TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – 2007

North American Electric Reliability Corporation
Control Systems Security Working Group

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

March 22, 2007

Preamble

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

Introduction

This reference document provides a non-prioritized list of the top 10 most common vulnerabilities that put control systems in the electricity sector at risk. The list is based on the combined expertise of the NERC Control System Security Working Group (CSSWG). The CSSWG updates the list annually based on changes in industry implementation or available technology. 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.

This year's list also includes explanatory examples for each vulnerability to clarify the intent of the CSSWG; in some cases ***cautionary notes*** are also provided where appropriate. However, in all cases the reader is reminded that technology should always be designed and tested for the specific control system environment where they are intended to be deployed to properly consider safety and operational considerations.

Top 10 Vulnerabilities of Control Systems

1. Inadequate policies, procedures, and culture that govern control system security.

- Clash between operational culture with modern IT security methods.
- Lack of overall awareness and appreciation of the risk associated with enabling the networking of these customized control systems.
- Absence of control system information security policy.
- Lack of auditing, enforcing, or adhering to control system information security policy not adhered to, enforced or audited.
- Lack of adequate risk assessment

Mitigation Strategies

Foundational

- Assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, robust control system security practices.
- Document and implement a cyber security policy that represents management's commitment and ability to secure its critical infrastructure assets. Periodically review and update.
- Develop security procedures and implementation guidance to enable employees to implement specific elements of the cyber security policy.
- Develop a risk management plan that identifies and documents a risk-based assessment methodology to identify its critical assets. Periodically review and update as necessary (particularly when operational changes result in new critical assets).
- Provide security awareness training for all employees.
- Provide adequate employee training based on task function.

Intermediate

- Ensure policies and procedures comprehensively include other parts of the enterprise, vendors, or contractors as appropriate.
- Form a teaming arrangement between information technology and control system operations staff to facilitate effective knowledge sharing.
- Provide briefings to executive management detailing control system risk posture.
- Share industry "best practices" in security-policy structure and topics.

Advanced

- Develop and implement a process for continuous improvement 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.
- Include security-related roles, responsibilities, authorities, and accountabilities in staff annual review and appraisal processes.
- Coherent and meaningful policies are understood and internalized by all employees so that they are continually working to achieve these goals as part of their daily task activities.

2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.

- Network security of control system devices were not adequately considered when originally designed. These systems were designed with availability and reliability in mind.
- Control systems may not be capable of secure operation in an internet worked environment without significant investment to reengineer the technology so it is in accordance with appropriate risk assessment criteria.

Mitigation Strategies:

Foundational

- Develop and periodically update a list of critical assets determined through an annual application of a risk-based assessment methodology.
- Implement electronic perimeters. Disconnect all unnecessary network connections, following the NERC security guideline "Control System — Business Network Electronic Connectivity Guideline"
- Implement strong procedural or technical controls at the access points to the electronic security perimeter to ensure authenticity of the accessing party, where feasible (e.g., restrict remote access to field devices).
- Include detailed security requirements in all design specifications.

Intermediate

- Implement compartmentalization design concepts to establish electronic security perimeters and cyber asset separation necessary for a defense-in-depth architecture.
- Use special purpose networks with minimal shared resources to transfer data between control system and non-control system networks.
- Replace devices as necessary to attain desired security functionality, or implement compensating security measures if replacement is not feasible.

Advanced

- Design specifications include comprehensive security standard references providing in-depth security coverage.
- Implement virtual local area networks (VLANs), private VLANs, intrusion prevention, intrusion detection, smart switches; secure dial-up access, etc.
- Implement host based protection in conjunction with network based protection.
- Implement physical security of network access points, including access control, or electronic methods for restricting access (e.g., MAC address filtering).

3. Remote access to the control system without appropriate access control.

- Inappropriate use of dial-up modems.
- Use of commonly known passwords or no use of passwords.
- Implementation of non-secure control system connectivity to the corporate Local Area Network (LAN).
- Practice of un-auditable and non-secured access by vendors for support.

Mitigation Strategies

Foundational

- 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).
- Maintain complete and current maps of control 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.
- Develop and implement policy for managing user and system access, including password policies.
- Change all default passwords where possible.
- Do not allow unauthenticated remote access to the control system.
- Use secure communication technology when the Internet is used for sensitive communications (e.g., VPN, SSH, SSL, IPSEC).
- External connections should be controlled and secured with an authentication method, firewall, or physical disconnection when not in use. This secure method should be established and monitored in accordance with the established security policy and procedures.
- Follow the NERC security guideline "Securing Remote Access to Electronic Control and Protection Systems".

Intermediate

- Define levels of access based on roles or work requirements. Assign access level and unique identifiers for each operator. Isolate user access to compartmentalized areas based on specific user needs. Log system access at all levels.
- Use multifactor authentication (e.g., two-factor, non-re-playable credentials).
- Implement a procedure whereby remote access to the control system must be enabled by appropriately authorized personnel.
- Perform regular audits of remote access methods.
- Periodically perform a passive network mapping and/or conduct war dialing to find undocumented external connections.
- Implement a network-intrusion detection system to identify malicious network traffic, scan systems for weak passwords, and separate networks physically.
- Include security access issues in contractual agreements with vendors or contractors.

Advanced

- Design access levels into the system that restricts access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms.
- Use proximity based authentication technology, such as RFID Tokens.
- Implement protocol intrusion detection and active response technology.

Cautionary note:

- The use of active response technology systems should be carefully considered. The technology should be engineered for application in a control system environment where

failsafe modes have been adequately considered for safety and operational considerations.

4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.

- Inadequate patch management.
- Lack of appropriately applied real time virus protection.
- Inadequate account management.
- Inadequate change control.
- Inadequate software inventory.

Mitigation Strategies

Foundational

- Inventory all software and hardware used in the control system.
- Develop and implement hardware and software quality assurance policy, including purchase, maintenance, and retirement, particularly how sensitive information is removed before reapplication or disposal.
- Establish a robust patch-management process, including tracking, evaluating, testing and installing applicable cyber security patches for hardware, firmware, and software, following the NERC security guideline "Patch Management for Control Systems."
- Document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures on a periodic basis.
- Periodically review authorization rights and access privileges to ensure consistency with job function.
- Revoke authorization rights and access privileges of users upon termination or transfer.
- Remove, disable, or rename administrator, shared and other generic account privileges including factory default accounts where possible.

Intermediate

- Evaluate and characterize applications. Remove or disconnect unnecessary functions.
- 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.
- Work with vendors to include the ability to validate the integrity of new code releases.
- Use screening technology at network entry points to prohibit the spread of malware.
- Establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity.

Advanced

- Automated removal of user accounts tied to badge systems or human resources upon employee termination.
- Work with vendors to develop and implement a formal software assurance process to verify proper functionality through testing, certification, and accreditation processes.
- Perform systematic vulnerability testing.
- Limit user accounts with administrative or root privileges when practical.

- Limit shared accounts to the extent practicable, except when necessary for safety or operational considerations.

5. Use of inadequately secured WiFi wireless communication for control.

- Use of commercial off-the-shelf (COTS) consumer-grade wireless devices for control network data.
- Use of outdated or deprecated security/encryption methods.

Mitigation Strategies

Foundational

- Perform periodic risk assessment of all wireless implementations, including denial of service considerations.
- Treat all wireless connections as remote access points. Document and implement a program for managing access to sensitive systems.
- Establish a security policy on where and how wireless may be used in the control system. For example, use of wireless for critical control applications should be discouraged.
- Implement encrypted wireless communication where possible, e.g., 802.11i WiFi Protected Access 2 (WPA2).
- Use non-broadcast server set identifications (SSIDs).
- Treat all routable protocol wireless connections as non-private communication paths.
- Implement procedure for disabling WiFi-capable equipment when it is connected to critical networks when wireless use is not intended, including laptops being introduced in control center environments or substations.

Intermediate

- Implement 802.1x device registration.
- Utilize media access control (MAC) address restrictions.
- Perform wireless signal detection survey to identify the boundaries of wireless perimeter.
- Use directional antenna design when possible.
- Implement technology to discover rogue wireless access points and devices for all wireless network types.

Advanced

- For 802.11: Implement wireless fidelity protected access (802.11i or WPA2) encryption with a RADIUS server.
- Implement 802.1x device registration along with unregistered device detection.
- Encrypt network traffic over wireless networks at the network, transport or application layer (e.g., IPSEC, TLS).
- Conduct RF mapping of wireless environment (e.g., characterize directional antenna side lobes).

6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes.

- Internet based Supervisory Control And Data Acquisition (SCADA)
- Inappropriate use of control channels for non-control data.
  - Asset management
  - Power quality data files
  - Metering
  - Maintenance
- Internet/Intranet connectivity initiated from control system networks.
  - E-mail
  - Web browsing
  - File Sharing
  - Instant Messaging

Mitigation Strategies
Foundational

- Develop and implement a policy that addresses applications and protocols introduced to a control system. Minimizing non-control system traffic reduces noise, enhancing effectiveness of security measures.
- 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 strong procedural or technical controls at all access points to the control system to ensure authenticity of the accessing party, where technically feasible.
- 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

- Implement protocol anomaly systems to enforce legitimate traffic.

7. Insufficient application of tools to detect and report on anomalous or inappropriate activity.

- Underutilized intrusion detection systems
- Under-managed network system
- Implementation of immature Intrusion Prevention Systems

Mitigation Strategies
Foundational

- Develop and implement network and system management capability to monitor network traffic.
- Regularly audit system logs, where available.
- Characterize normal traffic patterns.
- Timestamp system logs for event correlation.
- Preserve system logs for subsequent analysis.

Intermediate

- Install anomaly detection where available.
- Implement technologies to enforce legitimate traffic.
- Time-synchronize system logs and sequence-of-events recorders with GPS clocks or network time protocol (NTP).

Advanced

- Implement tamper-resistant or tamper-proof long term storage for all forensic data.
- Introduce control system protocol signatures when they become available.
- Work with vendors to develop tools to identify inappropriate control systems traffic.
- Implement technology to conduct automatic correlation of system logs for anomalous events.
- When practical, implement self-healing systems (e.g., protected operating systems).

Cautionary notes

- The use of active response intrusion prevention systems should be carefully considered. The technology should be engineered for application in a control system environment where failsafe modes have been adequately considered for safety and operational considerations.
- Intrusion detection will not encompass all vulnerabilities.

8. Unauthorized or inappropriate applications or devices on control system networks.

- Unauthorized installation of additional software to control system devices.
- Peripherals with non-control system interfaces, e.g., multi function or multi-network printers.
- Non-secure web interfaces for control system devices.
- Laptops.
- USB memory.
- Other portable devices e.g., personal digital assistants (PDAs).

Mitigation Strategies

Foundational

- Develop policy that will provide guidance for allowable applications and devices within the control system environment.
- Develop policy and procedures for change management.
- Develop and implement a hardware inventory tracking process.
- Ensure sufficient security awareness training of personnel responsible for component configuration and maintenance.
- Establish policy and procedures to implement strong procedural or technical controls at the access points into the control system for all devices to ensure authenticity of the accessing party, where technically feasible.
- Limit physical and electronic access to devices based upon organizational roles.
- Beware of automatic software shutdown mechanisms in critical systems (e.g., processes that enforce software licenses).

Intermediate

- Use intrusion detection to uncover inappropriate applications or devices.
- Implement malware detection.
- Develop and implement a policy regarding the use of removable media.
- Disable all unnecessary input/output ports on all devices.

Advanced

- Develop application baseline profile for each workstation and server on control network. Configure intrusion detection filters to identify and log baseline violations.

9. Control systems command and control data not authenticated.

- Authentication for LAN-based control commands not implemented.
- Immature technology for authenticated serial communications to field devices.

Mitigation Strategies
Foundational

- Limit connections and isolate control systems communications and networking infrastructure.
- Determine data authentication and integrity requirements.

Intermediate

- 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) associated with use of keys.

Advanced

- Use control system protocols that contain appropriate authentication and integrity attributes without affecting performance as the technology becomes available.

10. Inadequately managed, designed, or implemented critical support infrastructure

- Inadequate uninterruptible power supply (UPS) or other power supply systems.
- Inadequate or malfunctioning heating / ventilation / air conditioning (HVAC) systems.
- Poorly defined “6-wall” boundary infrastructure.
- Insufficiently protected telecommunications infrastructure.
- Inadequate or malfunctioning fire suppression systems.
- Lack of recovery plan.
- Insufficient testing or maintenance of redundant infrastructure.

Mitigation Strategies
Foundational

- Evaluate critical support infrastructures currently in place to determine adequacy and identify gaps.
- Include critical support infrastructure functionality in continuity of operation planning. Periodically exercise and test recovery plans.
- Adhere to regular maintenance and test procedures for critical support infrastructure systems.

Intermediate

- Establish and implement policies and procedures to comprehensively test critical support infrastructures, and periodically exercise test plan. Develop process for identifying and resolving gaps that are revealed through testing.

Advanced

- Implement mitigations to address gaps as indicated by analysis, audits, or testing to achieve acceptable levels of reliability/redundancy.
- Identify and test interdependencies between key systems and subsystems.