

XUESONG BAI

3435 Engineering Hall ◊ Irvine, CA, USA, 92697
(949)-529-0955 ◊ xuesong.bai@uci.edu ◊ xuesongbai.com

RESEARCH INTERESTS

My research predominantly focuses on improving the robustness and security of modern network infrastructures by designing new fuzzing techniques to test network protocol implementations, especially DNS. I have a solid knowledge of network system, and I'm eager to discuss and explore directions related to network security. including TCP/UDP, network protocols, CDN, and routing algorithms like BGP.

EDUCATION

University of California, Irvine 09/21 - 06/27 (expected)
M.S. & Ph.D. student in Computer Engineering
Advisor: Prof. Zhou Li

Chongqing University & University of Cincinnati 09/15 - 04/20
B.S. in Electrical Engineering
Honors: *Graduated with Cum Laude, Multiple Dean's List*

SKILLS

Programming Language C/C++, Python, Golang, Shell Script
Software & Tools Linux, Git, Docker, Kubernetes, AWS Services, Cloudflare, Wireshark

SELECTED PROJECTS

- Automatic Cyber-Attack Framework with LLM** 2023 - 2024
- Designed a framework to automate "hands-on-keyboard" attacks on a given network environment, jail-broke and leveraged LLM to analyze the situation and make decisions on the next move. The framework was tested in a simulated organizational network with varied attack tasks, endpoint configurations (Windows and Linux systems) with high success rate. Paper currently *in submission*.
 - **Skills:** Network Security, CTF (Capture the Flag), LLM, Network Configuration.
- Fuzzing on DNS Resolution Implementations** 2022 - 2023
- Analyzed all CVEs on DNS software, designed a stateful fuzzing framework with Docker, applied pair-wise network seed mutation, customized scheduler and oracles to find **logic flaws** in the software, used **differential testing** across popular DNS implementations to test resolution consistency.
 - 12 type of vulnerabilities, 23 bugs detected, 15 CVEs assigned among 6 DNS implementations.
 - Paper Accepted in **Security'24**, presented in DNS-OARC'42, NDSS'24 poster session, rewarded by Google Bug Hunters Program.
 - **Skills:** Fuzzing, Docker Network Configuration, Software Analysis, Cloudflare API, Python.
- DNS Cache Poisoning Attack Analysis & Defense** 2021 - 2022
- Investigated and measured the caching mechanism in popular DNS software and public DNS service providers in the global network, found a vulnerability where a revoked domain could still be used for malicious activity for a long time in the current DNS design.
 - 7 DNS software, 15 Public resolvers are affected, 9 CVEs assigned, Paper accepted in **NDSS'23**.
 - **Skills:** Large-scale Network Measurement, DNS Traffic Analysis, Software Analysis, Python.

PUBLICATIONS

Conference

- Qifan Zhang, **Xuesong Bai**, Xiang Li, Haixin Duan, Qi Li, and Zhou Li. *RESOLVERFUZZ: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing*. In Proceedings of the USENIX Security Symposium (**Security**), August, 2024.
- Xiang Li, Baojun Liu, **Xuesong Bai**, Mingming Zhang, Qifan Zhang, Zhou Li, Haixin Duan, and Qi Li. *Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation*. In Proceedings of the Network and Distributed System Security Symposium (**NDSS**), February, 2023.

Preprint

- Jiacen Xu, Jack W Stokes, Geoff McDonald, **Xuesong Bai**, David Marshall, Siyue Wang, Adith Swaminathan, and Zhou Li. *Autoattacker: A large language model guided system to implement automatic cyber-attacks*. In submission, available on *Arxiv*, 2024.

Poster

- Qifan Zhang, **Xuesong Bai**, Xiang Li, Haixin Duan, Qi Li, and Zhou Li. *RESOLVERFUZZ: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing*. In Proceedings of the Network and Distributed System Security Symposium (**NDSS**), February, 2024.

ACADEMIC SERVICES

External Reviewer

- IEEE S&P: 2025.
- NDSS: 2024, 2025.

Journal Reviewer

- Computer Networks.
- Peer-to-Peer Networking and Applications.

Artifact Evaluation Committee

- Security: 2024.
- NDSS: 2024, 2025.
- ACM CCS: 2024.
- EuroSys: 2023 Fall.

TEACHING EXPERIENCE

Reader, EECS 148 / CompSci 132: Computer Networks

University of California, Irvine

- *Instructor: Prof. Zhou Li*, Spring 2022 (#students: 233)

Teaching Assistant, ENED 3061: PROB STAT I

University of Cincinnati

- *Instructor: Dr. TJ Murphy*, Spring 2020 (#students: 91)

HONORS & AWARDS

- Distinguished Artifact Reviewer Awards, ACM CCS 2024.
- Henry Samueli Endowed Fellowship, 2024.
- Rewards from Google Bug Hunters program, 2022.