Jingwen Shi

East Lansing, MI, 48823 | +1-517-974-8921
GHC23 | SWE | WiCys | shijingwen9@gmail.com | https://shijingwen.github.io/

EDUCATION

Ph.D. - Computer Science and Engineering Aug 2019 - Dec 2024
Michigan State University GPA:4.0/4.0 Area: Security and AI, Wireless Network and Mobile System
Award Highlight: Freshgogo Website Bug Bounty, WiCyS Security Training Scholarship

M.S. - Applied Computer Technology Sep 2016 - May 2019
University of Chinese Academy of Sciences GPA: 80/100 Area: Cloud Computing
Award Highlight: Google Girl Hackathon in Beijing Best Practical Award

B.S. - Information Security Sep 2012 - May 2016
Hunan University GPA: 88/100 Area: Information Security
Award Highlight: Graduated with Honor (Summa eq.)

SKILLS

Expert in: Python, Java, Android, Supervised Machine Learning (LSTM, Siamese Neural Network, ResNet50, Bayesian Neural Networks), Unsupervised Machine Learning (DBSCAN, Isolation Forest, PCA, SVD), Linux, Wireshark, 3GPP, srsRAN, QXDM, USRP, OpenIMSCore, Keras
Intermediate in: C, C++, Go, Julia, Matlab, OpenSSL, goAccess, URL Fuzzy, Hashcat, Perf, MongoDB, Hbase, PostgreSQL, Hadoop, D3.js, PHP, Shell, Django, Scrapy, sqlite3, MySQL, Tensorflow

WORKING EXPERIENCE

Research Intern *Los Alamos National Lab* Jun 2021 - Aug 2021

- Project: Privacy Security of Cyber-Physical System (CPS)
  Developed a learning approach to re-construct a black-box cyber-physical system model from operating data samples. The cyber-physical system consists of physical equations and control rules. Developed CSP testbed in *Julia*. Pioneered privacy leakage of re-constructing a black-box CPS using machine learning *models* (*Ordinary Least Squares, SVM, Singular Value Decomposition*). Achieved accuracy of **97%.**

Research Intern *Alibaba* Jan 2019 - Jun 2019

- Project: Traffic Prediction and Uncertainty Estimation for Resource Allocation on Cloud
  1.QPS prediction is critical for resource allocation in the cloud. Designed *Bayesian Neural Networks* for real-time QPS prediction. Trained models on *Hadoop*, achieving **99.8%** accuracy in [**JST'19**].

- Project: Anomaly Detection for Virtual Machines Failure in Cloud
  1.Invented an automated anomaly detection framework for large-scale clusters. Integrated *unsupervised machine learning* models (*isolation forest, 3-sigma, and KDE*). Reduced **95%** of false alarms.

SELECTED PROJECT

- Project: Uncovering Loopholes of IMS (SMS/Call/RCS) in 5G/4G and Smartphone Sep 2019 - Present
  1.[Android and Mobile System Security] Created a range of malicious *Android* malware to find vulnerabilities in *Android* and mobile networks. Devised three attacks (*SMS Phishing, DoS, Covert channel*) and proposed defense on Android. Our study is under review at [**Mobicom'24**]. Invited by Google Android Connectivity Security team for **Google ASPIRE proposal (Co-PI)**.
  2.[911 Emergency Call Security] Constructed a comprehensive testbed including an IMS network, Radio Access Network (*srsRAN, USRP*), and software-defined phone (*srsUE*). Successfully defended DoS attacks against 911 services. One paper was accepted by [**Mobicom'22**] (**Best Community Paper, AT&T Security Award**).
  3.[5G/4G Radio Access Network Security] Discovered vulnerabilities in *5G/4G radio protocols of mobile networks*, leading to *side-channel attacks* (*privacy inference*, *identity deanonymization*, and *radio overshadowing*). For wireless radio channel eavesdrop, supervised machine learning *(Siamese Neural Network, LSTM)* and unsupervised machine learning *(DBSCAN)* were used. For video surveillance, applied object detection and segmentation *(Mask R-CNN)*, face detection (*DSFD, ResNet50*), and lip motion detection (*RNN*). Our security study will be presented at [**CNS'23**] and is under review by [**IEEE TMC**].

- Project: A Cloud Computing System for Geographical Data May 2017 - Dec 2018
  1.Created a data pipeline connecting *HDFS* to *PostgreSQL*, enabling storage, querying, and analysis of large-scale satellite images and traffic data.
  2.Created a spatial index reducing I/O traffic by up to **70%**. Evaluated performance with *Hbase* and *MongoDB*. Accepted paper at [**IPCCC'18**].

Publications

- Mobile Network/System Security: [IEEE TMC'22], [ACM Mobicom'22] (Best Community Paper, AT&T Security Award), [ACM GetMobile'23], [IEEE CNS'23], [ACM Mobicom'24, Peer Reviewing], [IEEE TMC'24, Peer Reviewing]
- Distributed System and Federated Learning: [IEEE IPCCC'18], [JST'19], [IEEE Internet of Things Journal]