Jingwen Shi

Personal Website | Google Scholar | Linkedin | shijingwen9@gmail.com | 517-974-8921 | East Lansing, MI 48823

EDUCATION

Research Area: Mobile Systems and Network, Security, Cloud Computing, AI for System

- **Michigan State University** Michigan, USA
  Ph.D. Candidate, Computer Science - GPA:4.0 *Aug. 2019 - Dec. 2024/Apr. 2025 (Expected)*
  Thesis: Exploring and Addressing the Vulnerabilities of Multimedia Services over Mobile Networks: From Infrastructure to Devices
- **University of Chinese Academy of Sciences** Beijing, China
  M.S., Applied Computer Technology - Google Girl Hackathon Best Practical Award *Sept. 2016 - May 2019*
  Thesis: Traffic Prediction and Uncertainty Interval Estimation for E-commerce Clusters
- **Hunan University** Hunan, China
  B.S., Information Security - Graduated with Honors *Sept. 2012 - May 2016*
  Thesis: Visual Search Engine with Crawler System for Information Security Laws

SKILLS

Python, C/C++, Java, Matlab, Swift, Android, iOS, Tensorflow, Keras, scikit-learn, Linux, srsRAN, USRP, QXDM, QPST, ADB, Wireshark, Plotly, Julia, Hadoop, MongoDB, PostgreSQL, OpenSSL, Django, MySQL

INTERNSHIP

AT&T Lab - Senior Associate Student Intern *Jun. 2024 - Aug. 2024, USA*

- Investigated large-scale cellular IoT network traffic with the team and defined a research topic focused on demystifying traffic from unknown IP addresses. Analyzed time-series similarities and anomalies in network traffic, providing use cases for mobile attack detection and billing explanations.
- Led the design and development of the "AI-Based Traffic Monitoring Platform for 5G/4G IoT Networks," utilizing machine learning, statistical analysis, and signal processing techniques.
- Developed an interactive data visualization website with various dashboards for production demos using Plotly.
- Presented insights to three market teams and a machine learning research team. Collaborated with a market team to advance the project to an online platform.
- Successfully submitted **one patent** application filed with the U.S. Patent Office.
- Proposed new 5G/4G IoV research **proposal** for long-term collaboration initiatives.

Los Alamos National Lab - Research Intern *Jun. 2021 - Aug. 2021, USA*

- Built a Cyber-Physical System (CPS) simulation testbed for a HVAC system, integrating a complex Finite State Machine and differential equations using Julia.
- Investigated the reconstruction problem of Cyber-Physical Systems from measurement data. Developed a learning framework using Ordinary Least Squares and SVD, achieving **97%** accuracy.

Alibaba - Research & Development Intern *Jan. 2019 - Jun. 2019, China*

- [**Project 1. AI-assisted Resource Allocation**] Collaborated with research and development teams to analyze real-time cloud platform, defining a research focus on AI-driven dynamic uncertainty prediction for worst-case QPS scenarios to optimize cloud resource allocation.
- Designed and developed Bayesian Neural Networks to enhance CNN and LSTM models for QPS prediction at Taobao, achieving **99.8%** accuracy.
- Successfully deployed deep learning algorithms on Hadoop and Alibaba EagleEye, a distributed tracing and monitoring system. Conducted large-scale evaluations comparing various deep learning models.
- [**Project 2. Anomaly Detection in Cloud**] Collaborated closely with a production team to improve their anomaly detection algorithm for identifying abnormal virtual machines in a cluster and automating the restart.
- Designed and developed a framework optimized for low-latency response on high-volume, low-level metrics data (e.g., CPU, memory). Addressed challenges by integrating machine learning and statistical techniques.
- Evaluated the solution on clusters with over 1,000 virtual machines, reducing false alarms by **95%.**
- Published **one paper** and contributed to **two patents**. [*JST'19*]

PROJECT EXPERIENCE

Project 1. Side-channel Attacks Against Radio Access Network [Lead] *Jun. 2019 - May. 2022, USA*

- Identified vulnerabilities in 5G/4G radio protocols (PHY/MAC/RLC/PDCP) as defined by 3GPP standards, revealing potential leaks of user call behaviors and speaking patterns in wireless communication.
- Applied AI techniques (e.g., DBSCAN, Mask RCNN) to associate radio identity (C-RNTI) with user identity.
- Designed a radio DoS attack that stealthily mutes a user's voice during a phone call by precisely overshadowing the radio resources assigned to calling user at the PHY layer (i.e., PDCCH/PDSCH/PUSCH). Implemented the tool using USRP, FPGA, UHD, srsRAN, Signal Booster Antenna and C/C++.
- Proposed a defense mechanism against potential side-channel attacks by enhancing existing radio protocols. Validated the solution by building a 5G/4G simulation testbed with USRP, srsRAN, Open IMS Core, and an IMS client. Successfully deployed and validated the solution on the testbed.
- Designed a series of radio sniffing attacks to infer if a victim is making a call with an Interactive Voice Response (IVR) system, identify the company being called, and detect if payments are being made. Analyzed PDCP layer radio log using deep learning models, including LSTM, ResNet50, and Siamese Neural Networks (SNN).
- Conducted real-world user studies to evaluate the impact of proposed attacks.
- Authored two research papers and one poster presentation. [*CERIAS'24 Poster*, *IEEE CNS'23*, *Preprint*]

Project 2. Mobile Operating System Security [Lead] *Aug. 2022 - Oct. 2024, USA*

- Discovered two vulnerabilities in mobile operating systems, specifically in the Android Linux kernel, enabling a DoS attack that blocks IMS clients from accessing networks over Wi-Fi, 4G LTE, and 5G NR, and allows SMS spoofing to fabricate arbitrary sender names.
- Investigated the cellular baseband architecture of modern phones, including DSP, RTOS, and modem components. Discovered a vulnerability in the modem that enables the hijacking of media traffic (via video H.264 codecs) during video calls, along with an additional vulnerability in the application processor.
- Test vulnerabilities on iOS by implementing proposed attacks in Swift and analyzing Darwin source code.
- Implemented all proposed attacks by developing malware for Android, VPN services, and Wi-Fi routers.
- Reported vulnerabilities were identified as **high severity and high quality** by **Google Bug Bounty and Vulnerability Reward Programs**. Invited to submit a 2023 Google ASPIRE proposal as Co-PI .
- Authored two research papers. [*ACM Mobicom'24*, ACM TON'24 Submission]

Project 3. Emergency 911 and Next Generation 911 [Participant/Lead] *Aug. 2023 - Oct. 2024, USA*

- Constructed the cellular network simulation testbed of Emergency 911 from device to 5G/4G core network.
- Successfully defended DoS and free-data attacks against 911 services.
- Investigated GSMA and FCC standard of Next Generation 911. Identified potential risk to spoof a 911 call.
- Authored three research papers. [*ACM Mobicom'22* (**SIGMOBILE Highlgiht, Best Community Paper, AT&T Security Award**), *ACM GetMobile'23*, *IEEE TON'24*]

Project 4. Distributed Storage Systems for Cloud [Participant/Lead] *Aug. 2020 - Oct. 2021, China*

- [**Project 1. Distributed Spatial Index**] Designed a distributed spatial index for large-scale mobility IoT and vehicle GPS data storage in collaboration with partners.
- Assisted in implementing the spatial index on HBase and MongoDB, reducing I/O traffic by **70%**.
- [**Project 2. Distributed Storage and Computing System**] Designed and implemented a data pipeline connecting HDFS to PostgreSQL for satellite images.
- Authored one research papers and two patents. [*IEEE IPCCC'18*, *Approved Patent CN 110147353 A*, *Approved Patent 2 CN 110147904 B*]

Project 5. Visual Search Engine with Crawler System for Laws [Lead] *Feb. 2019 - Apr. 2019, China*

- Designed and implemented a crawler system using Python, SQLite3, and Scrapy to collect Chinese laws, cases, regulations, and news related to information security.
- Developed a search engine with interactive visualization features using Django, Ajax, PageRank, and D3.js. Optimized the PageRank algorithm to function efficiently on systems with limited CPU and memory resources.
- Awarded the **Excellent Graduate Design**.