PING HE

✉ gnip@zju.edu.cn, 🌐 https://gnip.website/

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: Dr. Shouling Ji.

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

B.E. in Information Security, College of Computer Science and Technology — GPA: 91.62/100.00

RESEARCH INTERESTS

I am broadly interested in computer security and machine learning. My research bridges the domains of computer security and AI, particularly emphasizing the intersection of machine learning 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.

> This research introduces AdvDroidZero, which is an efficient query-based attack framework for generating adversarial Android malware under zero knowledge setting. AdvDroidZero employs within an innovative data structure termed perturbation selection tree utilizing perturbation semantics to optimize the perturbation selection. Furthermore, we propose an innovative approach to gauge attack costs by measuring implementation time, and evaluate AdvDroidZero against various mainstream ML-based Android malware detection methods, in particular, state-of-the-art such methods and real-world antivirus solutions.

[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.

> This research proposes JWBinder, a novel framework aimed at enhancing the static detection of JavaScript-WebAssembly Multilingual Malware (JWMM) which is a new type of malware integrating WebAssembly into its primary JavaScript component. JWBinder builds a unified structure termed Inter-language Program Dependency Graph to characterizes the functionalities of JWMM by capturing the cross-language interoperations. Our evaluation indicates that JWBinder substantially enhances the capabilities of existing real-world antivirus solutions in detecting JWMM.

[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**), June 2023.

> This research conducts the first large-scale analysis on the bogus traffic service in online social networks. We design an NLP-based method to detect the bogus traffic accounts by capturing their linguistic differences. By deploying the method, we uncover 296,916 topics potentially linked to the bogus traffic. Moreover, we elucidate the operational mechanisms of bogus traffic services, examining both the attack cycle and the entities involved.

[4] BaDExpert: Extracting Backdoor Functionality for Accurate Backdoor Input Detection. Tinghao Xie, Xiangyu Qi, Ping He, Yiming Li, Jiachen T. Wang, and Prateek Mittal.

In *the Twelfth International Conference on Learning Representations* (**ICLR**), May 2024.

> This research proposes BaDExpert, a novel backdoor defense method for detecting the backdoored inputs. BaDExpert leverages inference consistency of a backdoor expert model only preserving the backdoor functionality with the original backdoored model to filter out the backdoored inputs during model inference. Our evaluation indicates that BaDExpert is effective against 17 backdoor attack on multiple datasets, including ImageNet, and model architectures, including Vision Transformer.

SERVICES

Reviewer Service

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

External Reviewer

- **[CCS]** The ACM Conference on Computer and Communications Security: 2022, 2023, 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, Machine Learning Application Session, CCS 2023**

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