Secure Cloud SCADA for EDS

Website: https://cred-c.org/researchactivity/cloudscada

Researchers (Illinois): Klara Nahrstedt, Al Valdes

Industry Collaboration:

- Seeking industry collaborators who are considering cloud-based SCADA operations.

Description of research activity: This research activity will attempt to develop and demonstrate new cloud architecture variants for SCADA. Current SCADA systems typically feature a SCADA master communicating to one or more field sites. Each field site has one or more remote telemetry units (RTU) that communicate to the master. The RTU communicates to field devices for measurement and control.

The proposed activity will build on the microservice cloud model [4Ceed], specialized to obtain measurements from cyber-physical systems, securely curate and archive these measurements, and support separable workflows required by users accessing the system in a secure, role-based framework. The system includes a secure uploader to obtain and archive data (adapting the 4Ceed concept to a commercial SCADA historian, to be instantiated in the cloud); a curator to permit access, update, and edit; a coordinator to process, analyze, and correlate data from diverse sources, and support for processing components called microservices that handle diverse task requests using a publish/subscribe middleware layer with role-based access control. The individual security and SCADA service tasks (e.g., anomaly detection in SCADA data, analysis of historian data) will run as micro-services on top of Kubernetes or Docker Swarm, which are cluster resource management systems. The advantage of the micro-service cloud architecture and the overall 4CeeD middleware on top of Kubernetes will be that the processing of secure SCADA tasks and workflows will be light-weight.

Use cases to be demonstrated include detecting physically inconsistent system states, possibly indicative of an attack on measurements, as well as “look ahead” simulation to evaluate the impact of control commands before execution (Note that all these tasks are micro-services and will run on the cloud. The user can concatenate the tasks into a task graph, called workflow, and have them execute within micro-services where the 4CeeD middleware parses through the workflow/task graph and runs the whole workflow of tasks in a given order.)

The demonstration use case will be based on an ONG operational system identified jointly with an industry partner. However, except for the actual cyber-physical analytical models, this secure SDADA cloud system concept is applicable to SCADA in both ONG and electric power.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
Cloud-based SCADA is a potentially more resilient architecture for EDS OT, with system availability exceeding that of on-premise systems, providing for more robust EDS architectures and networks. The essentially limitless computational capability of a cloud environment permits big-data approaches to security not feasible on current constrained on-premise systems. In particular, security solutions based on high-fidelity simulation/emulation of the physical process can be invoked to leverage physics for security (for example, evaluate a control command for its impact on system state before allowing the command to execute on the physical system).

This activity promotes adoption of disruptive technologies such as cloud SCADA, edge computing, and IIOT “done right” from an operational and security standpoint.

A cloud SCADA architecture contains a virtual cloud copy of a physical OT system, including a virtual human-machine interface (HMI), field devices, and control-to-field communications. The cloud would likely interface with remote telemetry units, used in physical OT systems to aggregate communications with field devices, through an industrial internet of things (IIOT) hub (also called edge device) running protocol gateway services. Commands, measurements, and device state are duplicated in the cloud system, which has the capability for faster-than-real-time simulation, enabled by the limitless compute power in the cloud. This capability can be used to emulate the impact of a suspicious command in the cloud system before allowing its execution in the physical system. The capability builds on and extends the MS Azure concept of Device Twin [AZ] or Amazon AWS Device Shadow (also called Thing Shadow) [AWS].

Summary of EDS gap analysis: Refer to full EDS gap analysis.

Full EDS gap analysis: Driven by objectives of cost-effectiveness and system availability, OT environments are migrating an increasing amount of their computation from on-premise to cloud environments. Leading the adoption of this trend are SCADA asset owners in the oil and natural gas (ONG) sector, who are not faced with the time-criticality and latency challenges that arise from cloud-based SCADA operation in the electric power sector.

Cloud-based SCADA eliminates constraints of limited computation and communication of legacy SCADA systems, enabling advanced analytics for security as well as operational applications. Professional administration of cloud systems also addresses issues of patch management that impact on-premise systems.

The proposed activity will identify challenges, requirements, and best practices for SCADA and OT in cloud and mixed cloud/premise environments from a security and operational standpoint, and provide reference implementations to address sector needs.

Bibliography:

[4Ceed] Phuong Nguyen, Steven Konstanty, Todd Nicholson, Thomas O’Brien, Aaron Schwartz-Duval, Timothy Spila, Klara Nahrstedt, Roy H. Campbell, Indranil Gupta, Michael Chan, Kenton McHenry, Normand Paquin. “4CeeD: Real-Time Data Acquisition and Analysis Framework for Material-related Cyber-Physical Environments.” 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[AZ] Microsoft Azure, “Understand and use device twins in IoT Hub,” https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins, last accessed August 3, 2018.

[AWS] Amazon Web Services, “Device Shadow Service for AWS IoT,” https://docs.aws.amazon.com/iot/latest/developerguide/iot-device-shadows.html, last accessed August 3, 2018