Functional Security Enhancements for Existing SCADA Systems

Overview and Problem Statement

Although SCADA systems were originally endowed with relatively minimal networking capabilities, over the years they have increasingly migrated to IP networks that allow communication with numerous devices multiplexing the same communication medium. While that migration advances the value proposition of the emerging smart grid, it also clearly provides a vulnerable cyber medium through which potential attackers can access and manipulate critical physical power equipment, and Ethernet protocols are exposed to traffic from a wide variety of sources. Therefore, securing the networked SCADA systems of the emerging smart grid is undoubtedly of great importance in assessing the impact of any potential menace on the stability and security of such systems. A significant number of security countermeasures, such as firewalls, encryption, and network intrusion detection systems (NIDS), have been widely adopted to protect and isolate the network perimeter of the electric power grid from external attacks. Network intrusion detection is a widely used technique to address cyber attacks either inside or at the border of a network.

In this work, we proposed a novel use of NIDS tailored to detect attacks against networks that support hybrid controllers of power grid protection schemes. In our approach, we implement specification-based intrusion detection signatures based on the execution of the hybrid automata that specify the communication rules and physical limits that the system should obey. To validate our idea, we developed an experimental framework consisting of a simulation of the physical system and an emulation of the master controller, which serves as the digital relay that implements the power grid protection mechanism. Our Hybrid Control NIDS (HC-NIDS) continuously monitors and analyzes the network traffic exchanged within the physical system. It identifies traffic that deviates from the expected communication pattern or physical limitations, which could place the system in an unsafe mode of operation. Our experimental analysis demonstrates that our approach is able to detect a diverse range of attacks that attempt to compromise the physical process by leveraging information about the physical part of the power system.

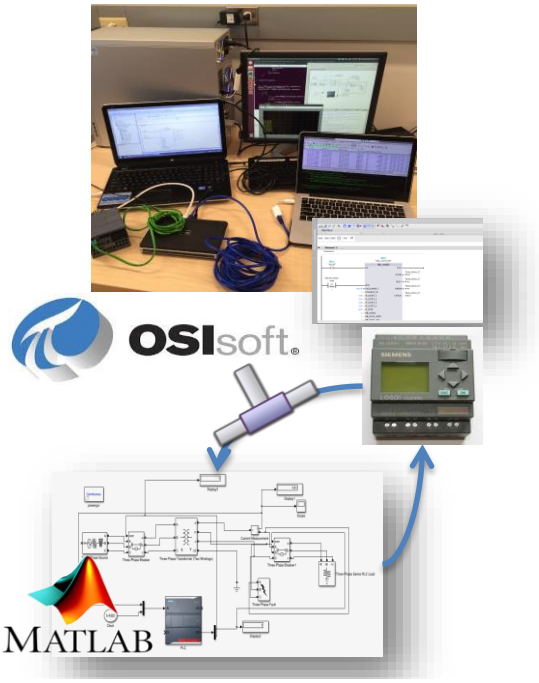

Figure 1. The developed testbed.

Most recently, we focused on the expansion of our developed security framework to work under the industry's standard real-time data management systems. In this project, we are collaborating with OSIsoft, one of the industry leaders in data management systems, to implement our security framework on their PI System. The PI System can be queried by our HC-NIDS, which implements a set of security policies and is aware of the physical laws and communication rules that designate the normal behavior of the cyber-physical system. A "network tap" grabs the network traffic exchanged between the Matlab/Simulink simulation of the physical system and a real programmable logic controller (PLC) that implements a protection mechanism, e.g., a power transformer's overcurrent protection mechanism. The captured network traffic is stored in the PI Server in the form of predefined tags, which HC-NIDS retrieves in order to check for possible anomalies or attacks. HC-NIDS executes a set of intrusion detection rules, detects any violations, and reports suspicious events by generating alerts and keeping track of the events that triggered alarms.

Research Objectives

Our goal is to identify and implement intrusion detection rules for protective digital relays in power systems based on the knowledge of the hybrid automata executed by the network of relays. To mitigate an important category of cyber-physical vulnerabilities, our novel use of NIDS integrates traditional NIDS approaches' computer and network security communication rules with information related to the system's physical limits and the expected execution of its hybrid automata models.

Technical Description and Solution Approach

Our Hybrid Control NIDS (HC-NIDS) assumes that the control environment runs protection control algorithms that are codified to allow the system to transition only in specific safe states. Those states are called *hybrid states* because they encompass the state of discrete switches (coils) and the normal dynamics of the analog system variables, under the specific configuration of switches. The allowed transitions between different hybrid states are described in hybrid automata models, which capture the combination of protection schemes and physical properties of a system as well as their safe range of operation. Transitions are triggered by physical changes and commands issued via network packets flowing between field devices and central controllers.

The NIDS method is aware of the hybrid automaton model and continuously monitors and analyzes the network traffic exchanged by the field devices that activate the protection scheme to ensure that the exchanged commands and information are consistent with the appropriate hybrid automaton model.

Each hybrid state corresponds to specific values for the switches and specific ranges for the current, voltage, temperature, and so forth.

Results and Benefits

We developed an experimental framework, shown in figure 1 that allows us to create communication between the simulated physical process and a PLC through an Ethernet interface that sends information via the Modbus TCP industrial control protocol. A "network tap" grabs the network traffic exchanged between the Matlab/Simulink simulation of the physical system, and the real controller (PLC) that implements a protection mechanism, e.g., a power transformer's overcurrent protection mechanism. The captured network traffic is stored in the PI Server in the form of predefined tags, which the HC-NIDS retrieves in order to check for possible anomalies or attacks. Any traffic that deviates from the expected normal operation of the protection scheme, as defined by our intrusion detection rules, is characterized as a possible threat and triggers the HC-NIDS to raise an alert. By utilizing the data stored in the PI Server in order to execute our HC-NIDS rules, which combine both communication and physical rules that the system should obey, we have shown that the HC-NIDS approach can detect sophisticated attacks against an overcurrent protection scheme for a power transformer.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Georgia Koutsandria, gkoutsandria@ucdavis.edu
- Masood Parvania, mparvania@ucdavis.edu
- Reinhard Gentz, rgentz@ucdavis.edu
- Mahdi Jamei, mjamei@ucdavis.edu

Industry and External Collaborators

- Sean Peisert, UC Davis/Lawrence Berkeley National Lab (LBNL)
- Charles McParland, Lawrence Berkeley National Lab (LBNL)
- OSIsoft, LLC

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security