Security and the Smart Grid: Reducing Risk with Understanding

Jack Danahy
Security Executive
Office of the CTO
IBM Software Group/Rational

Co-author: The Smart Grid Security Blog
smartgridsecurity.blogspot.com

March 23, 2010
So **WHAT** is a Smart Grid?

A future power delivery grid that meets the needs of the next generation of Americans:

- Enable *active participation* by consumers
- *Accommodate* all generation and storage options
- *Enable* new products, services and markets
- *Provide power quality* for the range of needs in a digital economy
- *Optimize* asset utilization and operating efficiency
- *Anticipate and respond* to system disturbances in a *self-healing* manner
- *Operate resiliently* against physical and cyber attacks, and natural disasters

It is not a replacement grid, it is the existing grid made better, smarter, and more suited to today’s challenges
So **WHY** is a Smart Grid?

- **The Brittle Grid**
  - Grid element Interdependence produces cascading failures
- **Volatility in Energy**
  - Costs vary widely for generation fuels
  - Regional conflicts impact fuel price and supply
  - Political pressure to decrease reliance on foreign sources
- **Growing Environmental Impacts**
  - Carbon emissions facing public scrutiny and federal/international regulation
  - Increases in traditional generation facilities face local resistance
- **Customer Dissatisfaction**
  - Seeking information and flexibility
  - Creating opportunities for new services, revenue, and products

*img courtesy NOAA*
Requirements for Energy are Always Increasing

- Consumption has risen drastically
- Power quality has become an issue
- Power pricing has stabilized
- A majority of new technologies require substantial additional power
- Supporting point of connection services becomes more expensive with broader service areas
- There is no slackening of consumption in sight
A Smarter Grid IS Coming: Market Forces Demand It

- Regulatory & Policy Changes
- Expectations of Financials Markets
- Customer Expectations
- Technological Advancements
- Environment & Climate
- Security
- Volatile Energy / Fuel Costs
- Aging Assets & Workforce Dynamics

© 2010 IBM Corporation
Who wants what?

**Customers**
- Demand more information about use and efficiency
- Are more environmentally sensitized to energy use
- Want more control over usage rates and schedule
- Will generate power to sell back to the grid
- Demand involvement in the evolution of the grid

**Utilities**
- Must reduce the cost to serve and support customers
- Are driven to adapt to new technologies
- Must meet new expectations for services
- Seek to monetize deployment of new energy services
- Experiencing massive operations transformation

A Bidirectional Network

*A Smarter Infrastructure creates a new generation of *Prosumers*, producing and consuming energy in a balanced and equitable system to the benefit of customers and utilities alike*
Security Challenges from/for the New Smart Grid

- **Complexity**: As systems are added and increase functionality, security is more difficult to address.

- **Connectivity**: Increasing connection to previously isolated systems and networks expands the threat surface.

- **Internetworking**: Connections between networks permit more rapid spread of any corruption or breach.

- **Communications Dependency**: Reliance on networking technologies introduces new risk based on network stability.

- **Confidentiality**: Critical and sometimes private data drives the “smart” in Smart Grid, creating a new area of concern.
Where are specific areas of concern?

**System security**
- Vulnerable software
- Lack of access control
- Mis-configuration of options

**Data Vulnerability**
- Weak/No encryption
- Inappropriate storage
- Installation of malcode

**Potential Fraud**
- Invalid credentials
- Weak authorization
- Insufficient tamper protection

**Downtime**
- Denial of service risk
- System corruption
Thus there are multiple scenarios to plan for…

<table>
<thead>
<tr>
<th>External Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural disasters</td>
</tr>
<tr>
<td>Economic upheaval</td>
</tr>
<tr>
<td>Changing Political Climate</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Denial of service</td>
</tr>
<tr>
<td>Sophisticated, organized attacks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intentional Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undiscovered back doors</td>
</tr>
<tr>
<td>Information theft</td>
</tr>
<tr>
<td>Insider fraud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accidental Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpatched systems</td>
</tr>
<tr>
<td>Code vulnerability</td>
</tr>
<tr>
<td>Lack of change control</td>
</tr>
<tr>
<td>Human error or carelessness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Insider Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
Smart Meters and Advance Metering Infrastructure (AMI)

- Advanced Metering Infrastructure (AMI) includes hardware, software, communications, customer associated systems and meter data management (MDM) software.

- AMI Meters support two-way communications and conform to AMI standards.

- Securing the AMI means understanding:
  - Where and how are you using AMI?
  - What kinds of information and services are you sharing with partners and customers?
  - Which products and services companies are involved in this AMI implementation?
  - Have the components been tested for security?
  - Are you protected from eavesdropping and attack?

Img courtesy: http://seclab.uiuc.edu
Net Metering and Demand Management

- **Net Metering** refers to the “net” difference between the production and consumption of electrical power by an entity
  - Under net metering, system owners receive credit for the electricity they generate
- **Demand Management** refers to the proactive reduction of power demand during periods when energy-supply systems are constrained.
  - Reduces the need for additional power generation by shifting usage

- Securing Metering and Demand Management means understanding:
  - How will the systems be configured to comply with the expected reductions in service?
  - How have the management systems been secured against corruption or inadvertent reductions in power?
  - Who will be empowered to reduce available power?
And What of the Infrastructure?

- **Securing the Existing Environment**
  - Critical SCADA systems typically use proprietary protocols designed with little security functionality
  - Grid infrastructure must typically fail open (ON), as reliability and availability of power are most important
  - Systems rely on operations completing in deterministic time, and security brings overhead

- **Securing the Oncoming Surge**
  - Data volumes are expected to grow by orders of magnitude, and require levels of integrity and privacy
  - Connections and participants are no longer limited to internal/partner organizations
An Integrated View Avoids Buridan’s Dilemma

Smart Grid Security Must Evolve
- Reasonable effort in each relevant category
- Appropriate focus and investment according to risk and mandate
- Integration of technologies with personnel and partner capability
- Product adoption trails standards/practices articulation

Broad adoption awaits test of utility and reasonableness
<table>
<thead>
<tr>
<th><strong>Where to begin, a checklist.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attain visibility into organizational power strategy:</strong> Develop and maintain risk profiles and lists of potential and planned partners and technology acquisitions</td>
</tr>
<tr>
<td><strong>Manage Identities and Access:</strong> Create processes for ensuring appropriate access control to planned strategic energy management and monitoring systems</td>
</tr>
<tr>
<td><strong>Protect Data and Information:</strong> Ensure capability for granular protection of unstructured &amp; structured data, data leak prevention and acceptable use policy monitoring</td>
</tr>
<tr>
<td><strong>Control Software and Application Releases:</strong> Process for assuring security, efficiency and integrity of any custom or contracted software development</td>
</tr>
<tr>
<td><strong>Manage Change and Configuration:</strong> Mandate regular process for routine, emergency and out-of-band changes that will minimize or prevent operational outages</td>
</tr>
<tr>
<td><strong>Understand and Address Threats and Vulnerabilities:</strong> Continually monitor systems and expert resources to remain informed on protection for enterprise infrastructure for new and emerging threats</td>
</tr>
<tr>
<td><strong>Implement Security Information and Event Management:</strong> Automate the process of auditing, monitoring and reporting on security and compliance posture across the enterprise</td>
</tr>
<tr>
<td><strong>Manage Problems and Incidents:</strong> Designate responsibility and ownership for any issues in security, reliability, or power quality, and their investigation. Maintain trained event forensics team or create relationship with expert provider.</td>
</tr>
<tr>
<td><strong>Provide Security Training &amp; Ensure Awareness:</strong> Ensure awareness of security issues in power and power facilities by providing consistent training to end users and operators</td>
</tr>
</tbody>
</table>
Questions?

Jack Danahy
jack.danahy@us.ibm.com
smartgridsecurity.blogspot.com