers to test algorithm accuracy;

A Personal Doctor for Software: An All-Round Automatic Operation and Maintenance System 2018 - 2019

- Improved algorithm to eliminate less influential variables, tested the vulnerability scanner of binaries;
- Propelled our research direction towards an intelligent, effective screening system of user comments.

AWARDS

Silver, Gold Award of China College Student Innovation and Entrepreneurship Competition 09/2019, 08/2018

Gold Award of 2018 MIT International Genetic Engineering Machine Competition (**iGEM**) 10/2018

Excellence Award of XJTU Mathematical Contest in Modeling (MCM) 05/2017