




# Xiao Yi

✉ yx019@ie.cuhk.edu.hk

☎ +852 56230606

📍 826B, Ho Sin-Hang Engineering Building, CUHK, Hong Kong SAR

## Education

- 2019/08 – 2023/07  **Ph.D., Information Engineering**, The Chinese University of Hong Kong.  
Thesis title: *Towards a Systematic Framework for Understanding and Detecting Blockchain System Vulnerabilities*.
- 2017/09 – 2019/01  **M.Sc., Computer Science**, Boston University.
- 2013/09 – 2017/06  **B.Eng., Software Engineering**, Xi'an Jiaotong University.

## Employment

- 2019/08 – present  **Research & Teaching Assistant**, Department of Information Engineering, CUHK. Advisor: Prof. Daoyuan Wu & Prof. Kehuan Zhang.
- 2018/06 – 2019/05  **Research Assistant**, School of Engineering and Applied Sciences, Harvard. Advisor: Prof. Boris Kozinsky.
- 2017/10 – 2019/05  **Research Assistant** (part-time), School of Government, Harvard. Advisor: Prof. Nadiya Kostyuk.
- 2015/05 – 2017/06  **Research Assistant**, MOE Key Lab for Intelligent Networks and Network Security, XJTU. Advisor: Prof. Chao Shen.

## Research Publication

### Conference Proceeding

- 1 Fang, Y., Wu, D., **Yi, X.**, Wang, S., Chen, Y., Chen, M., ... Jiang, L. (2023). Beyond “protected” and “private”: An empirical security analysis of custom function modifiers in smart contracts. In *Proc. ACM ISSTA*. CCF-A.
- 2 **Yi, X.**, Fang, Y., Wu, D., & Jiang, L. (2023). BlockScope: Detecting and investigating propagated vulnerabilities in forked blockchain projects. In *Proc. ISOC NDSS*. CCF-A.
- 3 **Yi, X.**, Wu, D., Jiang, L., Fang, Y., Zhang, K., & Zhang, W. (2022). An empirical study of blockchain system vulnerabilities: Modules, types, and patterns. In *Proc. ACM ESEC/FSE*. CCF-A.
- 4 Jia, Z., Shen, C., **Yi, X.**, Chen, Y., Yu, T., & Guan, X. (2017). Big-data analysis of multi-source logs for anomaly detection on network-based system. In *Proc. IEEE CASE*.
- 5 Shen, C., Li, Y., Yu, T., Yuan, S., **Yi, X.**, & Guan, X. (2016). Motion-sensor behavior analysis for continuous authentication on smartphones. In *Proc. IEEE WCICA*.

### arXiv Preprint



- 1 Yang, X., Wu, D., **Yi, X.**, Lee, J. H. M., & Lee, T. (2022). iExam: A novel online exam monitoring and analysis system based on face detection and recognition. In *CoRR arXiv* (Vol. abs/2206.13356).
- 2 Chen, M., Wu, D., **Yi, X.**, Xu, J., & Gao, D. (2021). A blockchain-based gateway for trustworthy App delegation from mobile App markets. In *CoRR arXiv* (Vol. abs/2101.06454).

### Under Review

- 1 Zhang, Z., Ma, H., Wu, D., Gao, D., **Yi, X.**, Chen, Y., ... Jiang, L. (2023). *Pinpointing insecure open-source method clones in Android apps via source-to-bytecode signature generation and search*. Under review in RAID 2023.






## Project Highlight

---

- BlockScope (in NDSS'23)      (i) Proposed an **effective and efficient** tool for vulnerable code clone detection;  
(ii) Discovered **101** cloned vulnerabilities in 16 Bitcoin/Ethereum's forked projects and reported them to their developers – most of them received positive responses;  
(iii) Obtained **two new CVEs** (CVE-2021-37491 of Dogecoin and CVE-2021-37492 of Ravencoin) and a **bug bounty reward** from Binance;  
(iv) Provided a **deep investigation** on the propagation and patching processes of the discovered vulnerabilities.
- BlockVuln (in ESEC/FSE'22)      (i) Proposed a vulnerability filtering framework to effectively identify **1,037** vulnerabilities and their **2,317** patches from 34,245 issues/PRs and 85,164 commits on GitHub;  
(ii) Revealed that the modules related to **consensus, wallet, and networking** are highly susceptible;  
(iii) Identified that around **70% of blockchain vulnerabilities are in traditional types**, but we also identify four new types specific to blockchains;  
(iv) Obtained **21 blockchain-specific vulnerability patterns** and demonstrated that they could be applied to detect similar vulnerabilities in other top blockchains.

## Teaching Assistant

---

- 22'F, 20'F, 19'F      IEMS 5710: Cryptography, Information Security and Privacy.  
23'S, 22'S      IERG 4210: Web Programming and Security.  
21'F      IERG 4130: Introduction to Cyber Security.  
21'S      IEMS 5722: Mobile Network Programming and Distributed Server Architecture.  
20'S      CSCI 2100: Data Structures and Algorithms.

## Reference

---

Available on Request