Online, Context-aware Anomaly Detection, Causality and Consequence Analysis for SCADA Systems

Wenyu Ren, Timothy Yardley, Klara Nahrstedt

Supervisory Control and Data Acquisition (SCADA) systems are industrial control systems (ICSs) for large-scale distributed critical infrastructure systems, such as, power grids and oil/gas pipelines. Critical as they are, SCADA systems are vulnerable to a wide range of serious threats due to the following reasons:

- The increasing complexity and interconnection of SCADA systems provides greater opportunity for attacks from malicious sources.
- Devices in SCADA systems are usually not built with consideration to cybersecurity and lack authentication or encryption mechanisms.
- Most ICS protocols lack authentication features and provide no protection for the network traffic.

We are eagerly seeking cooperation, support, and guidance from industry partners in the following areas:

- Procedures the operators need to follow to deal with various failures in systems
- Dataset to better understand the traffic in SCADA systems and evaluate our framework

Contact:
wren3@illinois.edu, yardley@illinois.edu, klara@illinois.edu
Activity webpage: https://cred-c.org/researchactivity/ContextAwareAD

Our entire framework consists of two sub-frameworks:

- An edge-based multi-level anomaly detection framework named EDMAND
- A causality-based anomaly analysis framework

We divide data in SCADA network traffic into three levels and apply appropriate anomaly detection methods respectively:

- Transport level: statistics in IP headers and transport protocol headers.
- Operation level: operation statistics in ICS protocols.
- Content level: measurement statistics from field devices.

The alert manager consists of two components:

- Alert aggregator: aggregates similar alerts to form meta-alerts.
- Alert scheduler: calculates priority scores of meta-alerts and decides their report frequencies.

We inject various anomalies in the three levels:

- EDMAND is able to detect all the anomalies injected with a false positive rate of 0.007% .
- All the anomalies generate 12184 alerts in total, which are aggregated to 31 meta-alerts.

What our framework provides for your system:

- Quick detection of anomalies on transport, operation, and content levels
- Potential causes and consequences of the detected anomalies
- Suggested responses to mitigate the anomalies

Business Benefit:

- Increased real-time situational awareness of your SCADA systems
- Actionable intelligence for your operators to react fast to attacks or failures

We are eagerly seeking cooperation, support, and guidance from industry partners in the following areas:

- Procedures the operators need to follow to deal with various failures in systems
- Dataset to better understand the traffic in SCADA systems and evaluate our framework

Contact: wren3@illinois.edu, yardley@illinois.edu, klara@illinois.edu
Activity webpage: https://cred-c.org/researchactivity/ContextAwareAD