XIANG LI

GitHub ⋄ Google Scholar ⋄ ORCID ⋄ Homepage ⋄ sean.lixiang97@gmail.com

RESEARCH INTERESTS

I aim to develop secure and reliable systems that protect users from vulnerabilities using Large Language Models. My research interest lies in **System Security**, with a focus on ***Linux Kernel Fuzzing*** recently. I have participated in several projects, including an LLM-Driven Kernel Fuzzing Framework(*Sneakoscope*), and Storage-Efficient Kernel Fuzzer Optimization(*Remembrall*). Before joined CityUHK, my research specifically lie on mitigating software/hardware security threats using ***Trusted Experiment Environment(TEE)***, which include distributed confidential computing(*TDSC'24a, ICICS'24, GLOBECOM'20, Patent'23ab*), hardware vulnerability mitigation(*USENIX'24, TDSC24'b, Exocist*).

EDUCATION

Xidian University	Aug 2019 - Jun 2022
M.Eng. with Thesis in Cyber Security(GPA: 86.49/100)	*Supervisor: Zheng YAN*
Imperial College London	July 2019 - August 2019
Summer School in Data Science Institute	*Supervisor: Yike GUO*
Nanyang Technological University	Jan 2019 - Jan 2019
Winter Exchange Student	*Supervisor: Kwok Yan LAM*
Xidian University	Aug 2015 - Jun 2019
B.Eng. in Information Security(GPA 3.4/4.0)	

HONORS AND AWARDS

Outstanding Master Student of Xidian University	Top 12%
Outstanding Bachelor Graduate in Xidian University	Top 5%
Excellent Undergraduate Thesis of Xidian University	Top 8%
DARPA's Artificial Intelligence Cyber Challenge Compitition	Finalist Team Member
Interdisciplinary Contest In Modeling	Honorable Mention
National Cryptography Competition	Third Prize
China Undergraduate Mathematical Contest in Modeling	First Prize in Shaanxi District

PUBLICATIONS AND PATENTS

(*indicates corresponding author)

[1]DMA: Mutual Attestation Framework for Distributed Enclaves
Peixi Li, Xiang Li*, Liming Fang*
International Conference on Information and Communications Security (ICICS), 2024 **(Rank: CCF-C)**

[2]Ensuring State Continuity for Confidential Computing: A Blockchain-based Approach
Wei Peng, Xiang Li, Jianyu Niu, Xiaokuan Zhang and Yinqian Zhang*
IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) 2024 **(Rank: CCF-A)**

[3]MaTEE: Efficiently Bridging the Semantic Gap in TrustZone via ARM Pointer Authentication
Shiqi Liu, Xiang Li, Jie Wang*, Yongpeng Gao, Jiajin Hu
IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 2024 **(Rank: CCF-A)**

[4]Peep With A Mirror: Breaking The Integrity of Android App Sandboxing via Unprivileged Cache Side Channel
Yan Lin, Joshua Wong, Xiang Li, Haoyu Ma*, Debin Gao
In Proceedings of the USENIX Security 2024 **(Rank: CCF-A, Top4 Computer Security Conference)**

[5]Flexible and Privacy-preserving Framework for Decentralized Collaborative Learning
Zhuoran Ma, Jianfeng Ma, Yinbin Miao*, Ximeng Liu, Wei Zheng, Xiang Li
In Proceedings of the IEEE Global Communications Conference (GLOBECOM) 2020 **(Rank: CCF-C)**

[6]Rememberall: Efficient Kernel Fuzzing via Dependency-Aware Checkpointing *(Manuscript in Preparation)*
Xiang Li and Heqing Huang

[7]Exorcist: Kernel-Level Detection and Mitigation of Spectre Vulnerabilities via Precise Event Based Sampling *(Draft completed to be submitted)*
Xiang Li, Haoyu Ma, Chang Liu and Debin Gao

[8]Decentralized crowdsourcing methods, systems and terminals that support efficient privacy protection(in Chinese) Patent Granted
Xiang Li, Zheng Yan
Invention Grant, CN114826684B

[9]Decentralized crowdsourcing methods, systems and terminals that support attribute privacy protection(in Chinese) Patent Granted
Xiang Li, Zheng Yan
Invention Grant, CN114826572B

[10]White Paper: Security and Privacy of Generative Large Language Models
Xiaogang Xu, Huiwen Wu, Zhusen Liu, Xiang Li, Wenxuan Tu, Weixuan Liang, Yi Zhang, Zhe Liu
Technical Report for Zhejiang Lab

RESEARCH EXPERIENCE

City University of Hong Kong

Research Assistant to Prof. Heqing HUANG *August 2024 - present*

- **LLM-Driven system-call sequence analyzer of Linux Vulnerabilities based on Syzkaller**
  - Designed a LLM-driven system-call sequence analyzer based on Syzkaller, automatically detecting specifically vulnerabilities(e.g. Out-of-Bounds Write) automatically.
  - Proposed a new primitive ***LLM-driven syscall selection method*** to reduce the search space for syscall sequences(i.e. Test case in Syzkaller).
  - Developed ***Sneakoscope***, an one-click deployment of automated kernel vulnerability discovering tools, which contributed to DARPA's Artificial Intelligence Cyber Challenge Compitition Finalist.
- **Optimizing Storage-Efficient Kernel Fuzzer with Dependency-Aware Checkpointing**
  - Designed ***Remembrall***, a kernel fuzzer with Storage-Efficient optimization, achieving 1.47x throughput gains via checkpoints selective creation.
  - Proposed a new primitive ***Dynamic Syscall Tree*** to search syscall sequences intuitively and assist checkpoint creation rapidly.
  - Explored methods in creating checkpoints with validation and scheduling valid checkpoints to reduce the checkpoint search space.

Alibaba DAMO Academy, OS Lab

Research Intern to Mr. Jia ZHANG *Aug 2023 - May 2024*

- **Enclave-CC: Process-level confidential container based on TEE**
  - Participated in the Enclave-cc open-source project of the openAnolis community.
  - Developed the SDK, which modified containerd shim and runc components to support Intel TDX.
  - Engaged in the CoCo (Confidential Container) open-source community communication work.

Zhejiang Lab

Senior Research Assistant to Dr. Haoyu MA *Jan 2023 - August 2023*

- **Kernel-Level Detection and Mitigation of Spectre Vulnerabilities**
  - Developed tools with real-time monitoring Spectre Vulnerabilities utilizing Intel Precise Event Based Sampling(PEBS), providing a precisely kernel-level detection method.
  - Proposed mitigation methods to defense against transient execution vulnerabilities, which request a patch request in OS community, improving the runtime mitigation overhead of 36.8%.
- **Mutual Attestation Framework for Distributed Enclaves**

- Explored a system to enhance remote attestation with strong freshness binding.
- Utilized consensus algorithms to overcome limitations of centralized trust determination.
- Implemented a prototype demonstrating the scalability and efficiency of decentralized design.

- **Detection and Mitigation of Vulnerabilities in ARM TrustZone**
  - Explored a system to address Semantic Gap Vulnerabilities(SGVs) in Arm TrustZone by utilizing Arm Pointer Authentication(PA) to bind requests to CA identities and verify them.
  - Conducted experiments showing that we effectively isolates sensitive data of different CAs, while demonstrating strong defense against SGVs with minimal runtime overhead of 2.19%.

Southern University of Science and Technology(SUSTech), Teecert Lab

Research Assistant to Prof. Yinqian ZHANG *May 2022 - Dec 2022*

- **Ensuring State Continuity for Confidential Computing with Blockchain-based Approach**
  - Developed the deployment of tendermint in the cloud, refactored and open-sourced the code.

Huawei Ltd, 2012Lab

Research Intern to Dr. Lijing ZHOU *Jul 2021 – Sep 2021*

- **Batch verification signature algorithms for HUAWEI Blockchain**
  - Proposed algorithms with random number generation function for Huawei Blockchain signature algorithms.
  - Developed the batch verification protocol for ECDSA and Ed25519 signature algorithms with 19.8% optimization.

Xidian University

Research Assistant to Prof. Zheng YAN *Aug 2018 – Jun 2022*

- **Node Attribute Privacy Preservation in Decentralized Crowdsourcing**
  - Designed two decentralized crowdsourcing privacy schemes (EDCP and ADCP) leveraging SGX and CP-ABE technologies to address node attribute leakage, achieving efficient task matching (O(logn) complexity) and dynamic attribute revocation.
  - Enhanced system efficiency by 32.9% via a blockchain-optimized batch verification algorithm and comprehensive task management architecture with trust evaluation and correlation verification mechanisms.
  - Implemented and validated solutions on Hyperledger Fabric, demonstrating superior robustness and confidentiality over existing systems through large-scale simulations (2,500+ tasks).

LEADERSHIP AND COMMUNITY SERVICES

Class Monitor of Undergraduates Class 1518012	2015-2019
Outstanding Student Leader	2016-2019
Director of External Relations Department, Student Union	2016-2017
Director of Academic Department, Graduate Student Union	2020-2021
Volunteer Service for	
the 10th National College Student Information Security Contest	Jul 2017
Advanced Individual and Outstanding Practice Team of	
Xidian University Summer Student Social Practice Activity	Oct 2017

ACADEMIC SERVICES

Subreviewer for *ICICS 2023*

SKILLS

C/C++: Linux Kernel; Go: Syzkaller; Go: Confidential Containers; Python; LaTeX