Timing Patterns and Correlations in Spontaneous SCADA Traffic for Anomaly Detection

Chih-Yuan Lin (chih-yuan.lin@liu.se)

Linköpings Universitet

Supervisory Control and Data Acquisition (SCADA) systems control and monitor critical infrastructures such as power plants, water distribution facilities, gas stations, etc. These assets are essential for the functioning of a society. The emergence of attacks targeting specific SCADA systems and the controlled critical infrastructures, such as Stuxnet[1], makes SCADA security a pressing issue.

SCADA traffic is known to have stable traffic patterns with request-response communications triggered by a polling mechanism and believed to be suitable for anomaly detection. In such a communication mode, a SCADA master sends requests to the field devices and receives a response accordingly. However, modern SCADA protocols such as IEC-60780-5-104 also allow non-requested communications. In the non-requested communication mode, the field devices can initiate messages spontaneously. Due to the lack of periodicity and cyclic sequences caused by a polling mechanism, many anomaly detection methodologies designed for request-response communications cannot be applied to traffic generated by modern SCADA protocols. New approaches to model spontaneous traffic need to be explored.

My research work done at LiU within the RICS center (www.rics.se) includes characterization of SCADA traffic from different sources (testbed and real SCADA systems), modeling the found characteristics, and building intrusion detection systems. My presentation will give an overview of the published work and briefly present some recent outcomes on exploiting characteristics of spontaneous traffic for anomaly detection.

In recent work, we provide a novel approach to model spontaneous traffic with respect to its timing patterns and correlations between flows. The approach is validated with traffic collected in a real power station. The tests are conducted with two attack scenarios. One attack scenario generates persistent anomalies by resource exhaustion attacks against the field devices, and the other generates intermittent anomalies caused by malware on the field devices, which is considered as stealthy. Our approach successfully detects the attacks causing persistent anomalies at the rate of 100% with false positive rates lower than 1%. For the attack scenario causing intermittent anomalies, our approach is effective for the attacks in the low volume traffic or attacks lasting over 1 hour.

The presentation will include:

- Overview of published work
- Traffic characteristics in spontaneous traffic collected in a real power station
- Timing pattern and correlation models for anomaly detection

[1] Stuxnet: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf