University of Victoria | Graduate Studies

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)**
2. **S. Saad**, I. Traore, “Machine Learning Techniques to Reduce False Positives”, Computer & Security journal, Elsevier, **(submitted 2014)**
3. **S. Saad**, I. Traore, M. Brocardo , “Reducing False Positives Using Rule Induction and Clonal Selection”, 10th ACM Symposium on Information, Computer and Communication Security (ASIACCS 2015), Singapore, **(2015 submitted)**
4. **S. Saad**, I. Traore, M. Brocardo “Context-Aware Intrusion Alerts Verification Approach”, 10th International Conference on Information Assurance & Security, IAS **2014**, Okinawa, Japan **(submitted)**
5. M. Brocardo, I. Traore, **S. Saad,** Isaac Woungang, "*Verifying Online User Identity using Stylometric Analysis for Short Messages*)", Journal of Networks **(accepted 2014)**
6. **S. Saad**, I. Traore, "Semantic-aware Attack Scenario Reconstruction", Journal of Information Security and Applications, Elsevier, Vol 18, Issue 1, **2013**
7. **S. Saad**, I. Traore, "Extracting Attack Scenarios Using Intrusion Semantics", 5th International Symposium on Foundations and Practice of Security (FPS 2012), **2012,** Montreal, QC, Canada
8. D. Zhao, I. Traore, B. Sayed, W. Lu**, S. Saad**, A. Ghorbani and D. Garant, "Botnet Detection based on Traffic Behavior Analysis and Flow Intervals", Computer & Security journal, Elsevier, vol. 39, **2013**, pp. 2-16.
9. **S. Saad**, I. Traore, "A Semantic-based Approach to Minimize IDS Alerts Flooding", 7th ACM Symposium on Information,

Computer and Communication Security (ASIACCS 2012), May 01-03, **2012**, Seoul, South Korea.

10. **S Saad**, I.Traore, Journal of Information Assurance and Security. Heterogeneous Multi-sensor IDS Alerts Aggregation using Semantic Analysis, Volume 7, No 2, **2012**.
11. D. Zhao, I. Traore, A. Ghorbani, B. Sayed, **S. Saad**, W. Lu. "Peer to Peer Botnet Detection Based on Flow Intervals". Information Security and Privacy Research, IFIP Advances in Information and Communication Technology Volume 376, **2012**, pp 87-102.
12. **S.Saad**, I.Traore, A semantic analysis approach to manage IDS alerts flooding. 7th International Conference on Information Assurance and Security, IAS 2011, Melacca, Malaysia, December 5-8, **2011.**
13. **S. Saad**, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, J. Felix, P. Hakimian, "Detecting P2P botnets through network behavior analysis and machine learning", Proceedings of 9th Annual Conference on Privacy, Security and Trust (PST2011), July 19-21, **2011**, Montreal, Quebec, Canada.
14. **S.Saad**, I.Traore, Method Ontology for Intelligent Network Forensics Analysis. Eight International Conference on Privacy, Security and Trust (PST 2010) pages 7-14. Ottawa, Canada. August **2010.**
15. **S.Saad**, I.Traore, "Ontology-based intelligent network forensics", Proceedings of 19th International Conference on Software Engineering and Data Engineering (SEDE2010), June 16-18, **2010**, San Francisco, CA, USA.