COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Clifford Kemp

for the degree of Doctor of Philosophy (Ph.D.)

"Collection And Analysis of Slow Denial of Service Attacks using Machine Learning Algorithms"

December 1, 2021, 10:30 a.m.
Virtual Dissertation

Zoom
Meeting ID: 899 6810 4318
Passcode: 202030

DEPARTMENT:
Electrical Engineering and Computer Science

ADVISOR:
Taghi M. Khoshgoftaar, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Xingquan Zhu, Ph.D.
Dingding Wang, Ph.D.
Mehrdad Nojoumian, Ph.D.

ABSTRACT OF DISSERTATION
Collection and Analysis of Slow Denial of Service Attacks Using Machine Learning Algorithms

Application-layer based attacks are becoming a more desirable target in computer networks for hackers. From complex rootkits to Denial of Service (DoS) attacks, hackers look to compromise computer networks. Web and application servers can get shut down by various application-layer DoS attacks, which exhaust CPU or memory resources. The HTTP protocol has become a popular target to launch application-layer DoS attacks. These exploits consume less bandwidth than traditional DoS attacks. Furthermore, this type of DoS attack is hard to detect because its network traffic resembles legitimate network requests. Being able to detect these DoS attacks effectively is a critical component of any robust cybersecurity system. Machine learning can help detect DoS attacks by identifying patterns in network traffic. With machine learning methods, predictive models can automatically detect network threats.

This dissertation offers a novel framework for collecting several attack datasets on a live production network, where producing quality representative data is a requirement. Our approach builds datasets from collected NetFlow and Full Packet Capture (FPC) data. We evaluate a wide range of machine learning classifiers which allows us to analyze slow DoS detection models more thoroughly. To identify attacks, we look at each dataset's unique traffic patterns and distinguishing properties. This research evaluates and investigates appropriate feature selection evaluators and search strategies. Features are assessed for their predictive value and degree of redundancy to build a subset of features. Feature subsets with high-class correlation but low intercorrelation are favored. Experimental results indicate NetFlow and FPC features are discriminating enough to detect DoS attacks accurately. We conduct a comparative examination of performance metrics to determine the capability of several machine learning classifiers. Additionally, we improve upon our performance scores by investigating a variety of feature selection optimization strategies. Overall, this dissertation proposes a novel machine learning approach for detecting slow DoS attacks. Our machine learning results demonstrate that a single subset of features trained on NetFlow data can effectively detect slow application-layer DoS attacks.

BIOGRAPHICAL SKETCH
Born in West Palm Beach, Florida
B.A., Florida Atlantic University, Boca Raton, Florida,1980
M.S., Florida Atlantic University, Boca Raton, Florida, 2010
M.S., Florida Atlantic University, Boca Raton, Florida, 2013
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2021

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION
Time in Preparation: 2015 - 2021

Qualifying Examination Passed: Fall 2014

Selected Published Papers:

C. Kemp, C. Calvert, and T. Khoshgoftaar, "Utilizing NetFlow Data to Detect Slow Read Attacks." in 2018 IEEE International Conference on Information Reuse and Integration (IRI). IEEE, 2018, pp. 108–116.

C. Kemp, C. Calvert, and T. M. Khoshgoftaar, "NetFlow Feature Evaluation for The Detection of Slow Read HTTP Attacks." in Reuse in Intelligent Systems, CRC Press, 2020, pp. 181–219.

C. Kemp, C. Calvert, and T. M. Khoshgoftaar, "Detection Methods of Slow Read Dos using Full Packet Capture Data." in 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI). IEEE, 2020, pp. 9–16.

C. Kemp, C. Calvert, and T. M. Khoshgoftaar, "Detecting Slow Application-Layer DoS Attacks with PCA." in 2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI). IEEE, 2021, pp. 108–116.

C. Kemp, C. Calvert, and T. M. Khoshgoftaar, "An Approach to Application-Layer DoS Detection." in Expert Systems with Applications, Elsevier, 2021(Under Review).