TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

CLUSTER: RESPONDING TO AND MANAGING CYBER EVENTS

NOVEMBER 12, 2014

AL VALDES

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

CLUSTER THEMES

- Grid cyber infrastructure
  - Enables safe, efficient, reliable grid operation
  - Presents an attack surface
- We build the most trustworthy systems we can, but we must anticipate that cyber events will occur
- This cluster addresses cyber events through
  - Advanced, grid-aware detection mechanisms
  - Response strategies that comprehend consequences and tradeoffs
  - Post-event forensics to restore systems to a secure state
- Benefit is a self-aware, self-healing grid from the cyber as well as physical standpoint

BACKGROUND

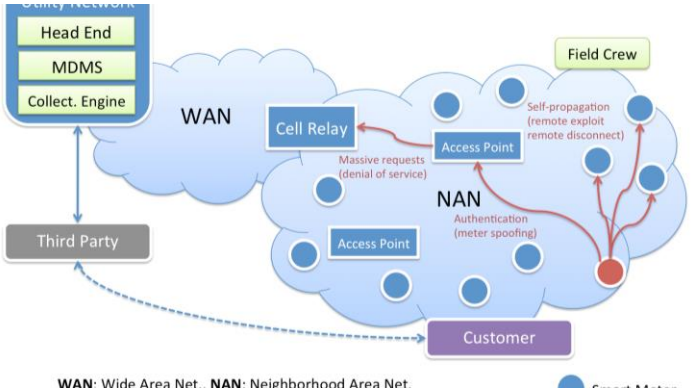
- The early days (before 2005): Cyber-event management not common
- The middle ages: Adapted enterprise security solutions for Intrusion Detection Systems (IDS), some Security Incident Event Management) SIEM
  - SCADA signatures for conventional IDS
  - DHS LOGIIC Event Correlation Project
- Now:
  - Security awareness in the sector
  - Sector-specific solutions
  - Regulatory framework

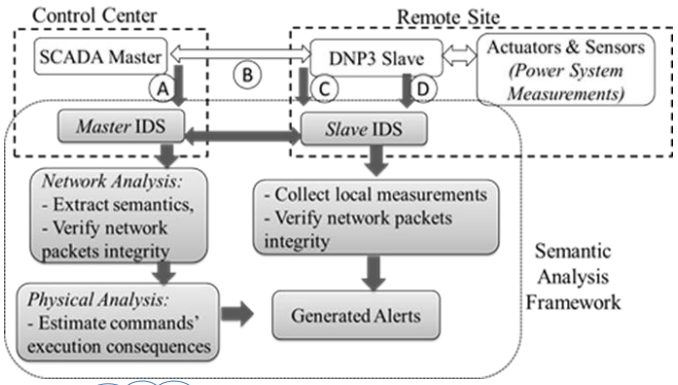
CLUSTER ACTIVITIES

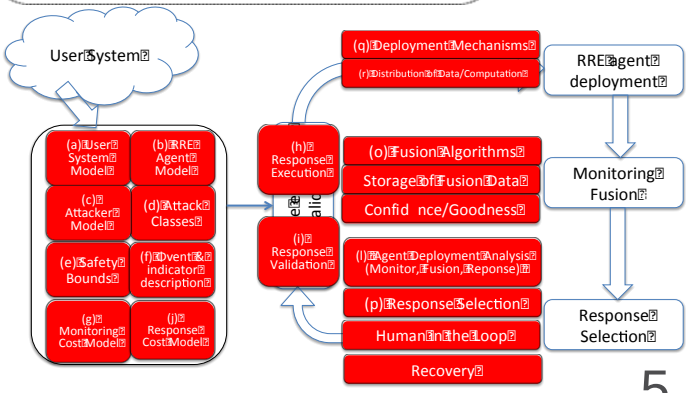
- Current
  - Response and Recovery Engine (RRE)
  - Forensics
  - AMI Malware Detection
  - IDS for Smart Grid leveraging real time properties
  - Specification-based IDS for DNP3
  - AMIlyzer
- Previous
  - Coordinating black start using synchrophasors
  - Hardware-based IDS for smart meters
  - Usable management tools for the smart grid “data avalanche”

CLUSTER ACCOMPLISHMENTS

- Specific solutions for grid delivery systems (AMIlyzer)
- Solutions that comprehend cyber and physical state
  - DNP3 security
  - TEDDI
  - Embedded systems security
- From event management to response and recovery (RRE)







CURRENT CHALLENGES

- Overcome limitations of legacy enterprise cybersecurity solutions as applied to grid systems
- Create detection, response, and recovery environment
  - At all levels of abstraction
  - Comprehend physical factors, hardware, software, networks
  - Reinforce detection and guide response based on indicators of the physical system state
- Validate solutions

EMERGING OPPORTUNITIES

- Advanced security analytics
  - Integrating physical and cyber indicators
  - Multi-resolution, multi-subscriber views
  - Cloud is coming
  - Informing effective incident response

EMERGING OPPORTUNITIES

- Sophisticated security detection, modeling, optimization, and decision support must interface with the “human in the loop”
  - Must be intuitive
  - Must comprehend heterogeneity of devices and their deployment
  - Must be consequence-aware
  - Must support of timely and effective planning, response, and restoration in both cyber and physical terms