University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Master of Applied Science

of

ASEM GHALEB

MSc (King Fahd University of Petroleum and Minerals, 2016)
BSc (Taiz University, 2007)

"Agentless Endpoint Security Monitoring Framework"

Department of Electrical and Computer Engineering

Tuesday, May 14, 2019
10:00 A.M.
Engineering Office Wing
Room 430

Supervisory Committee:
Dr. Issa Traore, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Mihai Sima, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Jens Weber, Department of Computer Science, UVic

Chair of Oral Examination:
Dr. Timothy Iles, Department of Pacific and Asian Studies, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Existing endpoint security monitors use agents that must be installed on every computing host or endpoint. However, as the number of monitored hosts increases, agents installation, configuration and maintenance become arduous and requires more efforts. Moreover, installed agents can increase the security threat footprint and several companies impose restrictions on using agents on every computing system. This work provides a generic agentless endpoint framework for security monitoring of computing systems. The computing hosts are accessed by the monitoring framework running on a central server. Since the monitoring framework is separate from the computing hosts for which the monitoring is being performed, the various security models of the framework can perform data retrieval and analysis without utilizing agents executing within the computing hosts. The monitoring framework retrieves transparently raw data from the monitored computing hosts that are then fed to the security modules integrated with the framework. These modules analyze the received data to perform security monitoring of the target computing hosts. As a use case, a real-time intrusion detection model has been implemented to detect abnormal behaviors on computing hosts based on the data collected using the introduced framework.