Today’s Presenters

Jesse Berst
Host & Moderator - Founding Editor
SmartGridNews.com

Eric Trapp
Global Smart Grid Security Lead
Accenture

Robert Humphrey
Lead IT Security Consultant
Duke Energy
Housekeeping

You will receive a copy of the slides
  – To the email you used to register
  – Plus links to video “replays”

You can ask questions as we go along
  – Simply type into the question box, as we will explain

You will receive a FAQ with answers
  – If we are unable to get to all the questions
If this is what you see – Click on the orange arrow The Questions box will open up.

Use the Questions box at any time to type questions

We will pause periodically to answer questions

If we run out of time, we’ll answer by email as a FAQ

Yes, you will receive a copy of the slides
Key principles

1. Defense-in-depth
   Prevent, detect, defend and recover

2. Standardization
   Push to rationalize thoroughly vetted technologies

3. Governance
   Implement an explicit governance structure and instill a culture of security

4. Education
   Invest in training and awareness
Key principles

1. **Defense-in-depth**
   Prevent, detect, defend and recover

2. **Standardization**
   Push to rationalize thoroughly vetted technologies

3. **Governance**
   Implement an explicit governance structure and instill a culture of security

4. **Education**
   Invest in training and awareness
### Speaker

<table>
<thead>
<tr>
<th>Name</th>
<th>Background</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Trapp</td>
<td><strong>Senior Executive - Accenture Security</strong></td>
</tr>
<tr>
<td></td>
<td>• North America Lead – Resources industry - Security Practice.</td>
</tr>
<tr>
<td></td>
<td>• Implemented and managed IT process improvement in diverse environments, as well as IT strategic planning, security, disaster recovery and cost containment.</td>
</tr>
<tr>
<td></td>
<td>• Led the Infrastructure Transformation for one of the largest U.S. gas and electric utilities.</td>
</tr>
<tr>
<td></td>
<td>• Highly proficient in the state and federal regulations, including those recently adopted by industry peer/oversight groups and has earned the CISSP and CISM certifications.</td>
</tr>
</tbody>
</table>
Key principles

1. **Defense-in-depth**
   Prevent, detect, defend and recover

2. **Standardization**
   Push to rationalize thoroughly vetted technologies

3. **Governance**
   Implement an explicit governance structure and instill a culture of security

4. **Education**
   Invest in training and awareness

- Security architecture for the grid must be designed end-to-end, leveraging defense-in-depth and not bolted on as an afterthought.

- Besides architecture, utilities will have to pay closer attention to the security of their applications and HW via risk assessments.

- Identity and access management assumes greater importance.

- Utilities must not only react to suspicious activity but also failsafe, proactively gather cyber intelligence, and thorough penetration tests and vulnerability assessments.

- Enhanced situational awareness should include real-time network security performance indicators.
Security architecture for the grid should be “blanketed” and designed end-to-end
Risk assessments will influence the management and preservation of controls

Step 1: Gather inputs including leading Smart Grid Security Risk Assessment practices, standards, and responses to Security Assessment questionnaires.
- Historical Risks (BU)
- Legal (TD)
- IT (TD)
- Operations & Management (TD)
- QA (TD)
- Testing / Audit (TD)
- Regulatory (e.g. NIST 800-37, NIST 800-30, NISTIR 7628, NIST 800-53r3 NERC CIP, AMI-SEC, SOX) (TD)

Step 2: Request vendor vulnerability/defect management data from vendors and from Utility “symposiums/forums”.

Step 3: Conduct Vulnerability Assessment for legacy and new equipment.

Step 4: Assess new and legacy systems against Internal Security Requirements, regulations/standards (e.g. NISTIR 7628, NERC CIP, AMI-SEC)

Step 5: Conduct Penetration Testing for new and legacy hardware and software.


Step 7: Recommend Compensating Controls

Step 8: Sequence Mitigations

Step 9: Document Risk Assessment Results, including results of Vulnerability and Penetration Testing. Roadmap remediation in Operational, Technical, and Management areas.

Step 10: Implement and rigorously monitor Smart Grid Security Architecture, including:
- Security Information & Event Management (SIEM) Tools and Intrusion Prevention Tools e.g., HIDS, IDS, WIDS
- Compliance Management Solutions

I. UNFILTERED RISK DATA  II. FILTERED RISK DATA  III. RISK ASSESSMENT REPORT  IV. SECURE OPERATIONS
Key principles

1. **Defense-in-depth**
   Prevent, detect, defend and recover

2. **Standardization**
   Push to rationalize thoroughly vetted technologies

3. **Governance**
   Implement an explicit governance structure and instill a culture of security

4. **Education**
   Invest in training and awareness
2. Standardization: push to rationalize thoroughly vetted technologies

• Utilities must be diligent in assessing their deployments for points of risk by collaborating with each other and vendors.

• Vet the Smart Grid environment through vulnerability assessments and penetration tests.

• A prerequisite to make smart grids more secure is the interoperability of security controls and compliance with regulations.
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Background</strong></th>
</tr>
</thead>
</table>
| Robert Humphrey | **Lead IT Security Analyst at Duke Energy.**  
  • Primary security consultant to the Duke Energy Smart Grid Program  
  • 10+ years of information technology and information security experience.  
  • A veteran of the United States Army, previously held positions as a Network Administrator and Lead IT Auditor at Michigan State University.  
  • He holds a BS and MS from East Carolina University and is currently pursuing his MBA at Elon University. Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP). |
A robust environment is typically the result of verification, vulnerability, and penetration tests.

• Completely new architecture with end-points / network reaching out to customer homes
• Never before seen devices
• Validating vendor security statements
• Media coverage
• Regulators
• We owe it to our customers
Verification tests are a gap analysis against internal requirements and NISTIR 7628
Vulnerability and penetration tests have technical and programmatic nuances.

**Technical:**
- Will the output be used for design determinations?
- Will the output be used for influencing purchasing decisions?
- How will access control to the report be handled?
- How will the risk assessment be updated?
- How will defect management be handled e.g., information feed to vendors?

**Programmatic:**
- What is the scope of the risk assessment?
  - New equipment
  - Legacy equipment
  - Multiple vendors
- Where to begin?
- What is your approach?
  - White, Grey, Black Box
- What is the communication plan?
  - Walking gently
- Who is going to actually do the work?
  - Internal
  - External
Leveraging internal resources may result in a reduction of overall test costs...

**Internal Resources:**
- Some technology similar to standard pen testing
  - Linux
  - Wi-Fi
  - Can utilize familiar tools (i.e., Backtrack, Wireshark)
- Great experience for internal teams
- Inexpensive
- Might not have exposure to certain technologies (i.e., embedded systems, RF, cellular, electrical engineering)

**External Resources:**
- Everyone is a smart grid security expert
- New revenue stream for the big players
- Just my opinion - You get what you pay for
- Non-disclosure agreement
- Organizing the effort
- Getting internal people comfortable with a 3rd party
- Knowledge transfer to your internal teams

...however, external resources may increase test quality and reduce the test execution time.
There are many programmatic considerations for security testing

<table>
<thead>
<tr>
<th>Security Testing Options</th>
<th>Cost</th>
<th>Time to Complete</th>
<th>Quality</th>
<th>Internal Resources</th>
<th>External Resources</th>
<th>Density of Activities/Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Validation, Comprehensive External Vulnerability Assessment and Penetration Test</strong></td>
<td>$</td>
<td></td>
<td>QQ</td>
<td><img src="image" alt="internal resources" /></td>
<td><img src="image" alt="external resources" /></td>
<td>High</td>
</tr>
<tr>
<td><strong>Comprehensive External Validation, Vulnerability Assessment and Penetration Test</strong></td>
<td>$$</td>
<td></td>
<td>QQ</td>
<td><img src="image" alt="internal resources" /></td>
<td><img src="image" alt="external resources" /></td>
<td>Moderate</td>
</tr>
<tr>
<td><strong>Internal Validation, Phased External Vulnerability Assessment and Penetration Test</strong></td>
<td>$$$$</td>
<td></td>
<td>Q</td>
<td><img src="image" alt="internal resources" /></td>
<td><img src="image" alt="external resources" /></td>
<td>Moderate</td>
</tr>
<tr>
<td><strong>Phased External Validation, Vulnerability Assessment and Penetration Test</strong></td>
<td>$$$$</td>
<td></td>
<td>QQ</td>
<td><img src="image" alt="internal resources" /></td>
<td><img src="image" alt="external resources" /></td>
<td>Low</td>
</tr>
</tbody>
</table>

**Security Testing Lessons Learned**

1. Pre-production testing results may not be representative of a fully integrated production environment.
2. Vendors are not always forthcoming with loaning custom in house testing tools and security defect information.
3. Poor in house custom code quality is not abnormal so code testing is recommended.
4. Support gaps prevail when vendors and support staff are not proactively aligned.
5. Budget for device spares because security testing will result in broken equipment.
6. Balance the detail of testing instruction given to vendors with the creative freedom they need to “follow the bread crumbs”.
7. IT Controls do not equal physical and HW security, test all.
8. Lack of detail in an RFP leads to unnecessary lengthy.
9. Vendors NDA need to be in place with testers well in advance.
10. Test environment preparation— e.g., accounts, seating, spare devices, oscilloscopes, soldering irons, logic analyzers, network sniffing tools— need to be assigned. What will vendors supply? Testers? Utility?
Thank you!
More questions?

Jesse Berst  
Host & Moderator - Founding Editor  
SmartGridNews.com  
jesse.berst@globalsmartenergy.com

Robert Humphrey  
Lead IT Security Consultant  
Duke Energy  
robert.humphrey@duke-energy.com

Eric Trapp  
Senior Executive  
Accenture Security  
eric.g.trapp@accenture.com