Smart Grid Cyber Security: Training for the Future

Overview and Problem Statement

The intent of this activity is to develop an open training platform that facilitates the rapid education of a wide variety of participants on important aspects of smart grid cyber security. The training platform will consist of both presentations and hands-on training exercises that will aid in the education of interested parties in research, industry, and government.

In this work, we aim to create a phased and modular learning platform that provides the essential base knowledge for this sector and builds upon that base knowledge with each lesson to advance students' understanding of smart grid cyber security. At each phase in the process, we will provide concrete applications of the topic areas to facilitate participants' learning. By using a combination of diverse educational strategies, we expect to be able to train a variety of people effectively and efficiently.

Research Objectives

- Develop a modular, phased learning platform for cyber security education in the electric power grid.
  - Made up of diverse topic areas spiraling deeper into relevant details of interest (tracks).
  - Consists of lecture material, an electronic exercise environment, and hands-on exercises to support learning.
- Provide a fully open, available, and vetted curriculum.
  - Material needs to be widely usable, and designed such that different experts can easily contribute new content and revise existing content as the landscape changes.
  - Made to be accessible to anyone, ranging from CEOs to engineers to office staff, while taking a project-based, hands-on, active-learning approach to reinforce the subject matter.
- **Smart Grid Application Area:** Education, training, and workforce development.

Technical Description and Solution Approach

- This effort started with an initial gap analysis and mapping of existing cyber security training for the electric power grid, in relation to the DOE Secure Power System Professional (SPSP) and DHS National Initiative for Cybersecurity Education (NICE) competencies and job responsibility designations.
- We are gathering topics of interest and information on sector needs by working with industry and leveraging existing knowledge of the sector.
- Based on the gap analysis, a core curriculum is being developed that is a combination of new material and material from previous TCIPG short courses on cyber security in the electric power grid, and is structured to facilitate easy extension into new areas.
- The material follows a phased approach to learning that includes active, project-based "learning by doing" to anchor the training material.
- We are preparing lectures along with hands-on exercises to reinforce the material under discussion.
- We will release the training in stages, and will revise it in response to feedback from the participants.
- Ongoing analysis will be conducted to determine coverage and needed topics for future releases.

Topics Covered

- Power fundamentals
- Cyber security fundamentals
- Communications and networking

Topics Covered (con't)

- Cyber infrastructure in the electric power grid
- Monitoring and situational awareness
- Advanced metering infrastructure
- Smart grid guidance documents
- Electric sector capability maturity model
- Privacy in the smart grid
- Critical infrastructure security examples and impact
- A perspective on security
- Security challenges in distribution automation
- Embedded assessment
- SCADA fundamentals
- Robust control systems
- And more…

Results and Benefits

- Gap analysis has been conducted along with a mapping to job responsibilities and competencies.
- Preliminary curriculum has been created.
- Several modules have been alpha-tested in the field with industry participants.
- Topical spirals into more detail are being developed.
- The training reflects the broad expertise of the TCIPG research team and acts as a training platform that future researchers, workforce, or government entities can build upon and adapt.
- Offers open, widely available training material on cyber security in the electric power grid that has been vetted by subject matter experts.
- Provides increased accessibility to training in this domain.
- **External Interactions**: CYBATI and SANS
- **Technology Readiness Level:** Alpha (but has already been utilized).

Field Use

- Prior incarnations of the lecture material and short courses have been used to train hundreds of attendees from academia, industry, and government.
- A very early version of the revised lecture material was used at the 3CS conference to provide training for community college educators and other interested parties.
- Modules of the core curriculum have been used to train vendors and utility personnel in this domain.
- Strong continued industry interest in the material.

Future Efforts

- Full open-source release planned for August 2015.
- Explore integration and use with other efforts such as cybatiWorks or the SANS curriculum.

Researcher

- Tim Yardley, yardley@illinois.edu

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