YU HUANG

+86 16651693068 ⋄ China
fatmo@nuaa.edu.cn ⋄ fatmo666.github.io

EDUCATION

Bachelor of Computer Science, Nanjing University of Aeronautics and Astronautics 2018 - 2022
GPA: 84/100
Relevant Coursework: Compiler Principles, Data Structures, Operating Systems, and Computer Architecture.

PUBLICATION

Publication 1 : PrSLoc: Sybil attack detection for localization with private observers using differential privacy.
Journal: Computer & Security(JCR Q1, CCF-B).
Co-authors: Yuan Yachao, **Yu Huang**, and Yali Yuan.
Publication Date: August 2023.
DOI: https://doi.org/10.1016/j.cose.2023.103289

PREPRINT

PREPRINT 1 : M3S-UPD: Efficient Multi-Stage Self-Supervised Learning for Fine-Grained Encrypted Traffic Classification with Unknown Pattern Discovery
Co-authors: Yali Yuan, **Yu Huang**, Xingjian Zeng, Hantao Mei, Guang Cheng.
Status: Submitted to *IEEE Transactions on Network and Service Management (TNSM)*, under review.
Link: https://doi.org/10.1016/j.cose.2023.103289

PREPRINT 2 : AnomalyAID: Reliable Interpretation for Semi-supervised Network Anomaly Detection.
Co-authors: Yachao Yuan, **Yu Huang**, Jin Wang.
Link: https://arxiv.org/abs/2411.11293

PREPRINT 3 : Adaptive NAD: Online and Self-adaptive Unsupervised Network Anomaly Detector
Co-authors: Yachao Yuan, **Yu Huang**, Yali Yuan, Jin Wang.
Link: https://arxiv.org/abs/2410.22967

PREPRINT 4 : Local Differential Privacy for Tensors in Distributed Computing Systems
Co-authors: Yachao Yuan, Xiao Tang, **Yu Huang**, Jin Wang
Status: Submitted to *IEEE Transactions on Information Forensics and Security (TIFS)*, under review.
Link: https://arxiv.org/abs/2502.18227

PREPRINT 5 : Robust Website Fingerprinting Attack against Concept Drift
Co-authors: Yali Yuan, Ruolin Ma, Xinyi Liu, **Yu Huang**
Status: Submitted to *INFOCOM 2026*.

SKILLS

Programming Languages	Python, Go, C
Cybersecurity Skills	Code auditing, Fuzzing test, IDS development, Web security
Security Tools	CodeQL, LibFuzzer, AFL, GDB, Burp Suite
Machine Learning Frameworks	PyTorch, Scikit-learn

REASEARCH EXPERIENCE

Research Intern March 2024 - Present
Southeast University. *Remote*

- Conducted research on privacy-preserving Sybil attack detection and network traffic anomaly detection, leading to a publication in Computers & Security (DOI:https://doi.org/10.1016/j.cose.2023.103289).

- Contributed to two manuscripts on adaptive anomaly detection, interpretable self-supervised learning, and novel LDP submitted to TNSM, and TIFS.

WORK EXPERIENCE

Cybersecurity Engineer July 2022 - March 2024
HUYA Inc. *Guang Zhou, China*

- Developed and maintained the company-wide bastion host system using Go and Bash, ensuring secure access and logging for internal resources.
- Extended the company's vulnerability scanner using Go, integrating the Nuclei scanner and enriching POCs for comprehensive vulnerability detection.
- Developed and maintained a software and container supply chain vulnerability detection program, integrating it into the development pipeline.

Data Security Engineer (Intern) July 2021 - October 2021
Ke Holdings Inc. *Beijing, China*

- Identified and addressed sensitive data leakage issues in the company's internal databases, logs, external traffic, and API call chains.
- Contributed to the development of the company's internal sensitive data mapping.

VULNERABILITY RESEARCH AND CVE CONTRIBUTIONS

- **Chuanhuchatgpt** (GitHub Stars: 15.3K, Rewards: $1,350): CVE-2024-5982, CVE-2024-6038.
- **Neural Compressor** (Intel, GitHub Stars: 2.2K, Rewards: $800): CVE-2024-28028, CVE-2024-37181.
- **PopojiCMS** : CVE-2021-28070, CVE-2021-28934.
- **EDUSRC** (China Education Security Response Center): Discovered 24 valid vulnerabilities, including 5 high-severity issues.

SELETED AWARDS AND HONERS

- Grand Prize, 2021 C4-Network Technology Challenge (Total $4,000 award across teams).
- First Prize, East China Preliminary Round, 2021 C4-Network Technology Challenge.
- Second-Class Academic Scholarship, 2019-2020 Academic Year, Nanjing University of Aeronautics and Astronautics.
- 2nd Place in the 5th Information Security Skills Competition, Nanjing University of Aeronautics and Astronautics.
- 16th Jiangsu Province College Student Physics Experiment and Works Competition Excellence Award.
- Third Prize in the 9th Science and Technology Innovation Fund Project, School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics.

SELF-EVALUATION

- **Extensive Cybersecurity Experience:** Possess approximately 2 years of professional experience in cybersecurity, successfully identified 6 CVE vulnerabilities, accumulated a total of $2150 in bug bounties, and was awarded a national-level competition's special prize.
- **Solid Research Background:** Published 1 CCF-B ranked academic paper, and have 5 preprint articles (with some submitted for review/actively preparing for submission).
- **Excellent Programming Skills:** Capable of rapidly translating research ideas into code implementations; possess practical industrial-level project development experience; independently responsible for experimental implementations of multiple academic papers; and experienced in developing and auditing open-source projects.