NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL
Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey08540-5731

TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – 2006

North American Electric Reliability Council
Control Systems Security Working Group

U.S. Department of Energy
National SCADA Test Bed Program

March 16, 2006

Preamble

This document addresses potential risks that can apply to some electricity sector organizations and provides practices that can help mitigate the risks. Each organization decides for itself the risk**s** it can accept and the practices it deems appropriate to manage those risk**s**.

Introduction

This reference document provides a non-prioritized list of the top 10 most common and threatening vulnerabilities to control systems in the Electric Sector based on the combined expertise of the NERC Control System Security Working Group (CSSWG) members. This list is prepared by the CSSWG and updated annually. Asset owners are encouraged to use this list to augment their risk management processes.

The U.S. Department of Energy National SCADA Test Bed (NSTB) program has provided initial recommended mitigation strategies to the list of vulnerabilities prepared by the CSSWG members. Three levels of mitigation strategies are proposed – ***foundational***, ***intermediate***, and ***advanced***. ***Foundational*** strategies are considered to be minimal mitigation strategies typically involving the establishment of security policy and fundamental implementations. ***Intermediate*** strategies are a next step in establishing a secure posture and involve readily available technologies or the stronger implementation of baseline policies. ***Advanced*** mitigation strategies provide long term achievable security posture guidance but may include tools or technologies that are currently not readily available.

Top 10 Vulnerabilities of Control Systems and Potential Mitigation Strategies

1. Inadequate Policies, Procedures, and Culture Governing Control System Security.

Mitigation Strategies:

- Foundational
  - Assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, standards (CIP-002 through CIP-009). (CIP-003-1 R2)
  - Develop and implement policies and procedures with executive-level buy-in, including the NERC critical infrastructure protection standards, which govern control system security.
  - Document and implement a cyber security policy that represents management's commitment and ability to secure its critical infrastructure assets.
  - Provide basic security awareness training for all employees. (CIP-004 R1 & R2)
- Intermediate
  - Have senior manager provide periodic briefings to executive management detailing control system risk posture.
  - Share industry "best practices" in security-policy structure and topics.
  - Provide periodic computer-based, control system cyber security training for all control systems personnel.
  - Provide social engineering awareness training for all employees.
- Advanced
  - Adopt a process for continuous improvement for implementation and enforcement of policies and procedures governing control system security.
  - Provide periodic hands-on cyber security training for control systems personnel taught by applicable vendor or consulting firm.
  - Perform periodic security-awareness drills and audits.

2. Inadequately Designed Control System Networks That Lack Sufficient Defense-In-Depth Mechanisms.

Mitigation Strategies:

- Foundational
  - Control system stakeholders and designers request security solutions from vendors.
  - Include detailed security requirements in all design specifications.

    - Implement electronic perimeters. Disconnect all unnecessary network connections, following the NERC security guideline “Control System — Business Network Electronic Connectivity Guideline” (also addressed in NERC CIP-005).
    - Access controls can be considered part of an organization’s defense-in-depth solution. (CIP-005 R2, CIP-007 R5)
- Intermediate
    - Reference existing standards and best practices as requirements in design specification.
    - Implement concentric electronic perimeters. Use autonomous networks with minimal shared resources between control system and non-control system networks.
    - Distribute the organization’s practices and guidelines to employees, vendors, and integrators as part of training and refresh cycle.
- Advanced
    - Design specifications include comprehensive security standard references providing in-depth security coverage.
    - Implement virtual local area networks (VLANs), private VLANs, intrusion prevention, anomaly detection, smart switches, secure dial-up access, etc.
    - Place security software on end devices.

3. Remote Access to the Control System without Appropriate Access Control.

Mitigation Strategies:

- Foundational
    - Develop and implement policy for managing user access.
    - Implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). (CIP 002-009)
    - Maintain complete and current maps of system topology. Identify and track up-to-date status for all access points.
    - Perform background personnel checks on employees with access to sensitive systems. Ensure vendors and contractors have implemented similar procedures. (CIP-004 R3)
    - Establish a policy for system access including password authentication. (CIP-005 R5)
    - Change all default passwords where possible. (CIP-005 R4)
    - Do not allow unsecured modems.
    - Use VPN technology when the Internet is used for sensitive communications.

    - Follow the NERC security guideline called Securing Remote Access to Electronic Control and Protection Systems. (CIP-005)
- Intermediate
    - Define levels of access based on need. (CIP-007) Assign access level and unique identifiers for each operator. (Implied by CIP-007) Log system access at all levels. (CIP-007) Implement a network-intrusion detection system to identify malicious network traffic, scan systems for weak passwords, and separate networks physically. (Partially covered in CIP-007)
    - Make contractual agreements for vendor access to control system components a requirement in RFPs.
    - Isolate user access to compartmentalized areas based on specific user needs.
- Advanced
    - Automated removal of user accounts tied to badge systems or human resources employee termination.
    - Design access levels into the system that restrict access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms. Use multifactor authentication (e.g., two-factor, non-re-playable credentials). Implement protocol anomaly-detection and active-response technology.

4. Auditable System Administration Mechanisms (System Updates, User Metrics, etc.) are Not Part of Control System Implementation.

Mitigation Strategies:

- Foundational
    - Perform periodic configuration auditing and backup.
    - Create and annually review recovery plan(s) for critical cyber assets.
    - Establish required metric for vendor update support of security patches as part of RFP. Maintain a maintenance agreement with software vendors for update notification and distribution. Define change-management process. (CIP-003)
- Intermediate
    - Maintain the development system for testing system updates prior to operational system deployment when appropriate.
    - Establish a schedule of checks for system updates for all applicable software, operating systems, and component firmware. Implement version control system and enforce change-management process. (CIP-007)

- Advanced
    - Phase out legacy systems that cannot support security requirements.
    - Utilize a dual-redundant or clustered-system architecture that allows for re-bootable updates without requiring system downtime. Security scan resources to ensure security patches are installed. (Caution: procedures should be developed to ensure online control systems are not compromised as a result of the scan).

5. Inadequately Secured Wireless Communication.

Mitigation Strategies:

- Foundational
    - Perform periodic risk assessment of all wireless implementations, including Denial of Service.
    - Treat all wireless connections as remote access points.
    - Establish a policy on where wireless may be used in the system.
    - Implement encrypted wireless communication where possible (e.g., wired equivalent privacy [WEP]).
- Intermediate
    - Authenticated control signals.
    - Implement 802.1x device registration.
- Advanced
    - For 802.11:
        - ▪ Implement wireless fidelity protected access (WPA) encryption.
        - ▪ Use non-broadcasting server set identifications (SSIDs).
    - Implement 802.11i.
    - Use public key infrastructure (PKI) and certificate servers.
    - Utilize media access control (MAC) address restrictions.
    - Implement 802.1x device registration along with unregistered device detection.

6. Use of a Non-Dedicated Communications Channel for Command and Control, such as Internet Based SCADA, and/or Inappropriate Use of Control System Network Bandwidth for Non-Control Purposes (e.g., VOIP).

Mitigation Strategies:

- Foundational
    - Define critical network paths. (CIP-003)
    - Restrict or eliminate non-critical traffic on the control network and ensure quality of service for all control system traffic.
    - Segregate functionality onto separate networks (e.g., do not combine e-mail with control system networks).

- Intermediate
    - Implement intrusion detection to monitor traffic. Evaluate network traffic and control system point counts and polling rates. Reconfigure for optimal use of existing resources.
- Advanced
    - Update system technology to allow for higher-bandwidth traffic. Separate critical and non-critical systems. Implement protocol anomaly systems to enforce legitimate traffic.

7. Lack of Quick and Easy Tools to Detect And Report on Anomalous or Inappropriate Activity. Inadequate or Non-Existent Forensic and Audit Methods.

Mitigation Strategies:

- Foundational
    - Audit network traffic periodically against policy. Regularly audit system logs, where available.
    - Time-synchronize system logs and sequence-of-events recorders with GPS clocks or network time protocol (NTP).
    - Install monitoring technology to log all existing and potential points of entry into the system. Preserve logs for subsequent analysis.
- Intermediate
    - Implement technologies to enforce legitimate traffic.
    - Install anomaly detection where available. Actively monitor logs.
- Advanced
    - Implement tamper-resistant or tamper-proof long term storage for all forensic data.
    - Introduce SCADA/Control System protocol signatures when they become available.
    - Work with vendors to develop tools to identify inappropriate control systems traffic.

8. Installation of Inappropriate Applications on Critical Control System Host Computers.

Mitigation Strategies:

- Foundational
    - Develop policy that will provide guidance for allowable applications and their introduction onto the SCADA/Control System LAN. (CIP-005)
    - Conduct inventory. Ensure sufficient training of personnel responsible for component configuration and maintenance.
- Intermediate
    - Implement mal-ware detection. (CIP-007)

- Advanced
    - Use anomaly detection to uncover inappropriate applications.
    - Develop application baseline profile for each workstation and server on control network. Configure intrusion-detection filters to identify and log baseline violations.

9. Software Used in Control Systems is Not Adequately Scrutinized.

Mitigation Strategies:

- Foundational
    - Develop and implement software lifecycle policy. The policy identifies how new software is acquired, including the purchasing and review process, how updates are managed, and how antiquated software is retired.
    - Require risk assessment and software quality control on new and existing systems.
- Intermediate
    - Evaluate and characterize applications. Remove or disconnect unnecessary functions.
    - Evaluate the patch-management process, including hardware, firmware, and software, following the NERC security guideline "Patch Management for Control Systems."
    - Maintain full system backups and have procedures in place for rapid deployment and recovery. Maintain a working test platform and procedures for evaluation of updates prior to system deployment.
    - Build security into applications during system design to include the ability to validate new code releases and to authenticate the code source.
- Advanced
    - Review source code and development tools.
    - Perform systematic search for additional vulnerabilities.

10. Control Systems Command and Control Data Not Authenticated.

Mitigation Strategies:

- Foundational
    - Limit connections and isolate control systems communications and networking infrastructure.
    - Identify the different types of SCADA/Control Systems. Determine which data sets need to be authenticated and protected for integrity.
- Intermediate
    - Assure basic data authentication/integrity.

    - Develop and implement, where possible, key management policies and systems based on an agreed set of standards, procedures, and secure methods for all issues (e.g., usage, storage, revocation, logging, auditing, etc.) associated with use of keys.
- Advanced
    - Authenticate and validate control system communication with integrity protection.
    - Utilize SCADA/Control Systems protocols that contain authentication and integrity attributes.