Enhance Security of SCADA systems with anomaly detection and flexible evaluation platform

Chih-Yuan Lin

Dept. of Computer and Information Science, Linköping University
chih-yuan.lin@liu.se

Keywords: SCADA, cyber security, anomaly detection, traffic generation

The increasing number of cyber-attacks against SCADA (Supervisory Control And Data Acquisition) systems operating critical infrastructures make SCADA system security a pressing issue. Due to the special characteristics like real-time requirement and unique network activities, general intrusion detection systems are not effective on SCADA systems. New approaches to develop and evaluate intrusion detection systems for SCADA systems need to be explored.

Compared with standard information communication systems, SCADA systems show more stable and persistent communications patterns. By analyzing the control protocols running on SCADA systems, together with their traffic, it is possible to model normal behaviors and build anomaly-based detection tools accordingly. The proposed solutions need to be evaluated in an open, flexible and realistic platform concerning its accuracy and performance. The platform includes

I. Realistic and attack-free dataset

Due to the sensitive nature of critical infrastructure, lack of an openly available test dataset is a significant challenge of research in this area. We plan to propose a systematic approach to generate SCADA-specific dataset as following. Real traces are analyzed and abstracted with their statistic characteristic for a SCADA traffic generator. In this regard, a metric is established to measure the distance of two dataset. For the data to be openly available but privacy preserving, the distance of generated data and the original one should be as far as possible.

II. Mirrored system replicate the performance of live SCADA system

Since it is impossible to attack a real critical infrastructure for tests and also it is too costly to maintain a physical one. In order to verify the functionality and performance of proposed IDS, IDS developers need a virtualized environment which is configurable and able to reflect the performance in different configurations. Nowadays, most of the testbeds for SCADA specific IDS contain real devices to reproduce the resource constrained situations. A pure software solution has yet to appear. However, the network performance, transmission speed and transmission delay of SCADA specific devices, are basically decided by the choice of physical media and transmission technologies. It is possible to simulate the network performance based on the knowledge of specification of real devices.