University of Victoria | Graduate Studies

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

of

ABDELRAHMAN AZIZ ALENAZI

BSc (Vancouver Island University, 2015)

"HTTP Botnet Detection using Passive DNS Analysis and Application Profiling"

Department of Electrical and Computer Engineering

Monday, December 11, 2017
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. Xiaodai Dong, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Kui Wu, 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

HTTP botnets are currently the most popular form of botnets compared to IRC and P2P botnets. This is because, they are not only easier to implement, operate, and maintain, but they can easily evade detection. Likewise, HTTP botnets flows can easily be buried in the huge volume of legitimate HTTP traffic occurring in many organizations, which makes the detection harder. In this thesis, a new detection framework involving three detection models is proposed, which can run independently or in tandem. The first detector profiles the individual applications based on their interactions, and isolates accordingly the malicious ones. The second detector tracks the regularity in the timing of the bot DNS queries, and uses this as basis for detection. The third detector analyzes the characteristics of the domain names involved in the DNS, and identifies the algorithmically generated and fast flux domains, which are staples of typical HTTP botnets. Several machine learning classifiers are investigated for each of the detectors. Experimental evaluation using public datasets and datasets collected in our testbed yield very encouraging performance results.