Data-Driven Assesment of Cyber-Security-Significant Properties of Industrial Control Systems

Rob Gillen

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.