Title: Detection and Prevention of Misuse of Software Components

Speaker: Mr Dai Ting

Date/Time: 28 April 2015, Tuesday, 10:00 AM to 11:30 AM

Venue: MR1, COM1-03-19

Supervisor: Dr Liang Zhenkai, Associate Professor, School of Computing
Dr Roland Yap, Associate Professor, School of Computing

Abstract:

Software components are designed for code reuse. Modern computer systems are complex integrations of these software components that encapsulate many sets of software functionalities. The complexity of these systems comes from both the interactions of the software components and various system settings. Unexpected uses of software components can be introduced into the system by such aspects of the complexity, which form the basis of a class of vulnerability that alters the goals of the original functionalities provided by the software components. We call such a vulnerability, a component misuse vulnerability.

In this thesis, we propose systematic solutions to detect and prevent the component misuse vulnerability. Binary loading behaviors in software programs can be misused due to the misunderstanding of various system settings, which causes a form of component misuse vulnerability called binary loading vulnerabilities. We develop an approach to detect binary loading vulnerabilities. It explains binary loading behaviors by listing various system settings, binaries and files that can affect the loading behaviors. It detects the unexpected uses of binary loading by identifying the factors that can be controlled by the attackers. The APIs in ActiveX controls can be misused due to the misunderstanding of component interactions, which causes another form of component misuse vulnerability called API-misuse vulnerability. We develop a mechanism to detect and prevent ActiveX API-misuse vulnerabilities in Internet Explorer (IE), by detecting unexpected uses of APIs in the component interactions. It blocks the APIs that can be misused in a fine-grained manner.

After studying the causes of the component misuse vulnerability from the two approaches, we propose a solution to mitigate the damage caused by component misuse vulnerability due to the interactions of software components in Android platform. We develop a prevention mechanism of privilege escalation in Android inter-component communication (ICC). It prevents the permission re-delegation in Android ICC that can cause the sender application (app) to gain additional privileges from the recipient app.