Potential Questions for Research Preparedness Assessment

Rob Gillen

Overview

The questions listed below are designed to serve as idea fodder for those writing questions for my comprehensive exam. They are written based on my limited knowlege/exposure to what this process looks like but are intended to emphasize questions I feel are relevant to the impending research effort. For each question, I have listed the class/subject area that I feel it relates to.

Question 1

Provide a list of algorithmic approaches to anomaly detection-based defensive systems. Describe which are most susceptible to attacks and why. Support your conclusions.

- ECE 7970: Selected Topics: Statistical Learning (Anderson)

Question 2

One could imagine that a system based on reinforcement learning may provide a foundation for the assessments/attacks you intend to perform. Discuss the suitability (or lack thereof) of this methodology and describe (if applicable) a rough experimentation approach.

- CSC 7970: Selected Unsupervised Learning Topics (Talbert)

Question 3

The Formby paper (A Case Study in Power Substation Network Dynamics) suggests that network traffic in the smart grid is not as regular as one might have expected. What is your opinion on the generalization properties of this paper? How does this affect the research you plan to conduct?

- CSC 7575: Security Topics in Smart Grid (Prowell)

Question 4

Justify your assertion that anomaly detection systems are subject to poisoning and describe a network attack that this might enable.

- ECE 7970: Selected Topics: Statistical Learning (Anderson)
- CSC 7970: Selected Unsupervised Learning Topics (Talbert)

Question 5

Explain the interplay between RTOS-based control devices and SCADA systems as it relates to anomaly-detection systems. Compare and contrast serial-based networks and IP-based networks in these scenarios.

- ECE 7170: Advanced Embedded Systems (Elkeelany)
- CSC 7575: Security Topics in Smart Grid (Prowell)

Question 6

Your PhD and Masters courses included a strong focus on GPU-enabled computing (9 hours). Your research abstract does not appear to utilize this topic in any fashion. Is this a fair assessment? Do you envision utilizing this knowledge in your research? Justify and explain your answer.

- ECE 6980: Directed Independent Study: Open CL (Anderson)
- CSC 6803: Dir. Indp. Study: CUDA for HPC (Scott)
- CSC 6803: Dir. Indp. Study: OpenACC for HPC (Scott)

PhD Courses

The following list are the courses taken in fullfilment of the requirements of the PhD program:

- ECE 7170: Advanced Embedded Systems (Elkeelany)
- CSC 7970: Selected Unsupervised Learning Topics (Talbert)
- ECE 6040: Signal Analysis (Qui)
- ECE 6250: Random Signals and Systems (Anderson)
- CSC 7575: Security Topics in Smart Grid (Prowell)
- CSC 6803: Dir. Indp. Study: OpenACC for HPC (Scott)

Masters Courses

These courses appear on my Program of Study in support of my Masters degree but, given my participation in the direct-admit program, contribute to my overall educational picture and prepared me for the research I intend to perform:

- ECE 7970: Selected Topics: Statistical Learning (Anderson)
- ECE 6900: Special Problems in Tehcnial Writing (Anderson)
- ECE 6980: Directed Independent Study: Open CL (Anderson)
- ECE 6170: High Performance Embedded Systems (Elkeelany)
- CSC 5760: Parallel Programming (Scott)
- CSC 6740: Parallel and Distributed Algorithms (Ghafoor)
- CSC 6220: Datamining (Eberle)
- CSC 6803: Dir. Indp. Study: CUDA for HPC (Scott)

Abstract

In recent years both government and industry have made significant investments and progress in developing approaches for the security and reliable operation of cyber physical systems. These investments span a wide range of research including hardware, software, modeling and simulation and empirical experiments. Many of these efforts have been funded on the premise that improved use of artificial intelligence-derived

data analytics (machine learning, deep learning, anomaly detection, etc.) is key to properly securing the cyber-physical systems which comprise our critical infrastructure.

Many of these efforts suffer from a common flaw. While much effort is exerted in developing the algorithms and techniques to support a given defensive mechanism, little effort is expended in attempting to defeat said approach. This “honeymoon period” is both expected and valuable as new research areas need time to mature before being attacked. The time has now come to develop a scientifically based critical eye when looking at these defensive techniques and to establish a capability to challenge their assertions in real-world scenarios. Such a capability should be both measured and disciplined in its approach and target the assumptions of both science and implementation.

I propose to take a data-driven approach to attacking the defenses of industrial control system networks. More specifically, I will focus on attacking and assessing anomaly-detection-based defenses. Existing research has established that, if one can know when an anomaly detection system is being trained, one can poison the training data and thereby affect the definition of “normal” - allowing attacks that would otherwise be caught to succeed. My research aims to measure the degree to which a given system is susceptible to these types of attacks and standard attacks can be made to succeed. Further, I aim to measure the bounds of the system’s definition of normal to ascertain if a patient attacker (using his own anomaly detection system for the purposes of discovering the likely bounds of the deployed system) can craft attacks such that they are accepted as normal by the protection platform. The output of this effort will be a scoring, or measurement system which conveys the degree to which a system is susceptible to these types of attacks and can be utilized to inform the defensive posture of such.

In a fashion not unlike cryptographic systems, it is often discovered that deployed systems exhibit behaviors different than the theoretical models and it is the assumptions or compromises made during the engineering and development that provide the most fertile ground for attack. As such, this research will focus on specific instantiations of the protection methodologies rather than evaluating theoretical or model-based designs.