



Master Thesis Defense

Speaker: Hai Zhou Ling

Supervisor: Dr. Debbabi

Examining Committee: Drs. Fancott, Radhakrishnan and Dr. Paquet (Chair)

Title: Towards the Automation of Vulnerability Detection in Source Code

Date: Thursday December 3, 2009

Time: 2:00 pm.

Place: EV3.309

ABSTRACT

Software vulnerability detection, which involves security property specification and verification, is essential in assuring the software security. However, the process of vulnerability detection is labor-intensive, time-consuming and error-prone if done manually. In this thesis, we present a hybrid approach, which utilizes the power of static and dynamic analysis for performing vulnerability detection in a systematic way. The key contributions of this thesis are threefold. First, a vulnerability detection framework, which supports security property specification, potential vulnerability detection, and dynamic verification, is proposed. Second, an investigation of test data generation for dynamic verification is conducted. Third, the concept of reducing security property verification to reachability is introduced.