PING HE

✉ gnip@zju.edu.cn, https://gnipping.github.io/

Rm. 320, Cao Guang Biao Main Building, Yuquan Campus, Zheda Road 38, Hangzhou, China, 310027

EDUCATION

Zhejiang University, Hangzhou, China — September 2022 - Present

Ph.D. in Computer Science and Technology, College of Computer Science and Technology

Supervisor: Prof. Shouling Ji.

Zhejiang University, Hangzhou, China — September 2018 - June 2022

B.E. in Information Security, College of Computer Science and Technology — GPA: 91.44/100.00

RESEARCH INTERESTS

I am broadly interested in computer security and machine learning. My research bridges the domains of computer security and machine learning, particularly emphasizing the intersection of AI with computer security. Presently, I am investigating the security vulnerabilities of AI-driven systems. Parallelly, I am passionate about leveraging AI to fortify security applications.

PUBLICATIONS

[1] **Efficient Query-Based Attack Against ML-Based Android Malware Detection Under Zero Knowledge Setting.** Ping He, Yifan Xia, Xuhong Zhang, and Shouling Ji.
In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (**CCS**), November 2023.

[2] **Static Semantics Reconstruction for Enhancing JavaScript-WebAssembly Multilingual Malware Detection.** Yifan Xia, Ping He, Xuhong Zhang, Peiyu Liu, Shouling Ji, and Wenhai Wang.
In *Computer Security–ESORICS 2023: 28th European Symposium on Research in Computer Security* (**ESORICS**), September 2023.

[3] **Towards Understanding Bogus Traffic Service in Online Social Networks.** Ping He, Xuhong Zhang, Changting Lin, Ting Wang, and Shouling Ji.
In *Frontiers of Information Technology & Electronic Engineering* (**FITEE**), March 2024.

[4] **BaDExpert: Extracting Backdoor Functionality for Accurate Backdoor Input Detection.** Tinghao Xie, Xiangyu Qi, Ping He, Yiming Li, Jiachen T. Wang, Prateek Mittal.
In *the Twelfth International Conference on Learning Representations* (**ICLR**), May 2024.

SERVICES

Reviewer Service

- **[TIFS]** IEEE Transactions on Information Forensics and Security: 2023, 2024
- **[TIP]** IEEE Transactions on Image Processing: 2023

Extenral Reviewer

- **[CCS]** The ACM Conference on Computer and Communications Security: 2022, 2023, 2024
- **[USENIX Security]** USENIX Security Symposium: 2024
- **[IJCAI]** International Joint Conference on Artificial Intelligence: 2023
- **[FITEE]** Frontiers of Information Technology & Electronic Engineering: 2024
- **[IEEE DSC]** IEEE Conference on Dependable and Secure Computing: 2022
- **[TIIS]** KSII Transactions on Internet and Information Systems: 2021

SKILLS

Machine Learning: Familiar with scikit-learn, PyTorch.

Program Analysis: Android application reverse engineering.

Programming Language: Fluent in Python, Java, C/C++. Experienced in x86_64, arm, RISC-V assembly language.

Languages: English, Chinese (native)

SELECTED HONORS AND AWARDS

Graduate with Merit A Performance, Zhejiang University 2023

Outstanding Bachelor Thesis, College of Computer Science and Technology of Zhejiang University 2022

Research Rising Star in Undergraduate Student, College of Computer Science and Technology of Zhejiang University 2021

Provincial Scholarships, The People's Government of Zhejiang Province 2020

First Class Prize, National Mathematics Competition for College Student 2019

TALKS

2023. 11 **Presenter, ML Application Session, CCS 2023**

Efficient Query-Based Attack Against ML-Based Android Malware Detection Under Zero Knowledge Setting

2024. 04 **Speaker, SJTU-CS GLOBAL LUNCH SEMINAR SERIES, SJTU**

On the Robustness of ML-Based Android Malware Detector