An Integrated Security System of Protecting Smart Grid against Cyber Attacks

[funded by DOE OE]
ISS - Overview

Main Challenge:
Provide security for new and legacy control systems currently used in the power grid without impacting operation.

Solution:
An integrated and distributed security system which overlays the power grid network and consists of three components: Manager, Switch, & Agent. Assessed, verified and validated by Idaho National Laboratory/NSTB.

Benefits:
• Allows asset owners to design a secure control system architecture.
• Enables the securing of legacy control system devices
• Provides centralized management, reporting, and in-band updates for a distributed solution.
Challenges in Smart Grid Communications

1. Typical Business Objectives
2. Connectivity
3. Protocols
4. Media
5. Quality of Service
6. Possible Cyber Attacks and Adverse Impacts
7. Security Requirements
Major challenges with new security solutions

1. Control System Security vs. IT Security
2. Many communication technologies
3. Legacy systems vs. new systems
4. Emerging requirements for smart grid
Design Principles of the ISS

1. Non-Intrusive
2. Scalable
3. Extendable
4. Inter-operable
# Introduction - ISS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Agent</th>
<th>Switch</th>
<th>Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography using OpenSSL*</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Access Control (AC) / Statefull Firewall</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Intrusion Detection (ID) based on control data pattern</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Traffic Shaping</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>- Traffic Differentiation</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>- Packet Scheduling</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Key Management</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Alarm Monitoring</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Configuring of the ISS network</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Security Policy Updates</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>AAA Server</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Deployment View

1) Security Agent as a stand alone device
2) Security Agent embedded into a device or application
3) Security Agent as stand alone protecting a group of devices
Deployment View

5) Security Agent embedded into the Security Switch. We assume that all connected devices are secure.

Benefits of the ISS

• Protects legacy control systems
• Meets Quality of Service requirements for control communication
• Protects against Denial of Service attack
• Independent of the underlying operating system
• Conforms to NERC CIP 005 and 007
• Designed to also protect SCADA systems outside of the Smart Grid (Oil & Gas Pipeline, etc)
1st on-site test was performed in July 2009

- 104 vulnerabilities were identified
- 19 were mitigated by the ISS
- 48 were partially mitigated by the ISS

2nd test was performed in December 2009