College of Engineering

TENNESSEE TECH

The Department of

Computer Science

Announces the Dissertation Defense

of

Robert Gillen

In Partial Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

September 24, 2020

8:00 a.m.

Tennessee Tech University

Zoom Link:

https://us02web.zoom.us/j/83659367584

Passcode: 660105

FIELD OF STUDY

Computer Science

Subfields: Cybersecurity, Machine Learning, Industrial Control Systems and Signal Analysis

Dissertation Topic

Method for Assessing Security Impact of Settings in Anomaly-Based Intrusion Detection for Industrial Control Systems

EXAMINING COMMITTEE

Dr. Stephen Scott (chairperson)

Dr. William Eberle

Dr. Mike Rogers

Dr. Sheikh K. Ghafoor

Dr. Stephen Canfield

ABSTRACT

Intrusion Detection Systems (IDS) based on algorithms derived from machine learning techniques can be an effective means of defending industrial control systems (ICS). Unfortunately, the relative immaturity of these systems within the commercial marketplace is often highlighted by the data scientist and mathematician focused set of configuration options that the network operations staff are ill-equipped to select. Should the system use multiple algorithms to evaluate each flow (ensemble) or a single algorithm? Should various features (eg. diurnal time period) be included or excluded? Should the alerting threshold be set at 3.48 or 3.65? How do each of these options really affect the security of the network to be protected?

Here, a method of assessment is presented that supports the system operators in understanding the relative security implications of various IDS settings. By defining the security categories of interest and mapping exemplars to those categories, operators have a solid basis for evaluation. We provide a testing and scoring system process by which they can compare the implications of one configuration set to another while allowing them to extend the approach and incorporate institutional or operator knowledge.

The results show that this assessment methodology provides a metric that, in concert with other data (eg. false positive count) can be used to make informed decisions regarding the configuration and protection of the network. Further, we show how the testing methodology can illuminate characteristics of the IDS that may make it susceptible to defeat given certain attacker behaviors.

BIOGRAPHICAL SKETCH

Robert Gillen was born in South Bend, Indiana and graduated with a BSc in Broadcast Electronics from Bob Jones University in 1998. He taught for a year and then went on to work at a startup before joining Planet Technologies in April of 2000 as a Solutions Architect. He gained experience as a professional developer with clients ranging from service providers in Europe and the Far East to corporate and federal customers in the US.

While at Planet Technologies, Rob was detailed to Oak Ridge National Laboratory in 2007 to support their IT modernization efforts. Rob worked in IT until the Spring of 2009 when he joined the Computer Science Research Group assessing cloud computing for scientific workloads. He joined ORNL as an employee in September of 2011 in the Computational Data Analytics Group developing solutions for federal law enforcement. Since then, Rob has worked on a number of research projects with a particular focus on cyber-security and machine learning. He is currently a member of the Vulnerability Science Research Group. Rob began his studies at Tennessee Technological University in January 2015 and

EDUCATION

Ph.D. Engineering
Tennessee Tech University, 2015-2020 (expected)

M.S. Computer Science
Tennessee Tech University, 2015-2018

B.S. Broadcast Electronics
Bob Jones University, 1994-1998