Dr. Weijie **Liu**

weijieliu@nankai.edu.cn

Appointments

Nankai University — *Tianjin, China*
Associate Professor — *Jun. 2024 - Present*

Ant Group — *Beijing, China*
Tech. Expert — *Nov. 2021 - May. 2024*

Indiana University Bloomington — *Bloomington, IN, U.S.*
Research Associate — *Jan. 2019 - Sept. 2022*

- Postdoc fellowship; Research topic: Confidential Attestation; Advisor: Prof. **XiaoFeng Wang** and Prof. **Haixu Tang**

Tencent — *Shenzhen, China*
Research Fellow — *Jul. 2018 - Dec.2018*

Education

Wuhan University — *Wuhan, China*
Ph.D. in Information Security — *Sept. 2012 - Jun. 2018*

- Research area: Virtualization Security Enhancement, Advisor: Prof. **Lina Wang**

Singapore Management University — *Singapore*
Visiting student — *Aug. 2015 - Nov.2016*

- Research topic: Side-channel attack mitigation in IaaS cloud; Advisor: Prof. **Debin Gao** and Prof. **Mike K. Reiter**

Wuhan University — *Wuhan, China*
B.S. in Information Security — *Sept. 2008 - Jun. 2012*

Selected Publication

Full list of publications at Google Scholar.

Lost along the Way: Understanding and Mitigating Path-Misresolution Threats to Container Isolation
Zhi Li, Weijie Liu, XiaoFeng Wang, Bin Yuan, Hongliang Tian, Hai Jin, Shoumeng Yan
ACM SIGSAC Conference on Computer and Communications Security (CCS), 2023

Robbery on devops: Understanding and mitigating illicit cryptomining on continuous integration service platforms
Zhi Li, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Xiaojing Liao, Luyi Xing, Mingming Zha, Hai Jin, Deqing Zou
IEEE Symposium on Security and Privacy (Oakland), 2022

Retrofitting LBR Profiling to Enhance Virtual Machine Introspection
Weijie Liu, Ximeng Liu, Zhi Li, Bin Liu, Rongwei Yu, Lina Wang
IEEE Transactions on Information Forensics and Security (TIFS), 2022

Practical and Efficient in-Enclave Verification of Privacy Compliance
Weijie Liu, Wenhao Wang, Hongbo Chen, XiaoFeng Wang, Yaosong Lu, Kai Chen, Xinyu Wang, Qintao Shen, Yi Chen, Haixu Tang
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021

Incremental CFG Patching for Binary Rewriting
Xiaozhu Meng, Weijie Liu
International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2021

Trust beyond Border: Lightweight, Verifiable User Isolation for Protecting in-Enclave Services
Wenhao Wang, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Hongliang Tian, Dongdai Lin
IEEE Transactions on Dependable and Secure Computing (TDSC), 2021

On-Demand Time Blurring to Support Side-Channel Defense
Weijie Liu, Debin Gao, Michael K Reiter
European Symposium on Research in Computer Security (ESORICS), 2017

Presentations & Talks

Training Lecture Series — *Beijing, China*
World Privacy-preserving Computing Competition — *Sept. 2022 - Nov. 2022*

- Step by Step Run Occlum

Invited Talk — *Intel Labs*
SPR tech. talk — *Nov. 2021*

- HySec-Flow: Privacy-Preserving Genomic Computing with SGX-based Big-Data Analytics Frame

Invited Talk — *UIUC*
Weekly reading group — *Aug. 2021*

- Confidential Attestation in SGX