

Zihan (Tomson) Li

bio.tomson.li

Email : tomson.li@tomson.li

Mobile : +1-765-301-1953

EDUCATION

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

EXPERIENCE

Graduate Research Assistant	May 2022 – Present
<i>Washington University in St. Louis</i>	<i>St. Louis, MO</i>
<ul style="list-style-type: none">Research focuses on system security and cyber-physical systems.Analyzed IoT firmware updates, examining 150 images from 33 device families. Discovered zero-day and n-day vulnerabilities, leading to 25 CVE IDs and one PSV ID through responsible disclosure.Developed 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	July 2020 – Sept. 2020
<i>Youme.im</i>	<i>Shenzhen, China</i>
<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.	

PUBLICATIONS

Resilient Federated Learning on Embedded Devices with Constrained Network Connectivity
<i>2025 62th ACM/IEEE Design Automation Conference (DAC)</i>
Zihan Li , Han Liu, Ao Li, Ching-hsiang Chan, Yevgeniy Vorobeychik, William Yeoh, Wenjing Lou, Ning Zhang
A Unified Hardware Performance Profiling Infrastructure to Measure and Manage Uncertainty
<i>19th USENIX Symposium on Operating Systems Design and Implementation (OSDI 25)</i>
Ao Li, Marion Sudvarg, Zihan Li , Sanjoy Baruah, Chris Gill, Ning Zhang
Tintin: PMU Scheduling to Minimize Uncertainty
<i>OSPERT Workshop at ECRTS 2025</i>
Marion Sudvarg, Ao Li, Zihan Li , Sanjoy Baruah, Chris Gill, Ning Zhang
Your Firmware Has Arrived: A Study of Firmware Update Vulnerabilities
<i>33rd USENIX Security Symposium (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

PROJECTS

Open Platform for Cyber Physical System Research (OPCPS)	April 2025 – Present
<ul style="list-style-type: none">• Design and implement an open-source platform specifically tailored for CPS security research testing• Offers modular components designed for easy replacement with alternative implementations.• Security instrumentations for various real-world CPS platforms• Performance and timing profiling to understand the real-time impact of CPS under different security instrumentations.	
EMILY: Electro Magnetic Interference Ledger & registrY EMI, Database	Nov 2025 – Present
<ul style="list-style-type: none">• Design database structure to improve the performance and maintainability of EMILY.• Implement backend for high performance and secure access to the database based on Springboot framework.• Design and implement a user-friendly front-end for astronomers to use the system with ease.• Real-world impact and public available at emily.tomson.li	
Federated Learning Optimization Machine Learning, Federated Learning, Python	Aug 2024 – Dec 2024
<ul style="list-style-type: none">• Designed adaptive ML protocols for distributed predictive modeling, using PyTorch, pandas, and NumPy. Cut communication costs by 30% while preserving 95% training accuracy.• 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 210x• Real-world FL simulation demonstrates the feasibility of the proposed approach.• Accepted by <i>2025 62th ACM/IEEE Design Automation Conference (DAC)</i>	
HONOR AWARDS	
2022 Dean's Select PhD Fellowship Washington University in St. Louis	
Nominated for the 2022 Dean's Select PhD Fellowship at Washington University in St. Louis.	
Dean's List DePauw University	
Recognized on the Dean's List for 2017 and 2020	
SERVICES	
Reviewer	
<ul style="list-style-type: none">• IEEE Transactions on Information Forensics and Security• IEEE/ACM Transactions on Networking• ACM Transactions on Cyber-Physical Systems• ISOC Symposium on Vehicle Security and Privacy (VehicleSec '24)• International Conference on Computer Communications and Networks (ICCCN)	
Artifact Evaluation Program Committee	
<ul style="list-style-type: none">• ACM Conference on Computer and Communications Security (CCS)	
TECHNICAL SKILLS	
Languages: C/C++, Python, Java, JavaScript, HTML/CSS, VHDL, Assembly, SQL, PHP	
Frameworks: React, Node.js, ROS, ROS2	
Developer Tools: Git, Cmake, Docker, VS Code, Visual Studio, Eclipse, Wireshark, Xcode, Ghidra, Database Management Systems, Excel, Gazebo	
Libraries: pandas, NumPy, Matplotlib, Tkinter, Pytorch	
OS: Linux Kernel Programming, Kernel Scheduler, Kernel Network Stack	