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

of

ABDULAZIZ ALDRIBI

MSc (University of Birmingham, 2011)
BSc (King Abdulaziz University, 2004)

“Cloud Intrusion Detection based on Change Tracking and a New Benchmark Dataset”

Department of Electrical and Computer Engineering

Wednesday, August 15, 2018
8:30 A.M.
Clearihue Building
Room B007

Supervisory Committee:
Dr. Issa Traore, Department of Electrical and Computer Engineering, University of Victoria
(Supervisor)
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Jianping Pan, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Natalia Stakhanova, Faculty of Computer Science, University of New Brunswick

Chair of Oral Examination:
Dr. Dr. Ralf St. Clair, Department of Curriculum and Instruction, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies
Abstract

The adoption of cloud computing has increased dramatically in recent years due to attractive features such as flexibility, cost reductions, scalability, and pay per use. Shifting towards cloud computing is attracting not only industry but also government and academia. However, given their stringent privacy and security policies, this shift is still hindered by many security concerns related to the cloud computing features, namely shared resources, virtualization and multi-tenancy. These security concerns vary from privacy threats and lack of transparency to intrusions from within and outside the cloud infrastructure. Therefore, to overcome these concerns and establish a strong trust in cloud computing, there is a need to develop adequate security mechanisms for effectively handling the threats faced in the cloud. Intrusion Detection Systems (IDSs) represent an important part of such mechanisms. Developing cloud based IDS that can capture suspicious activity or threats, and prevent attacks and data leakage from both inside and outside the cloud environment is paramount. However, cloud computing is faced with a multidimensional and rapidly evolving threat landscape, which makes cloud based IDS more challenging. Moreover, one of the most significant hurdles for developing such cloud IDS is the lack of publicly available datasets collected from a real cloud computing environment. In this dissertation, we introduce the first public dataset of its kind, named ISOT Cloud Intrusion Dataset (ISOT-CID), for cloud intrusion detection. The dataset consists of several terabytes of data, involving normal activities and a wide variety of attack vectors, collected over multiple phases and periods of time in a real cloud environment. We also introduce a new hypervisor-based cloud intrusion detection system (HIDS) that uses online multivariate statistical change analysis to detect anomalous network behaviors. As a departure from the conventional monolithic network IDS feature model, we leverage the fact that a hypervisor consists of a collection of instances, to introduce an instance-oriented feature model that exploits individual as well as correlated behaviors of instances to improve the detection capability. The proposed approach is evaluated the new cloud intrusion dataset and the experiments along with results are presented.