2013/2014

Seminar Series

www.cs.unb.ca/seminarseries

UNB Faculty of COMPUTER SCIENCE

Fredericton · New Brunswick · Canada

Towards Effective Feature Selection in Machine Learning-Based Botnet Detection Approaches

Elaheh Biglar Beigi Samani and
Hossein Hadian Jazi
Graduate Students
UNB Faculty of Computer Science

Botnets as one of the most formidable cyber security threats, are becoming more sophisticated and resistant to detection. In spite of the pressing need for automated detection of these evolving botnets, researchers have been struggling to offer comprehensive support for detection of different types of botnets (even having the same topology, e.g. P2P). A considerable research effort has been put into extraction of network flow features in order to provide a comprehensive picture of botnet behavior. However powerful in discovering a limited number of botnet types, the effectiveness of flow level features in terms of providing more detection coverage still remains in doubt. In this paper we revisited flow features introduced in previous work and evaluate their relative efficiency when applied to a diverse dataset.

Wednesday, March 12 @ 2:30pm
Information Technology Centre, ITC317