

Zihan (Tomson) Li

bio.tomson.li

Email : tomson.li@tomson.li

Mobile : +1-765-301-1953

EDUCATION

Washington University in St. Louis <i>Doctor of Philosophy in Computer Science</i>	St. Louis, MO (Anticipated May. 2028)
Washington University in St. Louis <i>Bachelor of Science in Computer Engineering, Master of Science in Cybersecurity Engineering</i>	St. Louis, MO Aug. 2020 – May 2023
DePauw University <i>Bachelor of Arts</i>	Greencastle, IN Aug. 2017 – May 2020

EXPERIENCE

Graduate Research Assistant <i>Washington University in St. Louis</i>	May 2022 – Present St. Louis, MO
<ul style="list-style-type: none">Research focuses on system security and cyber-physical systems.Conducted IoT devices firmware update pipeline vulnerability study. Validated 150 firmware images from 33 device families, leading to the discovery of both zero-day and n-day vulnerabilities. Our findings were disclosed responsibly, resulting in the assignment of 25 CVE IDs and one PSV IDDeveloped experimental Linux scheduler enforcer for timing violation detection and mitigation with an average performance overhead of only around 2.8%.Performed sensitive analysis on Linux perf counters, assisting offline CPU performance profiling.Optimization on communication cost of Federated Learning. Reducing communication cost by 30% while maintaining training accuracy of 95%.	
C++ Backend Development Intern <i>Yume.im</i>	July 2020 – Sept. 2020 Shenzhen, China
<ul style="list-style-type: none">Developed an end-to-end encryption module for audio and video real-time communicationIntegrated the encryption module into the cross-platform compilation build workflowUtilizing optimization techniques to ensure low-performance overhead for encryption and decryption.	

PROJECTS

Federated Learning Optimization <i>Machine Learning, Federated Learning, Python</i>	Aug 2024 – Present
<ul style="list-style-type: none">Developed adaptive machine learning protocols for predictive modeling in distributed environments, leveraging advanced statistical techniques and Python libraries such as Pytorch, pandas, and NumPy. Reducing communication cost by 30% while maintaining training accuracy of 95%Conduct an empirical study on communication cost for federated learning.Designed and optimized data pipelines for processing large-scale distributed datasets. Adaptive gradient compression rate can reach up to 210xReal-world FL simulation demonstrates the feasibility of the proposed approach.	

PUBLICATIONS

Your Firmware Has Arrived: A Study of Firmware Update Vulnerabilities <i>USENIX Security '24</i>
Yuhao Wu, Jinwen Wang, Yujie Wang, Shixuan Zhai, Zihan Li , Yi He, Kun Sun, Qi Li, Ning Zhang
Work-in-Progress: Measuring Security Protection in Real-time Embedded Firmware <i>2022 IEEE Real-Time Systems Symposium (RTSS)</i>
Yuhao Wu, Yujie Wang, Shixuan Zhai, Zihan Li , Ao Li, Jinwen Wang, Ning Zhang

HONOR AWARDS

2022 Dean's Select PhD Fellowship <i>Washington University in St. Louis</i>
Nominated for the 2022 Dean's Select PhD Fellowship at Washington University in St. Louis.
Dean's List <i>DePauw University</i>
Recognized on the Dean's List for 2017 and 2020

TECHNICAL SKILLS

Languages: C/C++, Python, Java, JavaScript, HTML/CSS, VHDL, Assembly, SQL, PHP
Frameworks: React, Node.js
Developer Tools: Git, Cmake, Docker, VS Code, Visual Studio, Eclipse, Wireshark, Xcode, Ghidra, Database Management Systems, Excel
Libraries: pandas, NumPy, Matplotlib, Tkinter, Pytorch
OS: Linux Kernel Programming, Kernel Scheduler, Kernel Network Stack