



EDUCATION

<b>The University of Delaware</b> <i>Ph.D Student in Computer Information Science</i>	Delaware, USA Aug 2025 - Now
<b>The Pennsylvania State University</b> <i>M.S. in Informatics</i>	Pennsylvania, USA Aug 2022 - May 2025
<b>Xiamen University</b> <i>B.E. in Computer Science and Technology</i>	Xiamen, China Sep 2015 - Jun 2019

CONFERENCE PROCEEDINGS

[1] 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] 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)*.

[3] 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

<b>QI-ANXIN Technology Research Institute</b> <i>Research and Development Engineer, Mentor: Dr. Lingyun Ying</i>	Beijing, China Aug 2019 - Aug 2022
<ul style="list-style-type: none"><li>Designed a macOS sandBox system to analyze malware behavior and network traffic.</li><li>Developed an infrastructure for large-scale continuous fuzzing.</li><li>Developed static analysis and UI automation testing tools for Android applications.</li><li>Maintained and optimized a graph database cluster for efficient component dependency analysis.</li><li>Implemented an Android firmware patch existence verification tools.</li></ul>	
<b>Institute of Information Engineering, Chinese Academy of Sciences</b> <i>Research Intern, Advisor: Feng Li</i>	Beijing, China Jul 2018 - Sep 2018
<ul style="list-style-type: none"><li>Detect IO2BO vulnerability using concolic execution.</li></ul>	

COMMUNITY SERVICE

<b>External Reviewer:</b> USENIX Security Symposium (USENIX Security) Network and Distributed System Security Symposium (NDSS) ACM Conference on Computer and Communications Security (CCS)	[2025] [2023, 2024, 2025] [2022, 2024]
<b>Teaching Assistant:</b> 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]
- ModelScope:** #1454 #1455