

Chenxiong Qian

+852-53136100 — cqian@cs.hku.hk — GoogleScholar — <https://i.cs.hku.hk/cqian/>

Research Interest — Security, Program Analysis, Software Engineering, Operating Systems

Education

| | |
|---|------|
| The Georgia Institute of Technology <i>PhD of Computer Science</i> Supervisors: Wenke Lee and William Harris | 2021 |
| Nanjing University <i>Bachelor of Software Engineering</i> | 2013 |

Awards

| | |
|--|-------------|
| Early Career Award (University Grants Committee) | 2024 – 2025 |
|--|-------------|

Grants

| | |
|--|-------------|
| ECS, <i>Improving Security and Performance in Post-Deployment Environments</i> , <u>1,030K HKD</u> | 2024 – 2027 |
| NSFC, <i>Software Debloating via Dynamic Code Managing</i> , <u>300K CNY</u> | 2023 – 2025 |

Services

TPC Member – CCS (2025), USENIX Security (2023, 2024), ACSAC (2023, 2024), SecureComm (2023, 2024)
Reviewer – Computers & Security, TDSC, TOSEM

Publications

- Qingyu Zhang, Jiayi Lin, Chenxin Sun, Chenxiong Qian, and Xiapu Luo. CherryPicker: A Parallel Solving and State Sharing Hybrid Fuzzing System. *IEEE Transactions on Dependable and Secure Computing (TDSC 25)*.
- Junzhe Li, Ran Shu, Jiayi Lin, Qingyu Zhang, Ziyue Yang, Jie Zhang, Yongqiang Xiong, Chenxiong Qian. Daredevil: Rescue Your Flash Storage from Inflexible Kernel Storage Stack. *Twentieth European Conference on Computer Systems (EuroSys 25)*.
- Jiayi Lin, Qingyu Zhang, Junzhe Li, Chenxin Sun, Changhua Luo, Hao Zhou, & Chenxiong Qian. Automatic Library Fuzzing through API Relation Evolvment. *32nd Network and Distributed System Security Symposium (NDSS 25)*.
- Jiang, J., Li, Z., Qin, H., Jiang, M., Luo, X., Wu, X., Wang, H., Tang, Y., Qian, C., & Chen, T.. Unearthing Gas-Wasting Code Smells in Smart Contracts with Large Language Models. *IEEE Transactions on Software Engineering (TSE 24)*.
- Chenxin Sun, Kai Ye, Liangcai Su, Jiayi Zhang, & Chenxiong Qian. Invisibility Cloak: Proactive Defense Against Visual Game Cheating. *33rd USENIX Security Symposium (SEC 24)*.
- Zhou, H., Wu, S., Qian, C., Luo, X., Cai, H., & Zhang, C.. Beyond the Surface: Uncovering the Unprotected Components of Android Against Overlay Attack. *31st Network and Distributed System Security Symposium (NDSS 24)*.
- Jing, P., Cai, Z., Cao, Y., Yu, L., Du, Y., Zhang, W., Qian, C., Luo, X., Nie, S., & Wu, S.. Revisiting Automotive Attack Surfaces: a Practitioners' Perspective. *2024 IEEE Symposium on Security and Privacy (SP 24)*.

8. Wu, S., Li, J., Zhou, H., Fang, Y., Zhao, K., Wang, H., Qian, C., & Luo, X.. CydiOS: A Model-Based Testing Framework for iOS Apps. *32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 23)*.
9. Oh, C., Lee, S., Qian, C., Koo, H., & Lee, W.. DeView: Confining Progressive Web Applications by Debloating Web APIs. *38th Annual Computer Security Applications Conference (ACSAC 22)*.
10. Qian, C., Koo, H., Oh, C., Kim, T., & Lee, W.. Slimium: Debloating the Chromium Browser with Feature Subsetting. *2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 20)*.
11. Xue, L., Qian, C., Zhou, H., Luo, X., Zhou, Y., Shao, Y., & Chan, A.. NDroid: Toward Tracking Information Flows Across Multiple Android Contexts. *IEEE Transactions on Information Forensics and Security (TIFS 19)*.
12. Qian, C., Hu, H., Alharthi, M., Chung, P., Kim, T., & Lee, W.. RAZOR: a framework for post-deployment software debloating. *28th USENIX Conference on Security Symposium (SEC 19)*.
13. Yu, L., Luo, X., Qian, C., Wang, S., & Leung, H.. Enhancing the Description-to-Behavior Fidelity in Android Apps with Privacy Policy. *IEEE Transactions on Software Engineering (TOSE 18)*.
14. Hu, H., Qian, C., Yagemann, C., Chung, S., Harris, W., Kim, T., & Lee, W.. Enforcing Unique Code Target Property for Control-Flow Integrity. *2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 18)*.
15. Xu, M., Qian, C., Lu, K., Backes, M., & Kim, T.. Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels. *2018 IEEE Symposium on Security and Privacy (SP 18)*.
16. Wei Meng, Chenxiong Qian, Shuang Hao, Kevin Borgolte, Giovanni Vigna, Christopher Kruegel, & Wenke Lee. Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks. *27th USENIX Security Symposium (SEC 18)*.
17. Fratantonio, Y., Qian, C., Chung, S., & Lee, W.. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. *2017 IEEE Symposium on Security and Privacy (SP 17)*.
18. Ren Ding, Chenxiong Qian, Chengyu Song, Bill Harris, Taesoo Kim, & Wenke Lee. Efficient Protection of Path-Sensitive Control Security. *26th USENIX Security Symposium (SEC 17)*.
19. Xu, M., Song, C., Ji, Y., Shih, M.W., Lu, K., Zheng, C., Duan, R., Jang, Y., Lee, B., Qian, C., Lee, S., & Kim, T.. Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques. *ACM Comput. Surv.*
20. Yu, L., Luo, X., Qian, C., & Wang, S. Revisiting the Description-to-Behavior Fidelity in Android Applications. *2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*.
21. Qian, C., Luo, X., Le, Y., & Gu, G.. VulHunter: Toward Discovering Vulnerabilities in Android Applications. *IEEE Micro*.
22. Xue, L., Qian, C., & Luo, X.. AndroidPerf: A cross-layer profiling system for Android applications. *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)*.
23. Shao, Y., Luo, X., & Qian, C.. RootGuard: Protecting Rooted Android Phones. *Computer*.
24. Shao, Y., Luo, X., Qian, C., Zhu, P., & Zhang, L.. Towards a scalable resource-driven approach for detecting repackaged Android applications. *30th Annual Computer Security Applications Conference (ACSAC 14)*.
25. Luo, X., Xue, L., Shi, C., Shao, Y., Qian, C., & Chan, E.. On Measuring One-Way Path Metrics from a Web Server. *2014 IEEE 22nd International Conference on Network Protocols*.

26. Qian, C., Luo, X., Shao, Y., & Chan, A.. On Tracking Information Flows through JNI in Android Applications. *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 14)*.