Song Liu

Ph.D. Student in Informatics

EDUCATION

The Pennsylvania State University

Xiamen University *B.E. in Computer Science and Technology*

CONFERENCE PROCEEDINGS

- VIPER: Spotting Syscall-Guard Variables for Data-Only Attacks. Hengkai Ye, Song Liu, Zhechang Zhang, and Hong Hu. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 2023).
- [2] Can We Trust the Phone Vendors? Comprehensive Security Measurements on the Android Firmware Ecosystem.
 Qinsheng Hou, Wenrui Diao, Yanhao Wang, Chenglin Mao, Lingyun Ying, Song Liu, Xiaofeng Liu, Yuanzhi Li, Shanqing Guo, Meining Nie, and Haixin Duan.
 In *IEEE Transactions on Software Engineering (TSE 2023)*.
- [3] Detecting Logical Bugs of DBMS with Coverage-based Guidance.
 Yu Liang, Song Liu, and Hong Hu.
 In Proceedings of the 31st USENIX Security Symposium (USENIX Security 2022).
- [4] Large-scale Security Measurements on the Android Firmware Ecosystem. Qinsheng Hou, Wenrui Diao, Yanhao Wang, Xiaofeng Liu, Song Liu, Lingyun Ying, Shanqing Guo, Yuanzhi Li, Meining Nie, and Haixin Duan. In 44th IEEE/ACM International Conference on Software Engineering (ICSE 2022).

INDUSTRIAL CONFERENCE

 One Flip is All It Takes: Identifying Syscall-Guard Variables for Data-Only Attacks. Hengkai Ye, Song Liu, Zhechang Zhang, and Hong Hu. In Black Hat Asia Briefings (Black Hat Asia 2024).

WORK EXPERIENCE

QI-ANXIN Technology Research Institute

Research and Development Engineer, Mentor: Dr. Lingyun Ying

- Designed a macOS sandBox system to analyze malware behavior and network traffic.
- Developed an infrastructure for large-scale continuous fuzzing.
- Developed static analysis and UI automation testing tools for Android applications.
- Maintained and optimized a graph database cluster for efficient component dependency analysis.
- Implemented an Android firmware patch existence verification tools.
- Applied BiLSTM-CRF model to extract vulnerability information from CVE text descriptions.

Institute of Information Engineering, Chinese Academy of Sciences

Research Intern, Advisor: Feng Li

• Detected IO2BO vulnerability using concolic execution.

COMMUNITY SERVICE

External Reviewer:

USENIX Security Symposium (USENIX Security) Network and Distributed System Security Symposium (NDSS) ACM Conference on Computer and Communications Security (CCS)

• Teaching Assistant:

Xiamen, China Sep 2015 - Jun 2019

Aug 2022 - Now

Beijing, China Jul 2018 - Sep 2018

Beijing, China Aug 2019 - Aug 2022

[2025] [2023, 2024, 2025] [2022, 2024]



PROJECTS

- CTF Wiki: The CTF Wiki is an open source knowledge base about CTF competitions (github, 8.4k stars).
- Awesome-Binary-Similarity: An awesome list of binary code similarity papers (github, 534 stars).
- Awesome-Binary-Rewriting: An awesome list of binary rewriting papers (github, 227 stars).

• PyPi-Typosquatting-Graph: Analyzing and visualizing typosquatting for Python packages hosted on PyPi.org (github).

VULNERABILITY DISCOVERED

- Adobe Acrobat Reader: CVE-2023-21610
- SQLite: [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58]