Auditing Input Validation from Assembly Code for Security Defence, Verification and Testing

Input validation – the checking of input submitted against its required properties in a program to ensure any input that does not satisfy the properties will be rejected – constitutes a major and very important requirement in most software systems. Recent reports on security attacks consistently showed most of the security attacks can be defended through preventing illegal input manipulation instead of inventing excellent security protocols or encryption methods. Adequate input validation is crucial for preventing illegal input manipulation in a software system. As input validation requirement depends on individual system, it cannot be implemented through adapting ready-made proven packages. Hence, the auditing of input validation in a software system is vital to its quality and therefore, the key for security defence.

This project aims to establish model, theory and method to automatically and comprehensively audit input validation from Assembly code of software systems for security defence, verification and testing. The project will also establish fault model for the detection of error associated with input validation implementation. In this project, we will explore on a novel research methodology that exploits the integrated use of program analysis, empirical science and reverse engineering techniques. A prototype system will be developed to provide full support to the proposed method.