Intrusion Detection in SCADA Systems via Network Analysis

Justin Jones
Department of Computer Science
Sam Houston State University
Huntsville, Texas 77341, USA
jxj037@shsu.edu

Yesenia Valles
Department of Computer Science
Sam Houston State University
Huntsville, Texas 77341, USA
yev001@shsu.edu

***Abstract* – Given the nature of SCADA systems, we postulate that it is possible to detect intrusions or otherwise malicious activity via network analysis. Utilizing machine learning, we will develop software to passively monitor systems and identify possible intrusions and complete a general study of SCADA networks.**

Index Terms – scada, network analysis, machine learning

I. Introduction

SCADA (Supervisory Control and Data Acquisition) [1] systems are used to support and monitor the infrastructure that serves as pillars for many industrialized areas. SCADA systems were historically created with an emphasis on availability of data as opposed to implementation of the X.800 security architecture. With the emerging prevalence of IoT security and edge-intrusion testing, the security of these systems has become an increasingly pertinent subject in the security community as networking and remote access becomes more and more desirable. Given that the purpose of SCADA systems is to enable users to manage and perform tasks on a large scale in industrial infrastructures as quickly and easily as possible, security vulnerabilities have the potential to cause serious damage if an attacker gains access to a system. One such example of the consequences can be seen from the Stuxnet worm, controlling and damaging Iranian nuclear reactors in 2010 [2]. The use of open standards for SCADA communication protocols are also increasing, largely due to low cost of implementation, so the risk of future security breaches will likely be applicable to multiple systems rather than limited to single product lines from a particular manufacturer.

II. Theory

It is now obvious that the security of SCADA systems is a pertinent subject for study. As there can be any number of zero-day attacks for these systems, it will likely be more productive to shift focus to detecting these intrusions rather than trying to prevent them. Given the nature of SCADA systems, it can be presumed that their network traffic is reasonably predictable. This leads to the proposition that there are detectable network patterns occurring with some regularity for any given system or otherwise some 'normal' level of activity. Once a certain normalization is established, one may then use that as a baseline to compare future traffic to in order to detect anomalies that may possibly indicate active attacks. Our proposal is that, instead of focusing on systems or network exploits themselves, we write a tool to establish and then passively detect any network anomalies.

III. Proposal

To implement this tool, we intend to utilize machine learning-based analysis trained on known 'regular' traffic levels. We will then introduce network/control anomalies indicative of non-normal system behavior to demonstrate the detection capabilities and to test proper training levels of the algorithm. The result of this research will then be this passive detection tool and a research report on SCADA networks and analyzing SCADA network traffic.

References

[1] En.wikipedia.org. (2017). SCADA. [online] Available at: https://en.wikipedia.org/wiki/SCADA [Accessed 19 Sep. 2017].

[2] Kushner, D. (2013). The Real Story of Stuxnet. [online] IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [Accessed 19 Sep. 2017].