University of Victoria | Graduate Studies

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

of

BASSAM SAYED

MASc (University of Victoria, 2009)
BSc (Helwan University, 2003)

"Protection Against Malicious JavaScript Using Hybrid Flow-Sensitive Information Flow Monitoring"

Department of Electrical and Computer Engineering

Wednesday, February 17, 2016
8:00 A.M.
David Turpin Building
Room A136

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

External Examiner:
Dr. Olaf Owe, Department of Informatics, University of Oslo

Chair of Oral Examination:
Dr. David McCutheon, School of Business, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Modern web applications use several third-party JavaScript libraries to achieve higher levels of engagement. The third-party libraries range from utility libraries such as jQuery to libraries that provide services such as Google Analytics and context-sensitive advertisement. These third-party libraries have access to most (if not all) the elements of the displayed webpage. This allows malicious third-party libraries to perform attacks that steal information from the end-user or perform an action without the end-user consent. These types of attacks are the stealthiest and the hardest to defend against, because they are agnostic to the browser type and platform of the end-user and at the same time they rely on web standards when performing the attacks. Such kind of attacks can perform actions using the victim's browser without her permission. The nature of such actions can range from posting an embarrassing message on the victim's behalf over her social network account, to performing online biding using the victim's account. This poses the need to develop effective mechanisms for protecting against client-side web attacks that mainly target the end-user. In the proposed research, we address the above challenges from information flow monitoring perspective by developing a framework that restricts the flow of information on the client-side to legitimate channels. The proposed model tracks sensitive information ow in the JavaScript code and prevents information leakage from happening. The main component of the framework is a hybrid flow-sensitive security monitor that controls, at runtime, the dissemination of information flow and its inlining. The security monitor is hybrid as it combines both static analysis and runtime monitoring of the running JavaScript program. We provide the soundness proof of the model with respect to termination-insensitive non-interference security policy and develop a new security benchmark to establish experimentally its effectiveness in detecting and preventing illicit information flow. When applied to the context of client-side web-based attacks, the proposed model provides a more secure browsing environment for the end-user.