Qiao Zhang

Hangzhou, Zhejiang Province, China
Email: j0k1ng@zju.edu.cn

Education

Chu Kochen Honors College (CKC), Zhejiang University (ZJU) Expected graduation date: Jun. 2024

- Bachelor of Science in Computer Science and Technology | *GPA: 3.32/4.0, 80.17/100* Sept. 2020 - Ongoing
- Major Coursework: Linear Algebra (H), Mathematical Analysis, Operating System, Object-Oriented,Programming (C++), Computer Architecture, Database Systems, Advanced Data Structures and Algorithm Analysis.

Publications

- Chong Fu, Yuwen Pu, **Qiao Zhang**, Jiayu Pan, Jing Qiu, Xuhong Zhang, Yiming Wu, and Shouling Ji, *SecretKeeper: Robust Vertical Federated Learning Against Label Inference Attacks*, **NSE 2023**.
- Shouling Ji, Oubo Ma, **Qiao Zhang**, Xuhong Zhang, Jiayu Pan, Yuwen Pu, Jian Shen, Li Jiang, Yingjie Zhou, and Xing Yang. 2023. *Adversarial Policy Attacks on Partially Observed Multi-Agent Reinforcement Learning Systems*. CN Patent Application 2023114363141, filed November, 2023. **Patent Pending**
- Boyu Chang, **Qiao Zhang**, Binbin Zhao, Yuan Tian, and Shouling Ji, *Fuzzing Is Not The End: Efficient Fault Localization in ARM IoT Firmware*, **CCS 2024** (*in submission*).

Research Experience

Knowledge-driven Fuzzing Mutation Strategy Scheduling Method
In-depth scientific research training, CKC, ZJU | The NESA Lab, ZJU Jun. 2022 - Dec. 2022
Advisor: Professor Shouling Ji, College of Computer Science and Technology, ZJU

- The advisor team introduced a novel mutation scheduling scheme, MOPT, enhancing the efficiency of mutation-based fuzzers in discovering vulnerabilities. Contributed to the project by gaining insights into MOPT during the research and devising an enhanced mutation operator to further elevate its effectiveness.

Adversarial Policy Attacks on Partially Observed Multi-Agent Reinforcement Learning Systems
The NESA Lab, ZJU Jun. 2022 - Dec. 2022
Advisor: Professor Shouling Ji, College of Computer Science and Technology, ZJU

- Proposed a novel black-box attack (called SUB-PLAY) against partially observable MARL in competi-tive environ-ments.Introduced the concept of con-structing multiple subgames to mitigate the impact of partial observability and suggests the sharing of transitions among subpolicies to improve the exploitability.

SecretKeeper: Robust Vertical Federated Learning Against Label Inference Attacks
The NESA Lab, ZJU Jun. 2022 - Jul. 2023
Advisor: Professor Shouling Ji, College of Computer Science and Technology, ZJU

- Proposed the first defense for split-learning-based Vertical Federated Learning (VFL) against label inference attacks to bridge the gap that existing defenses are designed for VFL without model splitting and cannot be applied to VFL with model splitting.
- The experimental results across multiple data sets and model architectures demonstrate the efficacy of our defense in reducing the label inference accuracy of the malicious party, while incurring only minimal performance degradation in the federated models' original task.

Fuzzing Is Not The End: Efficient Fault Localization in ARM IoT Firmware
The NESA Lab, ZJU Dec. 2022 - Ongoing
Advisor: Professor Shouling Ji, College of Computer Science and Technology, ZJU

- The particularity of the firmware operating environment has led to the fact that current mainstream and efficient firmware fuzzing is often based on analyzing failing test cases. Although some work has proposed automated root cause analysis methods, these methods are not suitable for IoT scenarios. We migrated them to ARM and made huge improvements.
- Developed and implemented an efficient analysis method tailored for closed-source ARM architecture IoT firmware crashes. This method provides valuable support and simplification for vulnerability mining tools, particularly fuzzing, enabling the analysis of a substantial number of crashing cases.

Leadership, Hobbies and Volunteering

Student Assistant at Student Affairs Department, Zhejiang University Mar. 2021 - Ongoing

- Engaged actively in the daily operations of the institution and took part in organizing pivotal components of large-scale student activities, including freshman orientation education.

Sports Events Participated, Zhejiang University

- Ranked Fourth in the Men's 100m Freestyle Swimming Competition, Zhejiang University. Jun. 2022
- Served as the Chief Referee of Timing Team in Zhejiang University Track and Field Games. Sept. 2022

Language

TOEFL iBT Score: 97 (R28 L23 S22 W24), GRE: 167 (Q) + 149 (V)