THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

50th Anniversary
Department of Computing
電子計算學系

THE RESEARCH CENTRE FOR BLOCKCHAIN TECHNOLOGY

RESEARCH SEMINAR

A Road Towards an Interaction between Cyber Security and AIGC

Prof. Yang LIU
Professor
School of Computer Science and Engineering
Nanyang Technological University
Singapore

Date : 20 May 2024 (Mon)
Time : 10:30am - 11:30am
Venue : HJ303

Abstract

AIGC and cyber security entails the systematic integration of security testing throughout all phases of the software development process. The objective is to automate the security expertise of human professionals by employing tools, thereby enabling early identification and resolution of security concerns during the early phase of the development life cycle. However, its effectiveness greatly relies on the capabilities of intelligent tools to simulate or potentially replace security experts. With the emergence of LLM, a new means to accomplish this objective is now available. In this presentation, I will discuss recent endeavors in utilizing LLM within the realm of application security, to cover the complete life cycle of the vulnerability analysis: vulnerability detection, diagnosis, POC generation and repair.

On the other hand, LLM's security is equally important to make sure the successful deployment of the AI applications. In this direction, we will demonstrate the latest research works regarding the attack surface of LLM, blackbox/whitebox attack generation for prompt injection, attacks for multi-modality models, backdoor attacks, and possible defense mechanism.

Finally, we are looking at the integration of the two aspects to develop an AI-enabled platform for application security analysis.

About the Speaker

Prof. Yang Liu is currently a full professor in Nanyang Technological University, director of the cybersecurity lab, and Executive Director of CyberSG R&D Programme Office (CRPO). In 2019, he received the University Leadership Forum Chair professorship at NTU, the President's Chair in 2024. Prof. Liu specializes in software engineering, cybersecurity and artificial intelligence. His research has bridged the gap between the theory and practical usage of program analysis, data analysis and AI to evaluate the design and implementation of software for high assurance and security. Many of his research has been successfully commercialized. By now, he has more than 500 publications in top tier conferences and journals, and 25 best paper awards and one most influence system award in top software engineering conferences. He is also leading several major research centers including CRPO, Trustworthy AI in NTU and CREATE center with ICL on medical device security. He has received a number of prestigious awards including MSRA Fellowship, TRF Fellowship, Nanyang Assistant Professor, Tan Chin Tuan Fellowship, Nanyang Research Award, ACM Distinguished Speaker, NRF Investigatorship and NTU Innovator Award.