6

**Title:**

Automated Diagnosis and Fixing of Software Vulnerabilities in Cyber-Physical Systems

**Supervisors:**

Dr. Yepang Liu (SUSTech) and Dr. Yulei Sui (UTS)

**Abstract:**

Cyber-physical systems (CPS) such as autonomous driving vehicles and IoT are becoming increasingly important in modern software. Software vulnerabilities in such systems can cause subtle but severe reliability issues, such as crashes, hangs and undefined behaviours. Worse, some vulnerabilities can also be exploited by hackers to launch security attacks, resulting in catastrophic consequences. However, detecting and fixing software security vulnerabilities in CPS is a relatively unexplored research area. This project aims to makes one step forward in addressing this important yet challenging topic through systematically understanding, detecting and repairing vulnerabilities in large-scale CPS. The outcome of this project will be an advanced static and dynamic program analysis framework to improve reliability and security of industrial-strength real-world CPS. Specifically, we will first conduct large-scale empirical studies based on well-known open-source projects to understand software vulnerabilities in CPS. Through bug data (e.g., bug reports, patches and historical development data) and code analysis, we will understand the root causes of various CPS software vulnerabilities by classifying them into different categories, and learning common patterns and repairing strategies of these vulnerabilities. Based on insights from the empirical study, we will develop a new theoretical foundation for automated diagnosis and fixing of CPS software vulnerabilities by combining static and dynamic program analysis for analyzing source code and binaries of CPS software. Finally, we will implement our approach as a tool chain and evaluate its effectiveness, efficiency and practicality by performing large-scale experiments on industrial-strength real-world CPS software.