Contribution ID: **581** Type: **Paper**

A process data integrated dynamic cybersecurity risk assessment approach for industrial control system

As digital instrumentation and control (I&C) systems are more fully integrated into nuclear power plants (NPPs) and communication networks cross boundaries of the business and operational systems, new opportunities for disrupting NPP operations are introduced. Enhancing the cybersecurity of digital I&C systems is key to ensuring the safety and economics of the nuclear power industry. Dynamic cybersecurity risk assessment helps decision-making by updating the risk value with architecture or configuration changes and cyber-attack movements.

The cybersecurity risk should include malicious cyber-attacks and unintentional cyber-incidents resulting from human factors. Here, the term cyber-events is used to indicate these two.
Cybersecurity risk assessment starts with vulnerability analysis for every digital device in the system. Common vulnerability libraries such as Common Vulnerabilities and Exposures (CVE) are used for finding entry points and vulnerabilities in these devices. To assess the risk accurately, ideally IT experts should find all possible attack paths for a system. However, it is impossible to emulate all the possibilities. Therefore, unknown cyber-attacks, such as zero-day attacks as well as unintentional cyber-incidents will lead to underestimation of the risk if they are excluded. One possible way of reducing these unknown factors is integration of process data into the evaluation of cybersecurity risk. An unsupervised anomaly detection model, which detects deviation from normal operation using process data results from cyber-events, is built to perform continuous risk assessment by updating the detected abnormal behavior. In addition, To avoid risk overestimation caused by process data deviation from a safety event, such as equipment and system failure or degradation, a model is proposed to distinguish cyber-events and safety events with a confidence interval.

Current literature suggests that the Bayesian network is a widely used approach in cybersecurity risk assessment because it conveys intuitive causal information as well as the conditional probabilities. Bayesian network is a directed acyclic graph (DAG) which is composed with nodes as variables and directed arcs which represents the conditional dependencies. The probability distribution of the nodes are usually presented by a conditional probability table (CPT).

A comprehensive dynamic cybersecurity risk assessment architecture is proposed in this research which consists of an evidence collection module which gathers information to identify the evidence of a cyber-event, including distinguishing the cyber-event and safety event; a Bayesian Network which presents intuitive dependency of different events; a regularly updated CPT built by Information Communication Technology (ICT), Operational Technology (OT), and Cybersecurity experts; and a risk value generation module which updates the risk dynamically.

A case study based on a real-time industrial control system (ICS) test bed will be conducted to demonstrate the proposed approach. This test bed consists of a physical experiment facility which simulates a typical two-loop nuclear power system thermal hydraulic component and a Supervisory Control and Data Acquisition (SCADA) system which controls the facility. A Bayesian Network will be built with a node description table.Simulated attacks will be conducted to assess the dynamic behavior of the proposed approach.

State

United States

Gender

Female

Authors: Ms ZHANG, Fan (University of Tennessee-Knoxville); Mr SPIRITO, Christopher (Idaho National Laboratory); Prof. COBLE, Jamie (University of Tennessee-Knoxville)

Presenter: Ms ZHANG, Fan (University of Tennessee-Knoxville)

Track Classification: CC: Information and computer security considerations for nuclear security