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 - Mar 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.Eng. in Computer Science and Technology
Minor in Innovation and Entrepreneurship

University of California, Berkeley *2017*
Summer Session

RESEARCH INTERESTS

Domain Name System (DNS). I'm interested in security, privacy and reliability of DNS. In particular, I'm interested in automated vulnerability detection with fuzzing techniques [Security'24]. Based on my automated tool, ResolverFuzz, several vital vulnerabilities have been discovered, including Pheonix Domain [NDSS'23] and MaginotDNS [Security'23]. 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. My past research demonstrated model extraction on Autonomous Vehicle using Gradient-Descent based methods [ACSAC'22]. Recently, I participated in FedMLSecurity [KDD'24], 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. Artifacts available on GitHub.

- **12** types of vulnerabilities, **23** bugs detected and **15** CVEs assigned among 6 popular DNS software.
- Presented in DNS-OARC'42 and NDSS 2024 poster session.
- ***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.*

· 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.* Accepted by ACM Knowledge Discovery and Data Mining Conference (**KDD**), 2024. Preprint available on arXiv. Artifacts available on GitHub.

· 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., 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.

SERVICES

Program Committee

· EAI ICECI: 2024

Artifact Evaluation Committee

· CCS: 2024, 2023
· USENIX Security: 2024
· NDSS: 2025, 2024

External Reviewers

· NDSS: 2025, 2023, 2022, 2021
· AsiaCCS: 2022, 2021
· SecureComm: 2023
· IEEE Transactions on Transactions on Information Forensics & Security (T-IFS)
· IEEE Transactions on Wireless Communications (TWC)
· IEEE Internet of Things (IoT)
· Elsevier Computer Networks
· Elsevier High-Confidence Computing
· Springer Peer-to-Peer Networking and Applications (PPNA)
· PeerJ Computer Science

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

- (Head TA) EECS 148 (S24): Computer Networks (#students: 217)
- (Head TA in F23) EECS 40 (F23, F22): Objected Oriented System & Programming (#students: 90/95)

Teaching Assistant ShanghaiTech University

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

HONORS

University of California, Irvine

- Student travel grant for USENIX Security (2024, 2021)
- Associated Graduate Students Conference Stipend (Winter 2024, Winter 2022)
- 2024 UCI Concerto Competition Winner
- 2023 ANRW Travel Grant
- ACSAC Student Conferenceship (Fall 2022)
- Student travel grant for NDSS (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