Usable Management Tools for the Smarter Grid's Data Avalanche

G. A. Weaver and S. W. Smith

Goals

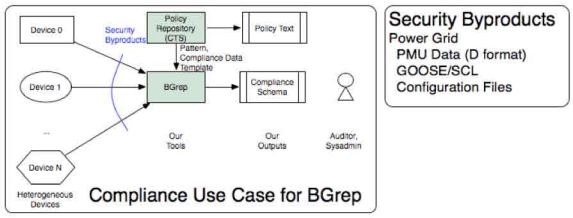
- The present and future smart grid has a vast population of diverse devices that generate data—lots of data.
- How will humans manage these data?
  - Dynamic generation of evidence for CIP audits.
  - Continuous monitoring of device behavior despite the variety, volume, and variability of data.

Fundamental Questions/Challenges

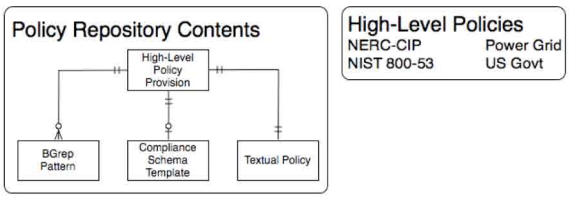
- ***How can humans deal with the smart grid "data avalanche" and thereby gain an increased situational awareness of cyber-security for the smarter grid?***
- Challenges in our discussions with industry partners on dealing with the data avalanche include the following:
  - *The variety of data formats:* PMU historian data come in the D and COMTRADE formats.
  - *The large volume of data:* 25 PMUs generated 2 TB of data in a year.
  - *The variability of data bandwidth:* If a bus fault occurs, a device may generate a flood of GOOSE data.

Research Plan

- We found that many byproducts of security processes are structured texts, and so we write tools to consume and analyze these structures. Our tools streamline audit processes and increase cyber-security situational awareness.
- Our approach has already been used successfully in other domains (see section on research results).
- We plan to do the following:
  - Apply our network management tools to CIP audits and monitoring.



  - Apply our PKI analysis tools to build a policy repository.



Research Results

- Previous work in other domains demonstrates the potential for tools that consume human-readable, machine-actionable security byproducts.
  - Preliminary results for our PKI certificate policy tools were published in *EuroPKI 2009* and *IDTrust 2010*. The tools have been used by Digicert and Protiviti.
  - Preliminary results for our network configuration tools were published at *USENIX HotICE 2011*. We are working with sysadmins to improve our tools.
- Our work in the power grid considers the potential of our tools to help humans manage the aforementioned "data avalanche."
  - Since this summer, we have been actively researching IEDs (primarily PMUs) that generate lots of data in the smarter grid of the present and future.
  - *Get data:* We have received sample PMU data in the D format.
  - *Understand data:* We have spoken to power engineers to understand the kinds of events that power engineers look at via PMU data.
  - *Relate data to cyber-security:* We are working to align PMU data as well as configuration data with various high-level regulations.

Broader Impact

- More generally, we are developing tools to process and analyze machine-actionable, human-readable security byproducts. We have already applied and are continuing to apply our tools to the domains of PKI and network configuration management.
- The similar tools we have built in other domains are already generating real-world interest.

Interaction with Other Projects

- In our efforts to apply network management tools to CIP audits and monitoring as well as our efforts to build a regulatory repository, we are working with several folks at UIUC, including Tim Yardley, Rakesh Bobba, Jun Ho Huh, and Edmond Rogers.
- In addition, the regulatory repository our project provides may also be of use to Sean Smith's "PKI for the Smarter Grid" project.

Future Efforts

- Moving into the future, we are going to do the following:
  - Continue to gain understanding of the different kinds of data that could be used to gain some situational awareness of compliance.
  - Continue to gain understanding of the kinds of events that power engineers are interested in, but also explore the possibility of cyber-security services built upon processed PMU data.
  - Look into change log generation for configuration files and reports of device behavior based on logs. In that way, we can generate documentation for humans based directly on the behavior of devices on the grid.
- ***We need***
  - ***Domain experts*** with nails that fit this hammer.
  - ***TCIPG professor*** to be external member of Ph.D. committee.