Intrusion Detection of a Simulated SCADA System using Data-Driven Modeling

Brien Jefferys (UT), Wes Hines (UT), Kenny Gross (Oracle)

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems have become integrated into many industries that have a need for control and automation. Examples of these industries include energy, water, transportation, and petroleum. A typical SCADA system consists of field equipment for process actuation and control, along with proprietary communication protocols. These protocols are used to communicate between the field equipment and the monitoring equipment located at a central facility. Given that distribution of vital resources is often controlled by this type of system, there is a need to secure the networked compute and control elements from users with malicious intent.

This paper investigates the use of data-driven modeling techniques to identify various types of intrusions tested against a simulated SCADA system. The test bed uses three enterprise servers that were part of a university engineering linux cluster. These were isolated so that job queries on the cluster would not be reflected in the normal behavior of the test bed, and to ensure that intrusion testing would not affect other components of the cluster. One server acts as a Master Terminal Unit (MTU), which simulates control and data acquisition processes. The other two act as Remote Terminal Units (RTUs), these simulate monitoring and telemetry transmission. All servers use Ubuntu 14.04 as the OS. A separate workstation using Kali Linux acts as a Human Machine Interface (HMI), this is used to monitor the simulation and perform intrusion testing. Monitored telemetry included network traffic, hardware and software digitized time series signatures.

The models used in this research include the Auto Associative Kernel Regression (AAKR) and Multivariate State Estimation Technique (AAMSET) [1, 2]. This type of intrusion detection can be classified as a behavior-based technique, wherein data collected when the system exhibits normal behavior is first used to train and optimize the previously mentioned machine learning models. Any future monitored telemetry that deviates from this normal behavior can be treated as anomalous, and may indicate an attack against the system. Models were tested to evaluate the prognostic effectiveness when monitoring clusters of signals from four classes of telemetry: combination of all telemetry signals, memory and CPU usage, disk usage, and TCP/IP statistics.

Anomaly detection is performed by using the Sequential Probability Ratio Test (SPRT), which is a binary sequential statistical test developed by Wald [3]. This test determines whether the monitored observation has mean or variance shifted from defined normal behavior [4]. For the prognostic security experiments reported in this paper, we established rigorous quantitative functional requirements for evaluating the outcome of the intrusion-signature fault injection experiments. These were a high accuracy for model predictions of dynamic telemetry metrics, and ultralow False Alarm and Missed Alarm Probabilities (FAPs and MAPS). The combination of AAKR or AAMSET for the pattern recognition engine, integrated with a SPRT for anomaly detection, was selected for this SCADA prognostic security research because those techniques have worked extremely well in prior machinery prognostic application when evaluated against the same functional requirements.

Intrusion testing used many of the software packages contained in Kali, such as Metasploit and Nmap, along with Linux related exploits taken from the CVE database. In this current work, six different intrusion types were tested against the test bed. These include network reconnaissance/discovery, three different DoS attacks, brute force password attacks, and information theft from the target machine. It is noted that many intrusions tested from Kali and the CVE database showed no clear indications of change in monitored telemetry. Intrusion signatures that yield low "true positive" rates with model-based prognostics place a higher reliance on conventional knowledge-based signature-dictionary detection. However, for signatures that yield 50% or higher detection rates with model-based prognostics, higher overall security for SCADA systems can be achieved with a hybrid approach, also called defense in depth. This uses conventional signature-dictionary detection for previously known exploits, with model-based prognostics presented in this paper for detection of "zero-day" attacks.

Of the 20 exploits employed in prognostic security evaluation experiments to date, 9 of those exploits were found to not show up in any monitored telemetry metrics and hence are not detectable by prognostic modeling approaches. An example of one of these exploits is the Linux OverlayFS exploit taken from the CVE database. While this exploit was employed successfully to elevate user privilege, the very small size of the payload and rapid time for successful exploitation would never manifest in any monitored telemetry. But for the 11 exploits that show up as alterations in the correlation patterns detected by the prognostic modeling approach introduced in this paper, we achieved a 100% detection rate (0% MAP) for detection. Moreover, for all intrusion detection experiments to date, the analysis that will be presented in the full paper also achieved 0% FAP. The conclusion of our investigations to date is that highly accurate nonlinear, nonparametric advanced pattern recognition, couple with a SPRT for anomaly detection, can be a very valuable technique for prognostic cyber security to augment; but not replace; conventional signature-based exploit detection in business and mission critical SCADA networks. In future work, we plan to extend the machine learning techniques presented here that have shown very high success for SCADA network security, to enterprise systems and networks.

References:

1. D. Garvey and J. W. Hines, "The Development of a Process and Equipment Monitoring (PEM) Toolbox and its Application to Sensor Calibration Monitoring", *Quality and Reliability Engineering International*, **22**, 1-13, 2007.
2. R. M. Singer, K. C. Gross, J. P. Herzog, R. W. King and S. Wegerich, "Model-Based Nuclear Power Plant Monitoring and Fault Detection: Theoretical Foundations", Proc. 9th Int. Conf. On Intelligent Systems Applications to Power Systems, pp. 60-65, Seoul, Korea (July 6-10, 1997).
3. A. Wald, Sequential Analysis, j. Wiley & Sons, New York, 1947.
4. K. C. Gross, K. Vaidyanathan and S. Valiollshzadeh, "Advanced Pattern Recognition for Optimal Bandwidth and Power Utilization for Wireless Intelligent Motes for IoT Applications", World Computer Conf., 2016.