PROGRAMME

The Final Oral Examination
for the Degree of

DOCTOR OF PHILOSOPHY
(Department of Electrical & Computer Engineering)

Sherif Saad Ahmed
2007 Arab Academy for Sci., Tech. & Maritime Transport M.Sc (Comp. Sci.)
2003 Helwan University B.Sc (Comp. Sci.)

Novel Intrusion Alert Analysis Framework Using Semantic Correlation

Wednesday, October 8, 2014
1:30 – 3:30 PM PST
David Turpin Building, Room A144

Supervisory Committee:
Dr. Issa Traoré, Department of Electrical and Computer Engineering, UVic (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. Mohammad Zulkernine, School of Computing, Queen’s University

Chair of Oral Examination:
Dr. Jacquie Green, School of Social Work, UVic
Abstract

In the last several years the number of computer network attacks has increased rapidly, while at the same time the attacks have become more and more complex and sophisticated. Intrusion detection systems (IDSs) have become essential security appliances for detecting and reporting these complex and sophisticated attacks. Security officers and analysts need to analyze intrusion alerts in order to extract the underlying attack scenarios and attack intelligence. These allow taking appropriate responses and designing adequate defensive or prevention strategies. Intrusion analysis is a resource intensive, complex and expensive process for any organization.

The current generations of IDSs generate low level intrusion alerts that describe individual attack events. In addition, existing IDSs tend to generate massive amount of alerts with high rate of redundancies and false positives. Typical IDS sensors report attacks independently and are not designed to recognize attack plans or discover multistage attack scenarios. Moreover, not all the attacks executed against the target network will be detected by the IDS. False negatives, which correspond to the attacks missed by the IDS, will either make the reconstruction of the attack scenario impossible or lead to an incomplete attack scenario. Because of the above mentioned reasons, intrusion analysis is a challenging task that mainly relies on the analyst experience and requires manual investigation.

In this dissertation, we address the above mentioned challenges by proposing a new framework that allows automatic intrusion analysis and attack intelligence extraction by analyzing the alerts and attacks semantics using both machine learning and knowledge-representation approaches. Particularly, we use ontological engineering, semantic correlation, and clustering methods to design a new automated intrusion analysis framework. The proposed alert analysis approach addresses many of the gaps observed in the existing intrusion analysis techniques, and introduces when needed new metrics to measure the quality of the alerts analysis process. We evaluated experimentally our framework using different benchmark intrusion detection datasets, yielding excellent performance results.
Awards, Scholarships, Fellowships

2009 – Graduate Award, University of Victoria.  
2008 – University of Victoria Fellowship. 

Publications

1. **S. Saad**, I. Traore, “Intrusion Alert Analysis Using Semantic Correlation and Computational Intelligence” Book Chapter, Recent Advances in Computational Intelligence in Defense and Security Springer August, **2015 (submitted)**


