

P2030 TF1 Cyber Security Team

Conference Call
July 9th, 2009



Agenda

- Roll Call: We'll need your name and affiliation.
- IEEE Patent slide review
- Review of Previous Meeting Minutes (no previous meeting this time)
- Old business (none yet!)
- New business: (need note taker)
 - Security Reference Overview
 - Scope Discussion
 - How to get started discussion
- Next meeting plans
- Adjourn

Security Reference Overview

- Organizations
- Documents of Interest
- Key Definitions

Security Related Organizations

■ NIST

- National Institute of Standards and Technology. Primarily IT and communications security.

■ Common Criteria

- <http://www.commoncriteriaportal.org/index.html>
International in scope their work has become a number of ISO standards. Good for definitions and more details. Used in specification and evaluation of security of commercial IT/Networking products.

■ US-CERT

- United States Computer Emergency Readiness Team. Fairly IT oriented but good catalog of security “controls” http://www.us-cert.gov/control_systems/

■ Others?

Power Organizations with Security Specifications

- NERC
 - North American Electric Reliability Corporation. Primarily aimed at bulk power side of things.
- IEEE
 - Institute of Electrical and Electronic Engineers...
- OpenSG
 - Open Smart Grid...
- Others?

Key NIST Documents

- FIPS 199 (*Contains basic definitions*)
 - Standards for Security Categorization of Federal Information and Information Systems
- SP 800-53 Rev. 3
 - Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-82
 - ***Guide to Industrial Control Systems (ICS) Security***
- Smart Grid Roadmap June 2009
- Others?

Other Security Documents

■ Common Criteria

- ISO/IEC 15408
- These folks come up with standards for security assurance and certification of many types of information technology products.
- Example products types include: firewalls, authorization servers, network intrusion prevention systems, etc...

■ US-CERT

- A number of useful “catalogs” of threat controls.

IEEE and NERC

■ IEEE

- IEEE 1686-2007 IEEE Standard for **Substation** Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.
- IEEE Std C37.231™, IEEE Recommended Practice for Microprocessor-Based **Protection** Equipment Firmware Control.
- Others?

■ NERC

- “NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.”
- “These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are

Security Objectives (NIST FIPS-199)

■ Confidentiality

- “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” 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...” A loss of integrity is the unauthorized modification or destruction of information.

■ Availability

- “Ensuring timely and reliable access to and use of information...” A loss of availability is the disruption of access to or use of information or an information system.

Impacts of a breach (NIST FIPS 199)

■ Low

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Impacts of a breach (NIST FIPS 199)

■ Moderate

- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Impacts of a breach (NIST FIPS 199)

■ High

- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Scope Discussion

- From the NIST Cyber Security Roadmap:
 - In a typical risk management process, **assets, systems and networks are identified; risks are assessed (including vulnerabilities, impacts and threats); cyber security requirements are specified and cyber security controls are selected,** implemented, assessed for effectiveness, authorized, and then monitored over the lifecycle of the system. In contrast, the final product of this effort will be a set of recommended cyber security requirements that will be allocated to interfaces of the Smart Grid.

Scope: relations to other teams and TFs

- Other TF1 teams
 - Would we or they do threat and impact assessments?
- TF2 Communications
 - It seems that they would pick appropriate mechanisms to safeguard information in motion based on our impact assessments.
- TF3 Information Technology
 - Would they specify the various IT security mechanisms based on our impact assessments?

How to get moving?

- Summarize/categorize key relevant documents?
- Model documents for us to emulate? E.g. IEEE 1686-2007
- Start brain storming on threats and impacts of various parts of the grid that we are familiar? (load, distribution, transmission)
- Your idea goes here!

Closing

- Next Meeting Plans
 - Dates, Times, Length?
- Don't forget to check in with Greg if you missed the roll call.
- Thanks for your participation!