第四届软件与系统前沿安全国际会议

The 4th International Conference on Advanced Security on Software and Systems (ASSS)

ASSS 2025

3-5 December 2025

承办单位
桂林电子科技大学

Advanced
Security on
Software and
Systems

腾讯会议 [线上参会]
会议主题：ASSS2025
会议时间：2025/12/03 09:00-18:00 (GMT+08:00) 中国标准时间 - 北京
点击链接入会，或添加至会议列表：
https://meeting.tencent.com/dm/Pqvoeo9OKCWT
#腾讯会议：903-261-375

会议时间：**2025** 年 **12** 月 **3** 日**-12** 月 **5** 日
会议地点：桂林电子科技大学花江校区 **1** 号楼

Conference Schedule

December 03, 2025	Wednesday	桂林电子科技大学花江校区1号楼 (online)
08:00-17:00	Registration and Arrival	
December 03, 2025	Wednesday	桂林电子科技大学花江校区1号楼 (online)
09:00-09:20	Welcome General/Program Chairs	
Session 1: Keynote Speak **Session Chair**		
09:20-10:00	Keynote 1	Dr. Guangdong Bai
10:00-10:40	Keynote 2	Dr. Zhi Zhang
10:40-11:00	Tea Break	
Session 2: Decentralized Security and Applications **Session Chair**		
11:00-11:15	Privacy-Preserving Federated Learning with Knowledge Distillation for Heterogeneous IoT Nodes	Keyu Fang, Shilong Li, Chengyu Tan, Wei Luo, Xiangyang Wang, Mingrui Zhang, Lin Xu and Lei Zhang
11:15-11:30	TraceBlock: Cyberattack Traceback System Based on Blockchain	Dagula Yang, Lei Xu, Keke Gai and Liehuang Zhu
11:30-11:45	CrossBuffer: Achieving Complete Atomicity for Cross-Chain Applications via Revocable State Buffering and Order-Preserving Conflict Resolution	Bohang Wei, Yang Yang, Fuyang Deng, Minghang Li, Qianhong Wu and Bo Qin
11:45-12:00	Enhancing Long-Range Security for Proof-of-Stake Consensus via Sampleable Verifiable Delay Functions	Xuecheng Lin, Decun Luo, Qianhong Wu and Bo Qin

12:00-13:30	Lunch Break	
Session 3： Resilient Method and Authentication **Session Chair**		
13:30 - 13:45	KG-Engine: A Compliance Evaluation Framework for Cryptographic Schemes Based on Ontology-driven Knowledge Graphs	Liujing He, Chenchen Pan, Runze Han and Yue Zhao
13:45- 14:00	Automated Program Repair Based on Large Language Model and Mask Templates	Xiaohan Wu, Lili Bo, Xiaohan Jiang, and Yuting He
14:00 - 14:15	A NIC-Host Binding Method for Scalable Authentication via EEPROM Read/Write Access	Fei Wang, Jielong Liu, Zhihan Zheng, Ruqi Zhang, Mu Mu and Yu-An Tan
14:15 - 14:30	A Data Storage and Playback System for Crowdsourced Cyber-Physical Integration Scenarios	Xin Wu, Zhenyu Li, Yong Ding, Ruwen Zhao and Changsong Yang
14:30 - 15:00	Tea Break	
Social Event **15:00-17:00**		
17:00-17:30	Closing Remarks	General/Program Chairs
18:00 - 20:00	Banquet	
December 04, 2025	Thursday	
10:00-16:00	AI Workshop (by Invitation)	
December 05, 2025	Friday	
10:00-16:00	Trusted Networking Workshop (by Invitation)	

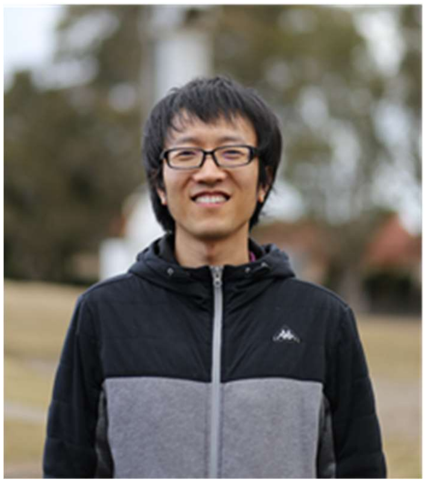
特邀报告专家：

Guangdong Bai is an Associate Professor at City University of Hong Kong. His research spans responsible machine learning, security, and privacy. He is an Associate Editor of IEEE Transactions on Dependable and Secure Computing and IEEE Transactions on Service Computing.

Title: LLMs as Bug Detectors: Extending Capabilities with Domain Knowledge

Abstract: Large Language Models (LLMs) are increasingly demonstrating significant potential in automated bug detection. Their deep semantics- and context-awareness capabilities allow them to understand complex codebases and associated documentation. However, this capability is fundamentally constrained when confronted with subtle and complex bugs, due to their hallucination or over-reliance on patterns learned from vast datasets. In this talk, we introduce our frameworks for augmenting LLMs with external knowledge. We investigate methodologies to integrate knowledge learned from domain information or relevant bug reports, to unlock LLM's capability in finding complex bugs.

EISA 2024



Zhi Zhang is a tenured Senior Lecturer at The University of Western Australia. He received his Ph.D. from The University of New South Wales. His main research interests are in hardware security and system security. He has published works in the top-4 security conferences and top-4 computer architecture conferences. He received the USENIX Security 2025 Honorable Mention Paper Award, the USENIX Security 2024 Distinguished Paper Award, and the ASIACCS 2023 Distinguished Paper Award. He serves as an Associate Editor for IEEE TDSC and on the program committees of ASPLOS, MICRO, DSN, and ASIACCS.

Title: Compromise Deep Learning through Hardware Vulnerabilities

Abstract: In today's public clouds, countless companies deploy powerful deep neural networks on popular platforms such as AWS, Azure, and Google Cloud, making machine learning as a service ubiquitous. However, this convenience comes with growing security risks. Even if the software stack is carefully hardened, shared underlying hardware can still be abused by malicious co-located tenants. In this keynote, I will focus on two such hardware attack vectors in a multi-tenant VM setting: a power side-channel attack that steals a victim's model architecture, undermining confidentiality, and a Rowhammer-based fault injection attack that degrades model inference accuracy, undermining integrity.