EPRI CIO Workshop

Common Cyber Security Services

November 30, 2012

System Stability through technology

Basic capability

Advanced capabilities

Mechanical controls

Fly by wire

Stability through physics

Stability through technology
Smart Grid Design Goals

• **More** – increased capabilities
  – More capabilities at the edge and enterprise, pervasive automation

• **Better** – faster, more reliable & secure
  – The electric grid is more resilient
  – Dynamic control of all security elements allows the system to adapt to evolving threats

• **Easier** – usability (convergence, unified control, visualization, information on demand)
  – Tens of Millions of nodes are manageable
  – Situational awareness
  – Common Services allow for easier integration of new capabilities and technologies

Smart Grid System of Systems (SoS) Research

Four evolutions of Smart Grid SoS Architectures

- **Silos**
- **ESB**
- **Adapter-based**
- **Common**

1. Current-state
2. Typical SI Approach
3. DoD-style approach
4. Standards-based Internet-style
CCS Introduction

- **Changing Landscape**
  - Increased attention from government, media, public
  - New class of adversary and malicious threats
  - Increase use of Communications and Automation on the grid
  - Customer and 3rd Party Interaction increasing

- **Objectives**
  - Security needs to keep pace with increasing pace of technology adoption
  - Security needs to be baked in to new procurements while addressing legacy environment (No device left behind)
  - Security needs to comply with all regulations and relevant standards
  - Adhere to common services architecture that reduces implementation and operational costs through reuse

- **Solution**
  - CCS is a common service for securing applications and devices
  - CCS focuses on securing all critical energy delivery operations
  - CCS is the first open and standards based implementation which meets all objectives

CCS Technology Highlights

- The most advanced security system in the energy sector
  - Next generation utility technologies
  - DoD technology transfer
  - Best practices from many sectors
  - Modern SOA style architecture

- The most compliant security system
  - NERC CIP Version X
  - All Federal Processing Standards (DHS, FIPS)
  - NIST Compliant (NISTIR, SP)

- A robust, scalable and dynamic security system
  - Supports all Grid Applications
  - Supports current and next generation networking (MPLS)
  - Supports all major protocols used on the Grid
  - Modular Construction
CCS Technology Highlights

- Easily Integrated into existing environment
  - Supports existing control and IT investments (Directory Services, Enterprise PKI)
  - 8 inflight advanced programs are relying on new services (e.g. ISGD, Phasor Measurement, SA3, C-RAS, etc.)
  - Supports gradual evolution to full compliance over time
- Ease of Use
  - AMI Security uses command line and requires vendor support
  - CCS has next generation web based graphical user interface
  - Enables a powerful and unified security operations center
- IEC has committed to align with CCS principles
  - Hosted IEC TC 57 Security Meetings
  - New Part to FERC reviewed/recommended 62351
- GE and Subnet are deploying CCS compatible devices and discussion are underway with other major vendors

CCS Concepts: Security Associations

Multiple scenarios supported
CCS Concepts: Advanced Visualization
Easy to use, intuitive interface

CCS Concepts: Control Plane
All Devices are centrally controlled
Initial CCS Capabilities

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Public Key Infrastructure (PKI), Identity Management, Attribute Certificates (BoH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Centrally Managed and Configured Security Associations (SAs)</td>
</tr>
<tr>
<td>Accounting</td>
<td>Audit &amp; Reporting (Alert, Syslog)</td>
</tr>
<tr>
<td></td>
<td>Security Information and Event Management (SIEM)</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity Management Authority (IMA)</td>
</tr>
<tr>
<td></td>
<td>Trusted Network Connect</td>
</tr>
<tr>
<td></td>
<td>Bill-of-Health</td>
</tr>
<tr>
<td>Quality-of-Trust</td>
<td>Source-based Data Labeling : Trusted, Questionable, Untrusted</td>
</tr>
<tr>
<td>Peer-to-Peer</td>
<td>Peer-to-peer middleware using Data Distribution System (DDS)</td>
</tr>
<tr>
<td>Communication</td>
<td>Use only for control plane</td>
</tr>
<tr>
<td></td>
<td>Several vendors available including open source</td>
</tr>
<tr>
<td>Dynamic Interactive</td>
<td>Accessed via Web Browser (Chrome 14, Firefox 7 and IE 10 in the future)</td>
</tr>
<tr>
<td>GUI</td>
<td>Built-in Test and Peek-Poke Capabilities</td>
</tr>
</tbody>
</table>

GUI Icon Legend

- All Nodes in the security network are displayed as circles and quadrants represent quality of security attributes.
To ensure proper operation, rigorous technology evaluation must take place in a controlled environment before smart grid technologies are deployed on the grid.