UW EE 500E / ME 523 Energy and Environment Seminar: Cybersecurity for the Electric Grid

September 29, 2011

Paul Skare paul.skare@pnnl.gov
Chief Cyber Security Program Manager
Advanced Energy and Power Systems
Electric Infrastructure
Topics for today’s discussion

- Lifecycles
- Electric Control Systems Landscape
- Useful Guidance / Standards
- Trends
- References
Software Development Lifecycle
Secure Coding Guidelines must be pervasive

http://www.corporatewebbing.com/sdl/sdl.jpg
Typical Product Life Cycle Curve

The Largest Man-Made Machine:
North American Electric Power Grid
Components of Electric Power Infrastructure

- Generation
- Transmission
- Distribution
Substations
More than 4,700 generation plants in the U.S.
- 1,400 are greater than 100 MW and generate 95% of the electricity

More than 350,000 miles of transmission lines in the U.S.
- 159,000 miles are greater than 230 kV

More than 21,600 substations in the U.S.
- 4,500 are larger than 230 kV
Synchronous Interconnections

Regions of the North American Electric Reliability Corporation (NERC)
## Major North American Blackouts

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Load Interrupted</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 9, 1965</td>
<td>Northeast</td>
<td>20,000 MW</td>
</tr>
<tr>
<td>July 13, 1977</td>
<td>New York</td>
<td>6,000 MW</td>
</tr>
<tr>
<td>December 22, 1982</td>
<td>West Coast</td>
<td>12,350 MW</td>
</tr>
<tr>
<td>January 17, 1994</td>
<td>California</td>
<td>7,500 MW</td>
</tr>
<tr>
<td>December 14, 1994</td>
<td>Wyoming, Idaho</td>
<td>9,336 MW</td>
</tr>
<tr>
<td>July 2, 1996</td>
<td>Wyoming, Idaho</td>
<td>11,743 MW</td>
</tr>
<tr>
<td>August 10, 1996</td>
<td>Western Interconnection</td>
<td>30,489 MW</td>
</tr>
<tr>
<td>June 25, 1998</td>
<td>Midwest</td>
<td>950 MW</td>
</tr>
<tr>
<td>August 14, 2003</td>
<td>Northeast</td>
<td>61,800 MW</td>
</tr>
</tbody>
</table>
Key Cybersecurity Principles

Confidentiality

▶ “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]
▶ A loss of confidentiality is the unauthorized disclosure of information.

Integrity

▶ “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]
▶ A loss of integrity is the unauthorized modification or destruction of information.

Availability

▶ “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542]
▶ A loss of availability is the disruption of access to or use of information or an information system.

Security Impact Levels (FIPS 199)

▶ Confidentiality, integrity, and availability (CI&A) impact levels
▶ The unauthorized disclosure of information could be expected to have at
  ▶ Low: …limited adverse effect on organizational operations, organizational assets, or individuals.
  ▶ Moderate: …serious adverse effect on organizational operations, organizational assets, or individuals.
  ▶ High: …severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
ISO/IEC 27000 series of standards

- These documents include a very comprehensive view of cyber security.

ISO 27001
This is the specification for an information security management system

ISO 27002
This is the 27000 series standard number of what was originally the ISO 17799 standard

ISO 27003
This will be the official number of a new standard intended to offer guidance for the implementation of an IS Management System.

ISO 27004
This standard covers information security system management measurement and metrics, including suggested ISO 27002 aligned controls.

ISO 27005
This is the methodology independent ISO standard for information security risk management.

ISO 27006
This standard provides guidelines for the accreditation of organizations offering ISMS certification.
NISTIR 7628

Introduction to NISTIR 7628
Guidelines for
Smart Grid Cyber Security

The Smart Grid Interoperability Panel
Cyber Security Working Group

September 2010

Created by the Smart Grid Interoperability Panel – a public/private partnership

NIST Interagency Report 7628 outlines what the components of the Smart Grid are, and the cyber security concerns.

There are three parts to download as well as an executive Summary (Shown Here)
NISTIR Actors within Smart Grid Domains
NISTIR Bottom-Up Analysis

- 27 cyber security problems with specific relevance/uniqueness in Smart Grid
  - Authentication and Authorization
    - Users and Field Equipment
    - Maintenance personnel to meters
    - Consumers to meters, etc.
  - Non-secure firmware updates
    - How to ensure malware is not installed
  - Absolute and accurate time information
    - Used by many types of power system devices for different functions
  - Openness and accessibility of Smart Grid standards
    - Barrier to evaluation and use of standards
NISTIR Smart Grid Cryptography

► Problems
  ■ General constraining issues (e.g. CPU, bandwidth, etc.) found in Smart Grid systems and communications
  ■ General cryptography issues (e.g. entropy, cipher suites, key management, etc.) for Smart Grid
  ■ System specific issues

► Design Considerations and Solutions
  ■ General design considerations (e.g. technique selection, RNG, cryptography modules, etc.)
  ■ Key management systems for Smart Grid (e.g. PKI and symmetric systems)

► NISTIR high level security requirements
  ■ Cipher suite for Smart Grid
  ■ KMS (Key Management System) attributes and requirements for high-level requirements impact levels
CEDS/NSTB (OE10) Research Agenda

Original Roadmap 2006, updated 2011

- www.controlsystemsroadmap.net

Challenges:

- Address Roadmap with partnered research leading to commercial solutions
- Influencing Supply Chain
- Advanced Persistent Threat
  - Advanced – Operators behind the threat utilize the full spectrum of intelligence gathering techniques.
  - Persistent – Operators give priority to a specific task over time, rather than opportunistically seeking to achieve the defined objectives.
  - Threat – Means that operators have a specific objective and are skilled, motivated, organized and well funded.

“In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.”
Categorizing against taxonomies

**NERC CIP**

002 Identify 003 Management 004 Personnel Training 005 Perimeter 006 Physical 007 Systems 008 Incident Response 009 Recovery

**CISSP CBK**

Trends Impacting Control System Security

► **Open Protocols**
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols

► **General Purpose Computing Equipment and Software**
  - Standardized computational platforms increasingly used to support control system applications

► **Interconnected to Other Systems**
  - Connections with enterprise networks to obtain productivity improvements and information sharing

► **Reliance on External Communications**
  - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications

► **Increased Capability of Field Equipment**
  - “Smart” sensors and controls with enhanced capability and functionality
References

► **DOE Roadmap**
  - [http://www.controlsystemsroadmap.net](http://www.controlsystemsroadmap.net)

► **NISTIR 7628**
  - [http://csrc.nist.gov/publications/PubsNISTIRs.html](http://csrc.nist.gov/publications/PubsNISTIRs.html)

► **NERC CIP**
  - [http://www.nerc.com/page.php?cid=2%7C20](http://www.nerc.com/page.php?cid=2%7C20)