# QIFAN ZHANG

3435 Engineering Hall, Irvine, CA, USA, 92697
Email: qifanz.uci@gmail.com; Tel: +1-(619)-678-1077

## EDUCATION

**University of California, Irvine** *Sept 2020 - Jul 2025 (expected)*
Ph.D. candidate in Computer Engineering
**Advisor**: Prof. Zhou Li
Department of EECS, the Henry Samueli School of Engineering

**ShanghaiTech University** *Aug 2016 - Jul 2020*
B.E. in Computer Science and Technology
Minor in Innovation and Entrepreneurship

## RESEARCH INTERESTS

**Domain Name System (DNS).** I'm interested in security, privacy and reliability of DNS. My past research covered protocol security [Security'23][NDSS'23], and automated vulnerability detection with fuzzing techniques [Security'24]. I have also surveyed DNS operational issues by mining, labelling and classifying main-stream public DNS forums [IEEE Access'22].

**Machine Learning Security and Privacy.** I'm also interested in security and privacy topics related to machine learning. His past research demonstrated model extraction on Autonomous Vehicle using Gradient-Descent based methods [ACSAC'22]. Recently, I participated in FedMLSecurity, a benchmark to simulate attacks and defenses on Federated Learning and Large Language Models (LLMs), and a zero-knowledge proof-based anomaly detection method on Federated Learning.

## PUBLICATIONS

**Conference Papers**

· **Zhang, Q.**, Bai, X., Li, X., Duan, H., Li, Q. and Li, Z. *ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing*. Accepted by the 33rd USENIX Security (**Security**), 2024. Extended version available on ArXiv.

- **12** types of vulnerabilities, **23** bugs detected and **15** CVEs assigned among 6 popular DNS software.
- Presented in DNS-OARC'42.
- ***Skills involved:*** *CVE reading and summary, Grammar-based fuzzing, Network environment settings on Docker, Code analysis on DNS software, Cloudflare API, concurrent programming.*

· **Zhang, Q.**, Shen, J., Tan, M., Zhou, Z., Li, Z., Chen, Q.A. and Zhang, H. *Play the Imitation Game: Model Extraction Attack against Autonomous Driving Localization.* Accepted by the 38th Annual Computer Security Applications Conference (**ACSAC**), 2022.

- Achieve cm-level precision with 40-second driving data.
- ***Skills involved:*** *model establishment and training on PyTorch, Optimization, Baidu Apollo, Autonomous Driving controller algorithms.*

· Li, X., Lu, C., Liu, B., **Zhang, Q.**, Li, Z., Duan, H. and Li, Q. *The Maginot Line: Attacking the Boundary of DNS Caching Protection.* Accepted by the 32nd USENIX Security (**Security**), 2023.

- **Vulnerability acknowledged** by CVE-2021-25220 (BIND 9), CVE-2021-43105 (Technitium), CVE-2022-32983 (Knot Resolver).
- Awarded $1,000 by Microsoft Security Response Center.

- ***Skills involved:*** *Network environment settings on Virtual Machine, debugging via GDB and CLion, Python Scapy, Code analysis on DNS software.*

· Li, X., Liu, B., Bai, X., Zhang, M., **Zhang, Q.**, Li, Z., Duan, H. and Li, Q. *Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation.* Accepted by the 30th Annual Network and Distributed System Security Symposium (**NDSS**), 2023.

- **Vulnerability acknowledged** by CVE-2022-30250, CVE-2022-30251 (Knot Resolver), CVE-2022-30252 (PowerDNS Recursor), CVE-2022-30254 (Simple DNS Plus), CVE-2022-30256 (MaraDNS), CVE-2022-30257, CVE-2022-30258 (Technitium), CVE-2022-30698, CVE-2022-30699 (Unbound)

- ***Skills involved:*** *Network scanning and measurement, Network environment settings on Docker, Python Scapy, Code analysis on DNS software.*

**Journal Papers**

· Liao, X., Xu, J., **Zhang, Q.** and Li, Z. *A Comprehensive Study of DNS Operational Issues by Mining DNS Forums.* Accepted by IEEE Access, 2022.

- ***Skills involved:*** *Data mining on DNS forums, DNS ticket labelling and classification.*

**Preprints/In Submission**

· Han, S., **Zhang, Q.**, Yao, Y., Jin, W., Xu, Z. and He, C. *LLM Multi-Agent Systems: Challenges and Open Problems.* Preprint available on arXiv.

· Han, S., Buyukates, B., Hu, Z., Jin, H., Jin, W., Sun, L., Wang, X., Xie, C., Zhang, K., **Zhang, Q.**, Zhang, Y., Avestimehr, S. and He, C. *FedMLSecurity: A Benchmark for Attacks and Defenses in Federated Learning and LLMs.* Preprint available on arXiv .

· Han, S., Wu, W., Buyukates, B., Jin, W., Yao, Y., **Zhang, Q.**, Avestimehr, S. and He, C. *Kick Bad Guys Out! Zero-Knowledge-Proof-Based Anomaly Detection in Federated Learning, with Application to Federated LLMs.* Preprint available on arXiv.

## PROJECTS

**Find DNSSEC Vulnerabilities via Fuzzing** *Feb 2023 - now*

Based on ResolverFuzz, we are now trying to fuzz DNS Security Extension (DNSSEC). We first summarized *Common Vulnerabilities and Exposures*(CVEs) of popular DNS software, such as BIND, Unbound, Knot, etc. Based on our observation from the CVE study, we first implemented a DNS fuzzer using *Probabilistic Context-Free Grammar* (PCFG) and byte-level mutation. We also built up a Docker-based DNS nameserver system, which supports DNSSEC validation chain. Then, we performed constrained stateful fuzzing by focusing on the query-response sequence. This project is still ongoing.
***Skills involved:*** *applied cryptography, OpenSSL, Grammar-based fuzzing, Network environment settings on Docker, Python Scapy, Code analysis on DNS software, concurrent programming.*

**Cardiac Ablation Aiding System** *Dec 2018 - Sept 2019*

***Instructor****: Prof. Zhihao Jiang (ShanghaiTech University)*
This project aims at extracting features of different kinds of cardiac arrhythmias, especially tachycardias and proposed a way that transfers electric signs into a graph to determine possible tachycardias. It will also instruct doctors which place of heart to be detected next, which could be used to aid doctors in cardiac ablation operation. The final model is stimulated on Matlab and Stimulink.
***Skills involved:*** *Matlab/Stimulink, unit test, code coverage, software validation.*

**Line-Based 3D Panorama** *May 2019 - Jun 2019*

***Instructor****: Prof. Laurent Kneip (ShanghaiTech University)*
Build a 3D panorama with LSD, line merging and line tracking. We use feature matching, seven-point

algorithm and scale propagation to calculate relative pose estimation.
***Skills involved:*** *OpenCV, line merging, pose calculation, bundle adjustment.*

## SERVICES

**Program Committee**

· EAI ICECI: 2024

**Artifact Evaluation Committee**

· CCS: 2023
· USENIX Security: 2024
· NDSS: 2024

**External Reviewers**

· NDSS: 2023, 2022, 2021
· AsiaCCS: 2022, 2021
· SecureComm: 2023
· **Journals**: PeerJ Computer Science, IEEE Internet of Things, IEEE Trans on Wireless Communications, High-Confidence Computing

## TECHNICAL SKILLS

| | |
|---|---|
| **Programming Language** | Python, Java, C/C++, Rust |
| **Software & Tools** | Matlab/Simulink, VMware Workstation Player, Docker, Cloudflare API, OpenCV, CLion, GDB |

## TEACHING

**Teaching Assistant** University of California, Irvine

· EECS 40 (F23, F22): Objected Oriented System and Programming (#students: 90/95)

**Teaching Assistant** ShanghaiTech University

· SI 100C (F17): Introduction to Computer Science and Technology (#students: 127)
· CS 100 (F18): Programming (#students: 243)
· CS 277 (F19): Introduction to Data Science and FinTech (#students: 23)
· (core TA) SI 100B (S18, S19, S20): Introduction to Information Science and Technology (#students: 203/174/410)

## HONORS

**University of California, Irvine**

· 2023 ANRW Travel Grant
· Associated Graduate Students Conference Stipend (Winter 2022)
· 2022 ACSAC Student Conferenceship
· Student travel grant for NDSS (2021)
· Student travel grant for USENIX Security (2021)
· Student travel grant for IEEE Symposium on Security and Privacy (2021)

**ShanghaiTech University**

· 2020 ShanghaiTech Outstanding Graduate

- SIST Outstanding Teaching Assistant (2020, 2019, 2018)
- Merit Student (2018-2019, 2017-2018, 2016-2017)
- Outstanding Personnel in 2017 Summer Camp