Song Liu

songliu@psu.edu
vancir.github.io
814-321-6052

Education

The Pennsylvania State University — Pennsylvania, USA
Ph.D. Student in Informatics — *Aug 2022 - Now*

Xiamen University — Xiamen, China
B.E. in Computer Science and Technology — *Sep 2015 - Jun 2019*

Conference Proceedings

[1] Optimizating Directed Greybox Fuzzing.
Song Liu, Hengkai Ye, and Hong Hu.
Note: the paper is still under submission and the title is the research goal.

[2] 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)*.

[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

[1] 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 — Beijing, China
Research and Development Engineer, Mentor: Dr. Lingyun Ying — *Aug 2019 - Aug 2022*

- 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.

Institute of Information Engineering, Chinese Academy of Sciences — Beijing, China
Research Intern, Advisor: Feng Li — *Jul 2018 - Sep 2018*

- Detected IO2BO vulnerability using concolic execution.

Community Service

- **External Reviewer**:

USENIX Security Symposium (USENIX Security)	[2025]
Network and Distributed System Security Symposium (NDSS)	[2023, 2024, 2025]
ACM Conference on Computer and Communications Security (CCS)	[2022, 2024]

- **Teaching Assistant**:

IST 454 Computer and Cyber Forensics	[Fall 2023, Fall 2024]

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]