Moving from conventional to real-time cyber security

November 8, 2010

Ken Van Meter
(610) 531 3177
Kenneth.d.van.meter@lmco.com
Addressing new risks in the Smart Grid

• Smart Grid deployments bring over 250 million of new hackable points within the next 5 years

• More interconnection with other entities

• Ability to do massive harm from a distance

• Harm can be persistent
  – Lack of spares for key components
  – Power control adds new risks

• Rapid and accurate threat information is not yet available

• Compliance uncertainties are forcing some utilities to make tough decisions
Conventional security is a life cycle process

### Security Risk Assessment
- Security Plan
- Current Security Environment Identification
- Identify & Assess Threats & Vulnerabilities
- Threat Modeling
- New or Modified Security Environment Identification
- Data/Info Criticality and Sensitivity
- C&A Criteria
- Baseline Focus Categories
- Policies, Processes, Standards, Laws, etc. Identification

### Secure Code Review
- Security Requirements
- Security Use Cases
- Security Misuse Cases
- Security Test Cases
- Evaluate Secure Solutions -> Input into COTS Selection
- Secure Coding Standards
- Secure Components
- Security built into Architecture Design

### Penetration Testing
- Secure Builds/Configuration
- Secure test plan/procedures/scenarios/cases Development
- Security Testing (vulnerability scans, penetration testing, web app scans)
- Discrepancy Report Mitigation
- Accreditation
- SRA Report
- Security Plans & Procedures

### Continuous Improvement
- CMMI, Six Sigma, Lean, Agile
- Functional Process/Procedures
- Metrics Collection/Analysis
Advance Persistent Threat (APT)

**Advanced**
- Well-coordinated
- Reconnaissance done on targets
- Work in teams

**Persistent**
- Campaign-scale attacks often span years

**Threat**
- Objectives: Exfiltrate sensitive data
- Do immediate or deferred harm to assets

Traditional view of cyber threats:
“To protect our infrastructure, we have to be right at every step; the bad guys only have to be right once.”

The new paradigm:
“To *compromise* our infrastructure, the bad guys have to be *right* at every step; we only have to be right once.”
Threat and Information Sharing overview

- Goal: Providing a collaboration portal for the collection of cyber threat information from multiple sources (including information partners and utility community experience) so utilities can more effectively identify threats and courses of action.

Smart Grid brings a new set of IT and cyber threats. Each utility user is likely to experience the same threats individually.

Utility User

Information Partners

Secure web portal that is built on Web 2.0 collaboration principles

Utility Users across America

Multiple Utility Users benefit from one user's experience and Information Partner information. They can implement Courses of Action against Threat A.

Threat A

Threat A is stopped

Threat A

Threat A

Threat A

Threat A
Cyber Attack Chain

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Act on Objectives

No matter where you block the sequence in the chain, you stop the attack.
Real time cyber security operations

- Lockheed Martin and AEP are building the first Cyber Security Operations Center (CSOC) today
- It will solve key issues in utility and grid security protection
- It will include Cyber as a Service (CaaS) capabilities for small and medium sized utilities that will deliver a high degree of protection for a low cost, and no capital outlays
CSOC system overview

CSOC

Real-Time
- Advanced Situational Awareness
- Data Correlation & Fusion
- Threat & Information Sharing

CSOC Integration

- Enterprise Wide Visualizations
- Courses of Action
- IT & Power System Correlation Rules
- Threat and Intelligence Collaboration Environment

Security Operations Center (SOC)
- Security Information Manager
- Security Event Monitoring Tools

Network Operations Center (NOC)
- Network Data Aggregation
- Network Configuration & Performance

Infrastructure Management
- Asset Health & Performance
- Asset SW/HW Configuration

Power Systems/“Smart” Infrastructure
- Power Event Aggregation
- Power Asset Monitoring Tools
The bottom line

• For regulatory purposes and for fundamental essential protection, the current and emerging standards and best practices for conventional cyber security are appropriate and must be followed

• Energy companies must engage in real time cyber security operations

• Energy companies must actively engage in threat and information sharing, but in a way that protects privacy of data and operational integrity

• A process must be implemented to ensure the secure and protected flow of threat and other data to and from key stakeholders, including government entities