University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

ALEXANDER HOOLE

MASc (University of Victoria, 2006)
BSc (University of Victoria, 2003)

"Security Vulnerability Verification through Contract-Based Assertion Monitoring at Runtime"

Department of Electrical and Computer Engineering

Tuesday, October 3, 2017
1:00 P.M.
Clearihue Building
Room B007

Supervisory Committee:
Dr. Issa Traore, Department of Electrical & Computer Engineering, University of Victoria (Supervisor)
Dr. Aaron Gulliver, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Kin Fun Li, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Jens Weber, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Vojislav B. Misic, Department of Computer Science, Ryerson University

Chair of Oral Examination:
Dr. Julian Lum, Department of Biochemistry and Microbiology, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

In this dissertation we seek to identify ways in which the systems development life cycle (SDLC) can be augmented with improved software engineering practices to measurably address security concerns that have arisen relating to security vulnerability defects in software. By proposing a general model for identifying potential vulnerabilities (weaknesses) and using runtime monitoring for verifying their reachability, and exploitability, during development and testing reduces security risk in delivered products.

We propose a form of contract for our monitoring framework that is used to specify the environmental and system security conditions necessary for the generation of probes which will monitor security assertions during runtime to verify suspected vulnerabilities. Our assertion-based security monitoring framework, based on contracts and probes, known as the Contract-Based Security Assurance Monitoring Framework (CB_SAMF) can be employed for verifying and reacting to suspected vulnerabilities in the application and kernel layers of the Linux operating system. Our methodology for integrating CB_SAMF into SDLC during development and testing to verify suspected vulnerabilities reduces the human effort by allowing developers to focus on fixing verified vulnerabilities. Metrics and measurements intended for the weighting, prioritizing, level of confidence, and detectability of potential vulnerability categories are also introduced. These metrics and weighting approaches identify deficiencies in security assurance programs/products and also help focus resources towards a class of suspected vulnerabilities, or a detection method, which may presently be outside of the requirements and priorities of the system.

Our empirical evaluation demonstrates the effectiveness of using contracts to verify exploitability of suspected vulnerabilities across five input validation related vulnerability types, combining our contracts with existing static analysis detection mechanisms, and measurably improving security assurance processes/products used in an enhanced SDLC. As a result of our empirical evaluation, we introduced two new security assurance test suites, through collaborations with the National Institute of Standards and Technology (NIST), replacing existing test suites. The new and revised test cases provide numerous improvements to consistency, accuracy, and preciseness along with enhanced test case metadata to aid researchers using the Software Assurance Reference Dataset (SARD).