Online, Context-aware, Intelligent Anomaly Detection, Causality and Consequence Analysis, and Response Suggestion for Supervisory Control and Data Acquisition (SCADA) Systems in Energy Distribution Systems

Website: http://cred-c.org/researchactivity/contextawaread

Researchers (Illinois): Wenyu Ren, Klara Nahrstedt, Tim Yardley

Industry Collaboration:

- Currently seeking collaborators from utilities and industry - specifically utility industry operators and existing network security solution providers. Contact Wenyu Ren for more information.

Description of research activity: SCADA systems are widely used in EDS to gather measurement data from field devices and send control commands to them. However, the legacy end devices and industrial control protocols, used in the SCADA system, make it vulnerable to various cyberattacks. There are existing solutions to provide intrusion detection for networks. However, most of them only focus on monitoring and event detection of network state at the transport layer and perform flow-level analysis, which is not enough to detect and reason about semantic attacks hidden in the application layer. Even for those solutions which parse the application protocol, they usually can detect the event only, but fail to provide any causes and consequences of the event. Therefore, it is hard or impossible for the operator to quickly digest the event and react to it. If any of the attacks are undetected or not resolved promptly, the entire system could suffer.

In this activity, we concentrate on developing an online, context-aware, intelligent framework for anomaly detection, anomalous data analysis, causal reasoning, consequence indication and response suggestion for SCADA networks. This is a large research space since the framework requires an integration of approaches in feature selection, machine learning, predictive reasoning, context-aware analysis and alert aggregation, to name a few. Our framework analyzes the network traffic and parses not only transport-layer but also application-layer information. Features are selected, transformed and reduced and feature vectors are constructed. Three scopes of features are considered to offer different granularity of analysis: (a) flow-level information such as addresses, ports of source and destination, delays and jitters; (b) control-protocol-level information such as function codes and parameters; (c) content-level information such as values to be written and results from reads. Machine learning techniques are then used upon feature vectors to perform anomaly detection. Those three levels of anomaly detection serve as the building blocks of our framework and trigger various alarms. Beyond those building blocks, we build a causality-based analyzer to aggregate and analyze the generated alarms. Domain knowledge and causal reasoning are considered and cyber-physical models of the system are built or utilized to aid the detection, causality and consequence analysis of anomalies. Potential responses are then analyzed and provided to the operator based on the analysis results and current states of the system from the cyber-physical models.

We notice that intrusion detection for critical infrastructure has been done many times in TCIPG and CREDC. However, most of the existing works [1-6] focus on detection only and utilize cyber information only. [7-8] also leverage physical models but still limit themselves to detection. [9] proposed a response and recovery engine to provide automated response after intrusion but all the analysis happens in the cyber domain. [10] combines the knowledge of both cyber and physical domains for attacks analysis, detection and mitigation. But it only focuses a specific type of attacks in cyber-physical systems. What we aim for, on the contrary, is to utilize cyber and physical domain knowledge to provide not only more general anomaly detection, but also causality and consequence analysis as well as feasible response suggestion for SCADA systems. We believe that, the cyber and physical domains, their event detections, causal analysis

and responses, when considered jointly instead of independently, can yield much better performance and provide more reliable and comprehensive security protection for SCADA systems.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity addresses the Roadmap by performing cyber monitoring, provenance tracking, event detection, and causal reasoning of abnormal events. Our activity monitors the network traffic in SCADA networks, detects anomalous events in real time, and provides context-aware information for those anomalies to guide reasoning and consequences of anomalous events, which lead to operational resilience and recovery.

Summary of EDS gap analysis: Due to the lack of security protection of various end devices and legacy control protocols used in SCADA systems, it is crucial to build a framework or the SCADA network to monitor and detect any abnormal events and determine their impact. Although there are many works focusing on anomaly detection in SCADA systems, causality and consequence analysis of the anomalies and response suggestion for the operators are not addressed as much. This activity fills that gap by designing an online, context-aware, intelligent framework to detect and analyze anomalies in SCADA networks. The framework monitors the network traffic in SCADA networks, detects anomalous events in real time, and provides context-aware information for those anomalies to guide reasoning and consequences of anomalous events, which lead to operational resilience and recovery.

Full EDS gap analysis: Supervisory Control and Data Acquisition (SCADA) systems have long been used in many Energy Delivery Systems (EDS). Critical as they are, SCADA systems consist of various end devices, most of which are resource-constrained and do not have their own protection mechanisms. To make things worse, the legacy control protocols used in most SCADA systems offer little or no security protection. Thus, it is crucial to build a framework to monitor and detect any abnormal events in the SCADA network, put them in context, and then determine what the impact may be.

This activity fills that gap by designing an online, context-aware, intelligent framework to detect and analyze anomalies in SCADA networks. Instead of only utilizing transport-layer statistics to perform flow-level analysis, our framework will understand the control protocols and thus be able to utilize application-layer statistics to perform anomaly detection. It will then intelligently combine context information to analyze the anomalies and provide potential causes and consequences of them. With cyber and physical models established and combined, our framework will also be able to provide valuable response and recovery plan for the operator.

This is intended to follow the path of turning data into knowledge, knowledge to understanding, and understanding to action. The key research value here is that there are plenty of IDS platforms that can tell when something abnormal is happening, but the focus of this effort is to understand what caused it and what the consequences are so that the information can result in actionable intelligence that an operator can utilize. This will combine traditional automated learning approaches with smart grid characteristics, validation methods, provenance tracking, reasoning approaches, and properties of the physical system, its assets, and their behaviors to derive a representation of what is happening and what to do about it.

This activity addresses two of the five strategies mentioned in [11]: (1) assess and monitor risk; (2) manage incidents. The first strategy is addressed by utilizing flow-level, control-protocol-level, and content-level information of the network traffic to perform online, context-aware, intelligent monitoring and anomaly detection. The second strategy is addressed by combining cyber and physical models to analyze and anomalies and provide useful responses for the operator to take. Generally, this activity aims at monitoring network traffic in the communication network and detecting many failure scenarios that can be observed from the traffic in the distributed energy resources and distribution grid management domains. Scenarios in [12] that could be addressed by this activity are listed in Table 1.

Table 1. Failure scenarios addressed by this activity.

DER's Rogue Wireless Connection Exposes the DER System to Threat Agents via the Internet
Compromised DER Sequence of Commands Causes Power Outage
Incorrect Clock Causes Substation DER System Shut Down During Critical Peak
EV Charging Station Ignores Utility Command to Limit Fast-Charging
Loss of DER Control Occurs due to Invalid or Missing Messages
DER Systems Shut Down by Spoofed SCADA Control Commands
Threat Agent Spoofs DER Data Monitored by DER SCADA Systems
DER SCADA System Issues Invalid Commands
Utility DERMS Miscalculates DER Energy/Service Requests
Microgrid Disconnect Process Compromised via DERMS
Threat Agent Gains Access to Utility DERMS via FDEMS
Compromised DERMS Weather Data Modifies DER Output Forecasts
Spoofed Microgrid Status Messages Cause Disconnect from Grid
Malicious Code Injected into Substation Equipment via Remote Access
Remote Access Used to Compromise DMS
Spoofed Substation Field Devices Influence Automated Responses
QoS Spoofed to Create Denial of Service for DGM Communications
Threat Agent Triggers Blackout via Remote Access to Distribution System
Threat Agent Causes Worker Electrocution via Remote Access to Distribution System
Threat agent compromises serial control link to substation
Threat agent adds spurious trip parameters on remotely located plant support equipment and trips unit offline
Malicious and Non-malicious Insiders Pose Range of Threats
Inadequate Network Segregation Enables Access for Threat Agents

Bibliography:

[1] Briesemeister, Linda, et al. "Detection, correlation, and visualization of attacks against critical infrastructure systems." *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*. IEEE, 2010.

[2] Berthier, Robin, and William H. Sanders. "Specification-based intrusion detection for advanced metering infrastructures." *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*. IEEE, 2011.

[3] Reeves, Jason, et al. "Intrusion detection for resource-constrained embedded control systems in the power grid." *International Journal of Critical Infrastructure Protection* 5.2 (2012): 74-83.

[4] Berthier, Robin, and William H. Sanders. "Monitoring advanced metering infrastructures with amilyzer." *Cybersecurity of SCADA and Industrial Control Systems* (2013).

[5] Krishna, Varun Badrinath, Gabriel A. Weaver, and William H. Sanders. "PCA-based method for detecting integrity attacks on advanced metering infrastructure." *International Conference on Quantitative Evaluation of Systems*. Springer International Publishing, 2015.

[6] Jamei, Mahdi, et al. "Automated Anomaly Detection in Distribution Grids Using μ PMU Measurements." *arXiv preprint arXiv:1610.01107* (2016).

[7] Parvania, Masood, et al. "Hybrid control network intrusion detection systems for automated power distribution systems." *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*. IEEE, 2014.

[8] S. Etigowni, M. Cintuglu, M. Kazerooni, S. Hossain, P. Sun, K. Davis, O. Mohammed, S. Zonouz. "Cyber-Air-Gapped Detection of Controller Attacks through Physical Interdependencies." *IEEE International Conference on Smart Grid Communications*, 2016.

[9] Zonouz, Saman A., et al. "RRE: A game-theoretic intrusion response and recovery engine." *IEEE Transactions on Parallel and Distributed Systems* 25.2 (2014): 395-406.

[10] Lin, Hui, et al. "Safety-critical cyber-physical attacks: analysis, detection, and mitigation." *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM, 2016.

[11] Energy Sector Control Systems Working Group. Roadmap to achieve energy delivery systems cybersecurity[J]. Energetics, Inc, URL https://www. controlsystemsroadmap.net/ieRoadmap/% 20Documents/roadmap.pdf, 2011.

[12] Lee A. Electric sector failure scenarios and impact analyses-Draft[J]. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group, 2015, 12.