Yiling He

github.com/E0HYL e0hyl.github.io heyilinge0@gmail.com

Publications

FINER | *Enhancing State-of-the-art Classifiers with Feature Attribution to Facilitate Security Analysis* CCS 2023
Yiling He, Jian Lou, Zhan Qin, Kui Ren

- Propose a formalization of the ERDS to establish explanation desiderata for security analysis. Propose to address the fidelity and intelligibility problems by explanation-guided model updating and IC-based explanation ensemble.
- Implement the framework FINER to promote data-driven risk detection classifiers into ERDS with high-fidelity and high-intelligibility explanations, which can meet the needs of different stakeholders at each stage of building an ERDS, and we make the dataset and code open-source.
- Evaluate FINER with three critical risk detection tasks and six representative FA methods, showing that explanation fidelity is improved across all ERDS settings, i.e., different combinations of the classifier and explainer. Demonstrate that FINER outperforms a state-of-the-art tool in localizing malware functions.

DeUEDroid | *Detecting Underground Economy Apps Based on UTG Similarity* ISSTA 2023
Zhuo Chen, Jie Liu, Yubo Hu, Lei Wu, Yajin Zhou, **Yiling He**, Xianhao Liao, Ke Wang, Jink Li, Zhan Qin

- Proposed a novel approach to effectively and efficiently detect underground economy apps (UEware for short) based on UTG similarity, including a novel technique that can cover new UI features and statically build precise UTG, and a novel algorithm that can efficiently embed UTG with differentdimension attributes.
- Implemented a prototype named DeUEDroid. The evaluation results demonstrate the effectiveness and efficiently of the system, with 98.22% UEware detection F1-score and 98.97% classification accuracy, and it is capable of performing large-scale detection to mitigate the real-world threats.
- Built up the first large-scale ground-truth UEware dataset with 1,700apps. We have released our system and the dataset on github to engage the community.

Msdroid | *Identifying Malicious Snippets for Android Malware Detection* TDSC 2022
Yiling He, Yiping Liu, Lei Wu, Ziqi Yang, Kui Ren, Zhan Qin

- Design a novel snippet-based Android malware detector named MsDroid, which identifies malicious snippets in malware with GNN. Each snippet is represented with a graph, encoding behavioral properties of *call graph*, *opcode*, and *permission*, and a customized training method is proposed to require no snippet labelling effort.
- Evaluate MsDroid on a dataset of more than 81K apps and conduct a comprehensive comparison with 5 baseline techniques in 4 settings. Experiments show that MsDroid reaches 97.82% testing accuracy, and is significantly more robust than state-of-the-art methods towards the zero-day threat, app evolution, and code obfuscation. Especially in *Reflection* obfuscation, the F1-score is with up to 49.52% higher.
- Propose a three-level explanation mechanism to facilitate malware analysis. It identifies suspicious API usages, visualizes malicious code with *calling heat graph* that tells questionable control flows, and gives similar behavioral snippets of known malware. The mechanism is proved useful with a family analysis and two case studies.

Experience

Reviewer | *IEEE Transactions on Dependable and Secure Computing* 2023

Internship | *Tencent Security Xuanwu Lab, Beijing, China* 2021.3 ˜2021.8
[Preprint] BrutePrint: Expose Smartphone Fingerprint Authentication to Brute-force Attack

Education and Award

Zhejiang University 2021.9 ˜2024.6
PhD of Cyberspace Security *Outstanding Graduate Student for the 2021 Academic Year; Academic Scholarship*
Zhejiang University 2019.9 ˜2021.6
Master of Cyberspace Security *Outstanding Graduate Student for the 2019 Academic Year*
Beijing University of Posts and Telecommunications 2015.9 ˜2019.6
Bachelor of Information Security *Outstanding Graduation Thesis Award in Beijing*