



RESEARCH SEMINAR

## Finding Permission Bugs in Smart Contracts with Role Mining



**Dr Yi LI**

Assistant Professor  
School of Computer Science and Engineering  
Nanyang Technological University

**Date : 20 June 2023 (Tue)**  
**Time : 3:30 pm - 4:30 pm**  
**Venue : FJ302**

### Abstract

Smart contracts deployed on permissionless blockchains, such as Ethereum, are accessible to any user in a trustless environment. Therefore, most smart contract applications implement access control policies to protect their valuable assets from unauthorized accesses. A difficulty in validating the conformance to such policies, i.e., whether the contract implementation adheres to the expected behaviors, is the lack of policy specifications. In this talk, I introduce a technique SPCon, mining past transactions of a contract to recover a likely access control model, which can then be checked against various information flow policies and identify potential bugs related to user permissions. The experimental evaluation on labeled smart contract role mining benchmark demonstrates that SPCon effectively mines more accurate user roles compared to the state-of-the-art role mining tools. Moreover, the experimental evaluation on real-world smart contract benchmark and access control CVEs indicates SPCon effectively detects potential permission bugs while having better scalability and lower false-positive rate compared to the state-of-the-art security tools, finding 11 previously unknown bugs and detecting six CVEs that no other tool can find.

### About the Speaker

Dr Yi Li is an Assistant Professor at the School of Computer Science and Engineering, Nanyang Technological University (NTU) and an Associate Director of the NTU Centre in Computational Technologies for Finance (CCTF). Dr Li has been leading the Software Reliability and Security Lab (SRSLab@NTU) since 2018. His research interests are in program analysis and automated reasoning techniques with applications in software engineering and software security. Together with his research team, he develops solutions enabling the construction of high-quality software systems that are both reliable and sustainable.

Currently, his work focuses on the security and fairness of decentralized applications and blockchain systems, as well as the robustness and dependability of AI systems. His work in these areas won three ACM Distinguished Paper Awards and two Best Artifact Awards at top-tier conferences, including ASE'15, ICSME'20, FSE'21, and ISSTA'22. He serves on the program committees of many flagship conferences in software engineering, including ICSE, FSE, and ASE. He co-chaired the program committees of ICFEM'23, ICECCS'20, SEASIS'22, and ICFEM'19 Doctoral Symposium.