

# XUESONG BAI

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

## EDUCATION

---

<b>University of California, Irvine</b> Ph.D. candidate in Computer Engineering Advisor: Prof. Zhou Li	09/21 - 06/27 (expected)
<b>Chongqing University &amp; University of Cincinnati</b> B.S. in Electrical Engineering	09/15 - 04/20

## PROFESSIONAL EXPERIENCES

---

<b>Software Engineer Intern</b> Meta Platforms, Inc. - Mentor: Yingjie Gu	06/25 - 09/25 Menlo Park, CA
<b>Graduate Student Researcher</b> UC Irvine - Advisor: Professor Zhou Li	06/22 - Present Irvine, CA

## SKILLS

---

<b>Programming Language</b>	C/C++, Python, Golang, Shell Script
<b>Software &amp; Tools</b>	Linux, Git, Docker, Kubernetes, LLVM, GDB, AWS Services, Cloudflare

## SELECTED PROJECTS

---

- |  |             |
|--|-------------|
| <b>Automatic Cyber-Attack Framework with LLM</b> | 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.
  - Outcome:** Paper currently *in submission*.
  - Skills:** Network Security, CTF (Capture the Flag), LLM (Large Language Model).
- |  |             |
|--|-------------|
| <b>Fuzzing on DNS Resolution Implementations</b> | 2022 - 2023 |
|--|-------------|
- Analyzed 200+ 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 types of vulnerabilities, 23 bugs detected, 15 CVEs assigned among 6 DNS implementations.
  - Outcome:** 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.
- |  |             |
|--|-------------|
| <b>DNS Cache Poisoning Attack Analysis &amp; Defense</b> | 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.
  - Outcome:** 7 DNS software, 15 Public DNS affected; 9 CVEs assigned; Paper accepted in NDSS'23.
  - Skills:** Large-scale Network Measurement, DNS Traffic Analysis, Software Analysis, Python.

## Intelligent Transportation

2019

- Developed a health-focused sensor collector app using Swift, featuring local data storage with SQLite, encrypted data uploads via Alamofire, and campus-wide distribution through Apple Edu Dev.
- Designed an integrated system with FreeRTOS-based embedded boards for GPU+BDS location data processing and an Android app for data compression, local storage, and secure RESTful API uploads.
- **Skills:** iOS, Android, Embedded System development, SQL, Swift, Java.

## 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. Poster accepted in NDSS'24.
- 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*

- Jiachen 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 cyberattacks*. In submission, available on *Arxiv*, 2024.

## HONORS & AWARDS

---

- More than 20 CVEs assigned.
- Distinguished Artifact Reviewer Awards, ACM CCS 2024.
- Henry Samueli Endowed Fellowship, 2024.
- Rewards from Google Bug Hunters program, 2022.

Last Updated: October 8, 2025