Abstract

Smart Grid Cybersecurity Experimentation: Architecture and Methodology

Doctoral Degree
Beuran's Laboratory
LE Duy Tan
s1820035

The smart grid is a vital part of the Japanese initiative named "Society 5.0". It is also one of the core technologies enabling sustainable economic and social developments. This next-generation electrical power system integrates the traditional electrical grid and computer technology to enhance the automation, connectivity, and communication of the different power network components. In recent years, various attacks have been made on the smart grid system, which lead to serious harmful consequences.

The smart grid structure is complex and includes two essential parts: network communication and the power grid. Researchers need to consider the relationship between these components for further system investigation and improvement. Moreover, it is not a trivial activity to implement a real smart grid system for the cybersecurity experiment and validation process, since it entails high risk of destroying the electrical infrastructure and equipment, resulting in enormous economic consequences and even in danger regarding human lives. As a result, in this critical domain where testing on a real system is so hazardous, simulation and analysis techniques can be considered as an effective solution to make smart grid cybersecurity experimentation possible.

The attack simulation and analysis tools are mainly applied to simulate attacks and emulate the actual circumstances in which these attacks occur, particularly system settings and network topologies. The application of real incident simulation tools to cybersecurity experimentation is a primary factor for enhancing the efficacy of the experimentation process. Due to its pioneering characteristics, not many research studies currently exist on practical cybersecurity experimentation for the smart grid. To the best of our knowledge, this is one of the first research works that thoroughly addresses this important issue.

This dissertation identifies the need for realistic cybersecurity experimentation for the smart grid and formulates the corresponding system design requirements. A general architecture for smart grid cybersecurity experimentation, which fulfills these specifications, is also introduced. To deal with the great system complexity but still achieve our goal, we divided smart grid cybersecurity experimentation into two parts: the co-simulation approach and the analytical modeling approach. The specifications, general architectures and methodologies of both are determined and detailed herein.

In the co-simulation approach, we introduced and implemented GridAttackSim. This novel co-simulation framework enables the simulation of smart grid infrastructure characteristics, allows various cybersecurity attacks to be simulated, and evaluates their consequences. A case study was performed with two different test feeders to validate the functionality of GridAttackSim.

In the analytical modeling approach, we first provided a literature review on the current state-of-the-art for smart grid attack analysis. The most promising directions were then applied to design and implement GridAttackAnalyzer (Cyber Attack Analysis Framework for Smart Grids). A case study with various attack scenarios was conducted to validate this framework.

This dissertation's main contribution is a methodology that can effectively support realistic cybersecurity experimentation for the smart grid. This methodology was implemented in the form of the two frameworks mentioned above, GridAttackSim and GridAttackAnalyzer. Using these frameworks, researchers can determine the consequences of various attack types, thus making possible the early development and evaluation of new anomaly detection methods and mitigation even before their actual implementation. Moreover, the frameworks can also be used to define effective approaches for the implementation of smart grid technology, for instance, to determine efficient communication requirements for device operation.

In addition, the systems can be used for cybersecurity training of IT experts and cybersecurity professionals. For example, based on evaluating various security metrics, IT experts and cybersecurity professionals can discover all the possible attack paths, and determine which vulnerable devices on those paths should be protected in advance to prevent the most significant damage. It also becomes possible to compare the effectiveness of specific device-level strategies deployed for different devices. For the network level, the performance of various defense strategies for smart grid systems can be assessed. Furthermore, our work can help system planners to estimate the attack damage cost on a smart grid system.

Keywords: smart grid, cybersecurity experimentation, simulation, co-simulation, attack analysis.