Responding To and Managing Cyber (and Physical) Events

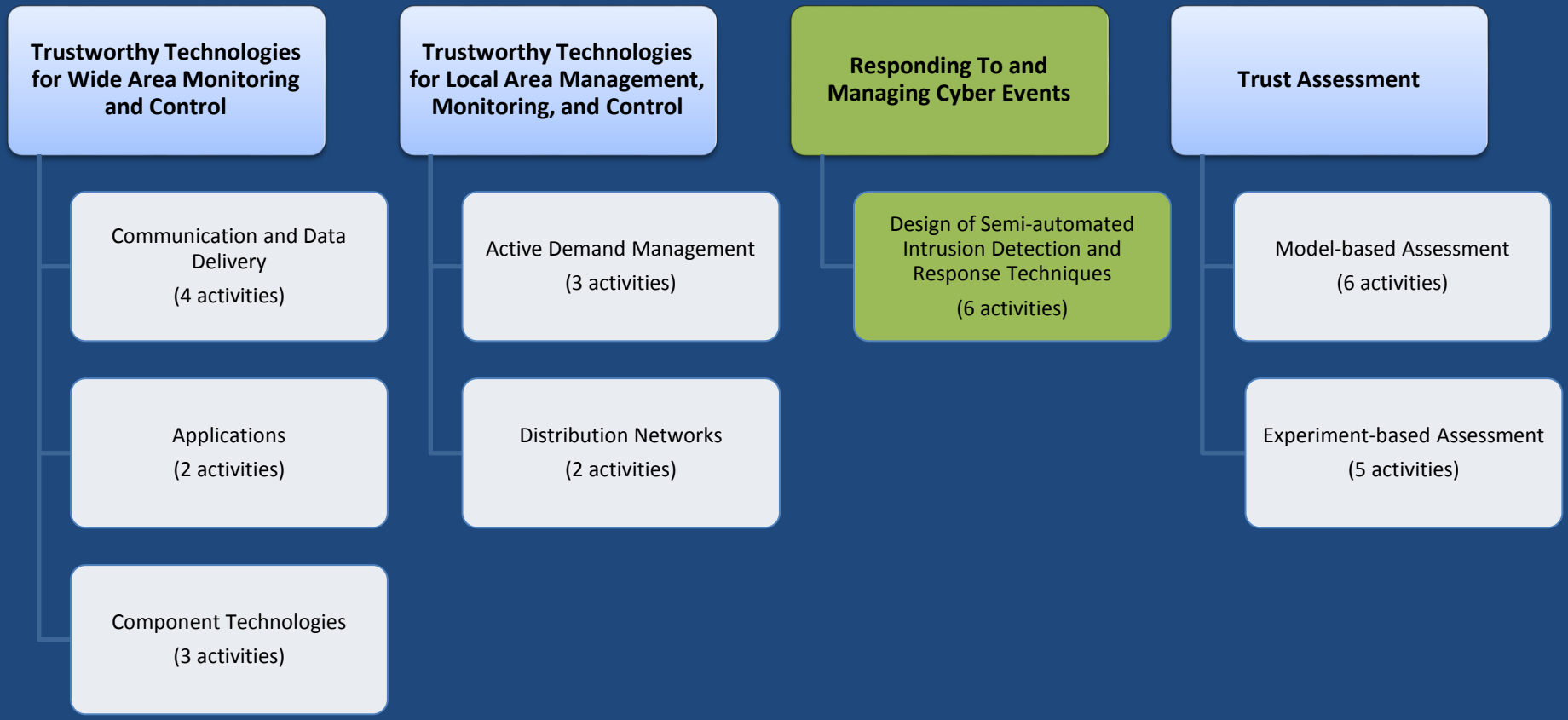
Bill Sanders

Number of Activities: 6

2012 Industry Workshop

October 30, 2012

TCIPG Technical Clusters and Threads



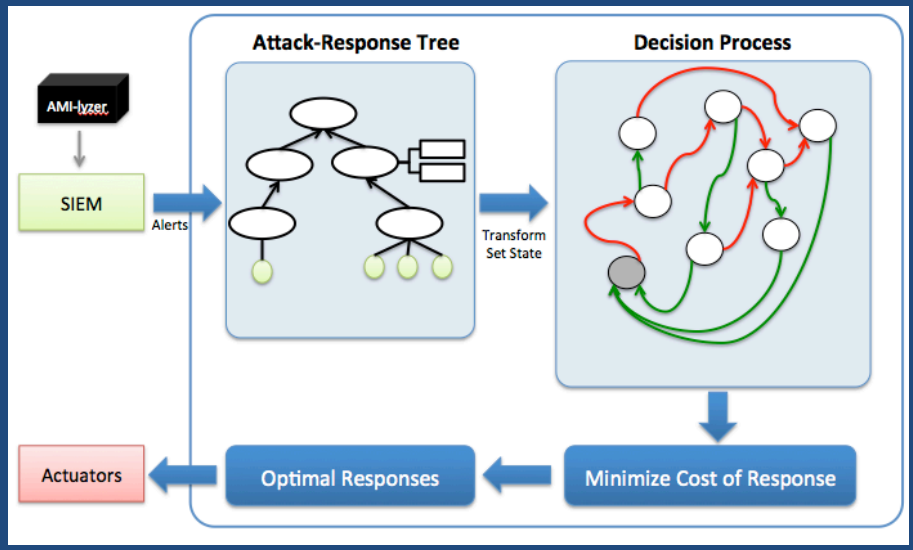
Cluster Overview

- Combined cyber and physical attack detection, response to detected attacks, and recovery from attack consequences is essential to providing resilience
- Existing detection and response methods are *ad hoc*, at best, and rely on assumptions that may not hold
- Aim to detect and respond to cyber and physical events, providing resilience to partially successful attacks that may occur:
  - Making use of cyber and physical state information to detect attacks
  - Determine appropriate response actions in order to maintain continuous operation
  - Minimize recovery time when disruptions do occur and use forensics to learn to prevent future attacks

Cluster Approach

Create complete detection, response, recovery, and forensics environment, at all necessary levels of abstraction:

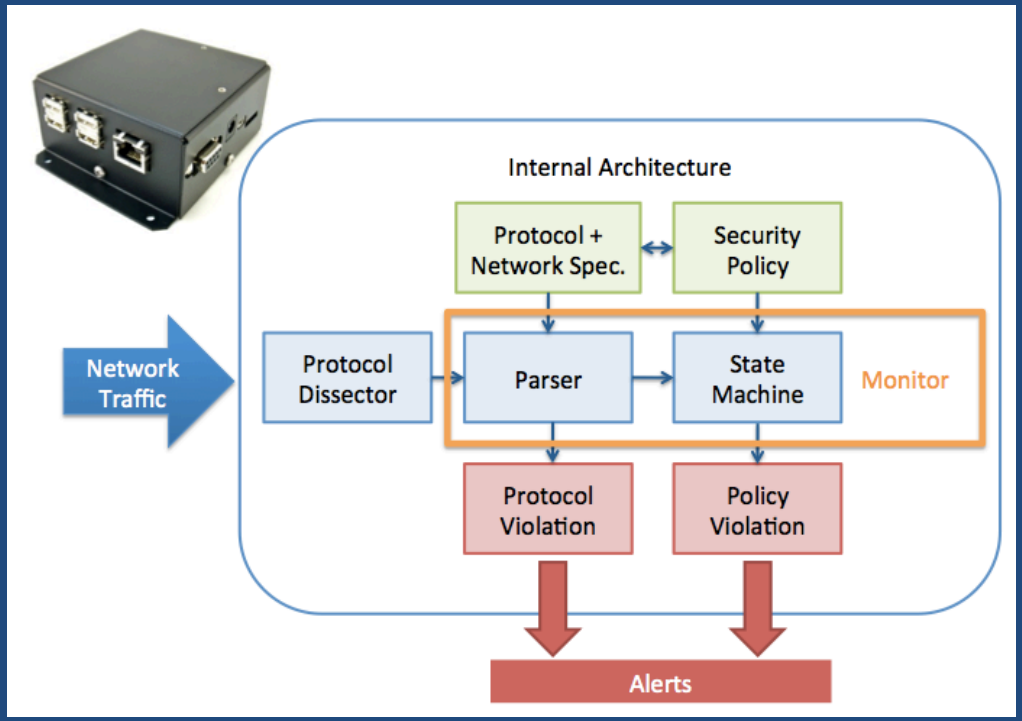
- Physical level
  - Taking into account noise and malicious manipulation of values
- Hardware level
  - Respecting embedded and cost sensitive nature of power system components
- OS/Platform level
  - Dealing with lack of source code and other observability limitations
- Computer network level
  - Accommodating observability limitations due to encryption and protocols



Activity Highlights

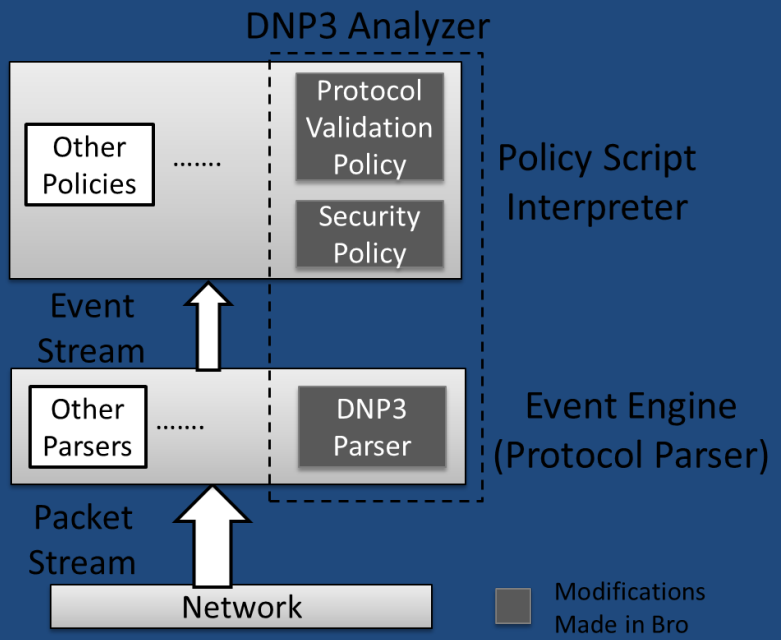
- *Specification-Based IDS for Smart Meters:* Design an efficient monitoring architecture (AMI-Iyzer) to detect and potentially prevent intrusions targeting or originating from an Advanced Metering Infrastructure (AMI)

- Collaboration with Fujitsu Labs, FirstEnergy, EPRI, and Itron
- Prototype being deployed in Utility AMI Testbed



Activity Highlights, cont.

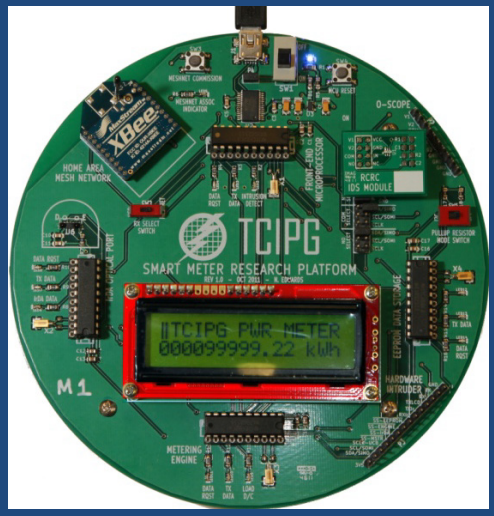
- *Specification-Based IDS for DNP3 Protocol*: Develop specification-based IDS, using Bro, for DNP3 protocol
- Source code is being merged into Bro's source code repository

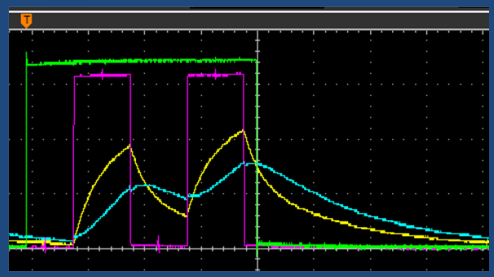


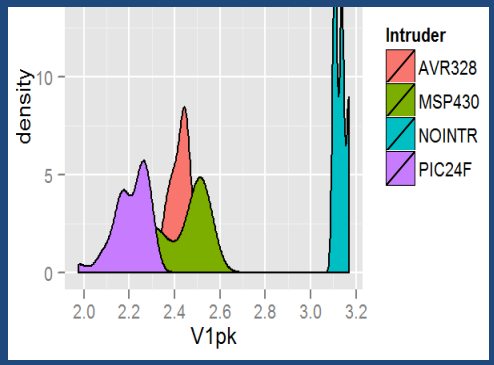
- *Usable Management Tools for the Smarter Grid's Data Avalanche:* Designed, developed, and are currently evaluating our eXtended Unix text-processing Tools (XUTools)
- Practitioners can use XUTools to analyze security policies in terms of high-level language constructs

Activity Highlights, cont.

- *Hardware-Based IDS for AMI Devices:* Completed development of and demonstrated analog signal-level hardware-based IDS for smart meter and other embedded infrastructures
- System can identify the presence of a hardware Trojan at 100% accuracy with dataset of over 2000 measurements, and correctly distinguishes between several types of implanted Trojans at 89% accuracy.

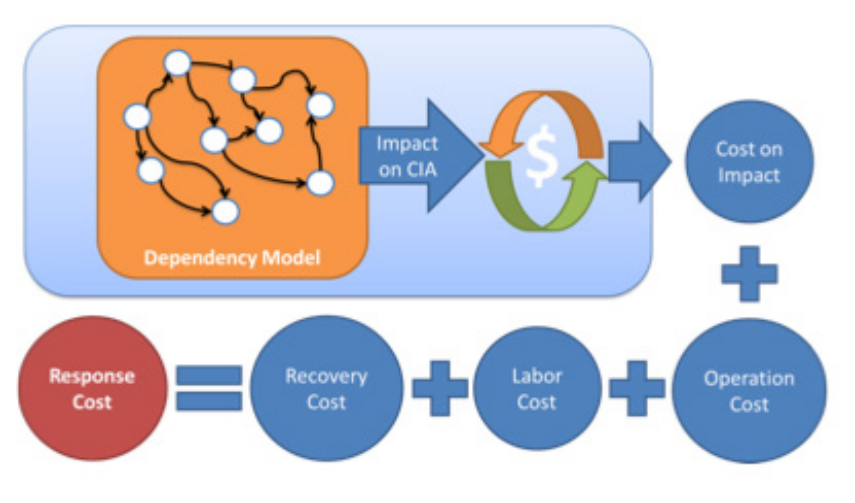






Activity Highlights, cont.

- *Game-Theoretic Intrusion Response and Recovery Engine:* Extended Recovery-Response Engine (RRE) uses knowledge about the power grid's current security-state and its security level
- Completed integrated AMI attack detection and response demonstration
- Developing large scale case study using
  - Cost model derived from real GIS Data



- *Assessment and Forensics for Large-Scale Smart Grid networks:* Create a framework to input and interpret infrastructure polices in the architecture which is scalable and resilient to small numbers of compromised nodes

Cluster Impact

- Working with FirstEnergy on a pilot deployment of TCIPG's AMI-lyzer which protects AMI systems using C12.22 and C12.19 protocols
- Demonstration of AMI-lyzer at EPRI Power Delivery and Utilization meeting
- Funded work with EPRI to map NESCOR AMI failure scenarios to AMI-lyzer checkers
- 3 provisional patent applications for hardware-based IDS for meters
- XUTools Data Analysis tools appeared on the front pages of Slashdot and Reddit due to USENIX LISA 2012 poster; articles also featured in ACM Tech News, CIO Magazine, Communications of the ACM, and Computerworld, etc.

Planned Research for Coming Year

- Build large scale, realistic AMI case study for combined detection, response, and recovery using RRE and AMI-lyzer
- Work with EPRI and utility partners to deploy AMI-lyzer in utility testbed or pilot settings
- Develop new version of RRE engine, using symbolic data structures and other theoretical advances to achieve scalability
- Merge Bro DNP3 specification checkers into its public source code repository; work with DNP3 User's group to further enhance detection capability of the code
- Using XUTools, work with security practitioners to create an inventory of network security primitives, measure the similarity between objects in that inventory, see how those primitives are used, and then measure the evolution of the network through time

Questions?