COLLEGE OF ENGINEERING
AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Charles Wheelus

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

“Network Feature Engineering and Data Science Analytics for Cyber Threat Intelligence”

November 20, 2020, 3:00 p.m.
Virtual Dissertation

DEPARTMENT:
Computer and Electrical Engineering and Computer Science

ADVISOR:
Xingquan Zhu, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Xingquan Zhu, Ph.D., Chair
Martin Solomon, Ph.D.
Hanqi Zhuang, Ph.D.
Mehrdad Nojoumian, Ph.D.

ABSTRACT OF DISSERTATION
Network Feature Engineering and Data Science Analytics for Cyber Threat Intelligence

Network services continue to play an ever-increasing role in our daily lives. Our information infrastructure requires a concerted, well-conceived and fastidiously executed strategy to remain viable. Government agencies, Non-Governmental Organizations ("NGOs"), and private organizations are all targets for malicious online activity. Security has deservedly become a serious focus for organizations that seek to assume a more proactive posture to deal with the many facets of securing their own infrastructure. In addition, the paradigm changing Internet of Things (IoT) has recently shifted the Internet from being a platform primarily used on computers and mobile devices to an operational network that connects devices that were previously stand alone. IoT brings the Internet further into everyday life, and a host of security issues become more pervasive as well.

This dissertation explores the pairing of machine learning and security, with an emphasis on feature engineering at the network layer. Additionally, it considers the efficacy of various approaches in the context of application and usefulness; seeking to identify a way forward to implementing machine learning and network security analytics in a pragmatic fashion.

The dissertation examines the security domain in general and considers past datasets that have been produced for the purpose of evaluating methods of detecting network intrusions. Various aspects of several well-known security datasets are discussed, with the motivation of creating new network features that are predictive of attacks at the network layer. Additionally, the requirement of architectures capable of producing cyber-security artifacts at scale are considered and a reference architecture is proposed for “big data” scenarios. The problem of class imbalance and methods of addressing it are also explored in the dissertation. Additionally, the dissertation explores threats and risks in IOT network security, and proposes a framework for data driven defense for IoT.

Several of the chapters include numerous case studies that bring the context to the concepts contemplated in the dissertation. These include network-based attacks, malware, and IoT attacks. In these case studies, data are converted from raw packets to features suitable for machine learning. A publicly available dataset, which was released concurrently with the recent publication of “IoT Network security: Threats, risks, and a data-driven defense framework”, is reviewed in detail in the dissertation.

BIOGRAPHICAL SKETCH
Born in Tallahassee, Florida
Principal Data Scientist, HarmonyLogic

B.S., Florida Atlantic University, Boca Raton, FL, 1993
M.S., Florida Atlantic University, Boca Raton, FL, 2010
Ph.D., Florida Atlantic University, Boca Raton, FL, 2020

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2014-2020

Qualifying Examination Passed: April 2012

Selected Published Papers:

1. Charles Wheelus and Xingquan Zhu. IoT Network security: Threats, risks, and a data-driven defense framework. *Internet of Thing (IoT)*, Special Issue on ”Cyber Security and Privacy in IoT”, pages 259-285, October 2020 (**https://doi.org/10.3390/iot1020016**).

2. Tsoi Shing and Charles Wheelus. Traffic signal classification with cost-sensitive deep learning models. In *Proc. of the 11th IEEE International Conference on Knowledge Graph (ICKG-2020)*, pages 586–592. IEEE, 2020.

3. Charles Wheelus, Elias Bou-Harb, and Xingquan Zhu. Tackling class im-balance in cyber security datasets. In *Proc. of the IEEE 19th International Conference on Information Reuse and Integration for Data Science*, pages 229–232. IEEE,2018.

4. Charles Wheelus, Elias Bou-Harb, and Xingquan Zhu. Towards a big data architecture for facilitating cyber threat intelligence. In *Proc. of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages1–5. IEEE, 2016.

5. Charles Wheelus, Taghi M. Khoshgoftaar, Richard Zuech, and Maryam M Najafabadi. A session-based approach for aggregating network traffic data – the SANTA dataset. In *Proc. of the 2014 IEEE International Conf. on Bioinformatics and Bioengineering (BIBE)*, pages 369–378. IEEE, 2014.