A Distributed Collaborative Approach to Botnet Detection

The Oakland University and School of Engineering and Computer Science communities are invited to attend Zahraddeen Gwarzo's defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.

A Distributed Collaborative Approach to Botnet Detection

Committee: Mohamed A. Zohdy, Ph.D. (Chair), Hua Ming, Ph.D. (Co-Chair), Andrew Rusek, Ph.D., Richard Olawoyin, Ph.D., Hany Othman, Ph.D.

Time: **2:00 – 4:00 p.m.**
Date: **Tuesday, April 17, 2018**
Location: **347 EC**

Although there have been many significant achievements in Botnet research, hackers continue to develop highly sophisticated new Botnets and covert ways to control their networks. Researchers face a number of challenges in doing experiments that will pave the way for the design and development of effective Botnet detection systems.

Better security decisions are usually linked with experience in cyber security, advanced-technologies, and rich data and information. Therefore, an earnest and determined collaborative approach to Botnet detection is likely to have a significant positive outcome in tackling the menace of Botnets. The goal of this research is to develop a robust system that will leverage the expertise and experience of several research collaborators, as well as the abundant data and information at each collaborator's disposal, to detect Botnets irrespective of a command and control protocol, type of architecture, or infection behavior. Machine Learning approach has been used to classify data payloads from a dataset generated by this research into Botnet related or Benign. Five different classification algorithms are used to train and test the datasets. Decision Tree was selected as the best performing algorithm. This research also develops robust algorithms that are aimed at detecting inefficient and malicious collaborating nodes, hence-forth boosting the overall efficiency and reputation of the System.