Contribution ID: **503** Type: **Paper**

Toward a Localized Cybersecurity Strategy for Critical Assets

Monday 10 February 2020 11:45 (15 minutes)

The quantity and capability of cyber-attacks targeting Industrial Control System (ICSs) is growing rapidly. The integration of digital technology and communication channels in Nuclear Power Plants (NPPs) introduces vulnerabilities to cyber-attacks that may threaten the safety and operation of nuclear power facilities. Current efforts in developing and deploying cybersecurity solutions have focused largely on intrusion prevention, but focus is now turning toward detecting cyber-attacks and ICS intrusions.

Assuming that Intrusion Detection Systems (IDSs) based on host system and network data fail to detect the evidence of a cyber-attack, detection models based on process data (sensor data and control data) can detect deviations from normal operation, which could be a potential cyber-attack. However, most of these process data-based IDSs focus on detecting abnormal signals based on the relationship between the various signals measured by different types of sensors in NPPs. Therefore, these models are unable to detect cyber-attacks where the attacker intelligently tampers with most or all of the signals used in an analysis; if the attacker can tamper with one signal, it is reasonable that they can also tamper other signals simultaneously. In a replay attack, for example, an attacker masks the malicious activity by replaying older measurements. This paper proposes a localized cybersecurity strategy to address cyber-attack detection under scenarios where the sensors are compromised. This proposed strategy excludes the measurements that may be compromised.

The proposed strategy integrates a Kalman Filter into the controller itself to use the command it issued at time t and the state values at time t−1 to predict the expected response of the state values of t+1. This expected response is compared with measurements at t+1; deviations between these values that are greater than a threshold are considered anomalous and potentially caused by a cyber-attack. A Hardware-In-the-Loop (HIL) testbed, which consists of an NPP simulator and a Programmable Logic Controller (PLC), was built to evaluate the effectiveness of the proposed method. The PLC is programmed to control the Steam Generator (SG) water level at the desired set point, by adjusting the feedwater pump speed. A false data injection attack was launched towards the PLC, in which the attacker altered the SG water level measurement using a Man-In-The-Middle (MITM) attack. The altered water level measurement received by the PLC shows that the water level is higher than the set point, which leads the PLC to output commands to lower the feedwater pump speed and subsequently the measured water level. Assuming that the attacker tampered with the SG water level measurement at time t, the model implemented in the controller takes the command issued at time t, which is not compromised, and the state values at time t−1 as inputs, to predict the expected state values at time t+1. By comparing the expected value and the measurements of the state values, which are tampered by attacker at time t+1, the anomaly may be detected. The results of the Kalman Filter implemented in the PLC will be presented in the full paper.

State

United States

Gender

Female

Authors: Ms ZHANG, Fan (University of Tennessee-Knoxville); Prof. COBLE, Jamie (University of Tennessee--Knoxville); Mr ALLISON, David (AIT Austrian Institute of Technology); Dr SMITH, Paul (AIT Austrian Institute of Technology); Prof. BUSQUIM, Rodney (University of Sao Paulo)

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

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

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