Peiran Wang

(86) 17883693551 | whilebug@gmail.com | github.com/whilebug

Education and Work

Sichuan University (SCU) Chengdu, China
B.E. in Cybersecurity, Cyberspace Security excellence class, GPA: 3.90, rank: 2/172 *Sept. 2019 – Jun. 2022*

Research Experience

Full-time Research Intern Jun. 2022 – Current
Johns Hopkins University *Baltimore, USA*

- Develop Cross-site fingerprint framework (ongoing).

Full-time Research Intern Jun. 2022 – Current
University of Waterloo *Waterloo, Canada*

- Research on Fuzzing smart contract (ongoing).

Full-time Research Intern Sep. 2021 – Current
Microsoft Research Asia, Systems & Networking Group *Beijing, China*

- Build auto parallel system for deep learning (ongoing).

Undergraduate Research Assistant Sept. 2020 – May. 2022
Sichuan University *Chengdu, China*

- Developed a Byzantine defense framework in Federated Learning.
- Developed a privacy protection platform to deal with the leakage of user privacy in IoT.
- Developed an operating system attack detection system based on machine learning.
- Proposed A solution to the problem of non-IID data in Federated Learning.
- Proposed a static detection method to detect malicious mining JavaScript code in browser.

Awards

National Scholarship (for top 2% students)
Sichuan University **First Class** Scholarship
National-Level College Students' Innovative Entrepreneurial Training Plan Program
Internet + competition province-level sliver prize
26th IEEE Symposium on Computers and Communications (ISCC 2021) **Best Paper Award**
Third prize Annual National Mathematical Modeling Competition in Sichuan
Third prize Annual National Mathematics Competition in Sichuan

Publication

[1] Li, Beibei and Wang, Peiran and Kong, Qinglei and Yuan, Zhang and Lu, Rongxing. Defending Byzantine Attacks in Ensemble Federated Learning: A Reputation-based Phishing Approach. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TIFS (under revision)*, 2022.

[2] Li, Beibei and Wang, Peiran and Huang, Hanyuan and Ma, Shang and Jiang, Yukun. FLPhish: Reputation-based Phishing Byzantine Defense in Ensemble Federated Learning. *2021 IEEE Symposium on Computers and Communications (ISCC)*, Best Paper Award, 2021.

[3] Li, Beibei and Jiang, Yukun and Sun, Wenbin and Niu, Weina and Wang, Peiran. FedVANET: Efficient Federated Learning with Non-IID Data for Vehicular Ad Hoc Networks. *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021.

[4] Wang, Peiran and Sun, Yuqiang and Huang, Cheng and Du, Yutong and Liang, Genpei and Long, Gang. MineDetector: JavaScript Browser-side Cryptomining Detection using Static Methods. *The 24th IEEE International Conference on Computational Science and Engineering (CSE 2021)*, 2021.

[5] nnParallel: An Automatic Parallelism Compiler for Large Scale Neural Network *(Working paper in MSRA, main developer).*

Projects

Byzantine Clients Detection in Federated Learning Oct. 2020 – May. 2022

- Proposed a method to detect and prevent Byzantine attacks in Federated Learning.
- *A paper was accepted by IEEE ISCC 2021, and awarded Best Paper Award.
- *A working paper was submitted to IEEE TIFS.

Automatic AI Distributed Parallelism System Sep. 2021 – Current

- Research on proposing a brand new parallelism search algorithm for large scale AI System.

Javascript Cryptojacking Detection in Web Browser Apr. 2020 – May. 2021

- Proposed a static detection method to detect malicious mining JavaScript code in browser.
- *A paper was accepted by IEEE CSE 2021.

A Framework for Solving non-IID Problems in Federated Learning Oct. 2020 – Aug. 2021

- A Framework for Solving non-IID Problems in Federated Learning.
- *A paper was accepted by IEEE Globecom 2021.

IoT Privacy-Enhancing Platform Mar. 2021 – Aug. 2021

- Developed a privacy protection platform to deal with the leakage of user privacy in IoT.
- As the team leader, he led the research and development of the project team, which improved his project management organization ability and presentation ability.

Operation System Intrusion Detection System Oct. 2019 – Aug. 2020

- Developed an operating system attack detection system based on machine learning.
- As the team leader, he led the research and development of the project team, which improved the project management organization ability and presentation ability.
- Top 100 elites Award in 100 Elites Competition 2020.

Research Interest

System: System Security/Machine Learning System/Distributed System/Networked System
Networking: Networking Measurement/Video Stream Optimization/Video Analytics
Software: Software Security/Fuzzing/Software Analysis/Software Debugging

Skills

Programming: C/C++, Python, Latex, JavaScript, HTML, CSS, Assembly
Developer Tools: Linux, Git, Docker, MySql, PyTorch, Keras
Languages: Chinese (native speaker), English (IELTS: overall 7.5; GRE: overall 326)
Research Skills: Database Management, Data Analysis, Deep Learning, Modeling Analysis, Program Analysis

Personal Statement

After entering Sichuan University, he was selected as a member of Cyberspace Security excellence class of Sichuan University. In the first academic year, he won the national scholarship and the annual first-class scholarship of Sichuan University. His compulsory grade ranks 2/173, with an average score of 91 and GPA of 3.90. He performs well in English, with IELTS score of 7.5 and GRE score of 326, and can communicate with native speakers fluently. He also has rich project experiences as stated above. He has many research experiences and began to participate in scientific research in his sophomore year. 3 conference papers of him has been accepted or published and 1 journal paper is under review. Recently he joined Microsoft Research Asia to start a research internship on AI system.