

Potential Mitigation Strategies for the Common Vulnerabilities of Control Systems Identified by the NERC Control Systems Security Working Group (CSSWG)

Submitted on behalf of the DOE National SCADA Test Bed

by

Jeff Dagle, PE
Pacific Northwest National Laboratory
(509) 375-3629
jeff.dagle@pnl.gov

Discussion draft, November 17, 2005

Preface

- The following mitigation strategies may be applicable to some electricity sector organizations and not applicable to others.
- Each organization must determine the risk it can accept and the practices it deems appropriate to mitigate vulnerabilities.
- If an organization can not apply some of the technology suggested here, then other strategies should be applied to mitigate the associated vulnerability.

1. Inadequate policies and procedures governing control system security.

- Foundational

- Implement policies and procedures governing control system security. (ref: NERC CIP Standards)

- Intermediate

- Share industry best practices in security policy structure and topics.
- Enforce policies and procedures governing control system security.

- Advanced

- Adopt a process for continuous improvement for implementation and enforcement of policies and procedures governing control system security.

2. Poorly designed Control System Networks that 1) fail to compartmentalize communication connectivity with corporate networks and other entities outside of the Control System electronic security perimeter; 2) fail to employ sufficient “defense in depth” mechanisms; 3) fail to restrict “trusted access” to the control system network; and 4) rely on “security through obscurity” as a security mechanism.

- **Foundational**

- Implement electronic perimeters. Disconnect all unnecessary network connections. (ref: Control System — Business Network Electronic Connectivity Guideline)

- **Intermediate**

- Implement concentric electronic perimeters. Use autonomous networks with minimal shared resources between control system and non-control system networks.
- Training: supply company’s best practices and guidelines to new employees, vendors, integrators.

- **Advanced**

- Implement virtual LANs, private VLANs, intrusion prevention, anomaly detection, smart switches, etc.

3. Misconfigured operating systems and embedded devices that allow unused features and functions to be exploited. Untimely implementation of software and firmware patches. Inadequate testing of patches prior to implementation.

- Foundational
 - Conduct inventory. Ensure sufficient training of personnel responsible for component configuration and maintenance.
- Intermediate
 - Evaluate and characterize applications. Remove or disconnect unnecessary functions.
 - Patch management process: Hardware, firmware, software. 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. (ref: Patch Management Guideline)
- Advanced
 - Active vulnerability scans. (Caution: recommend use of development system so that on-line control systems are not compromised during the scan.) Disable, remove, or protect unneeded or unused services/features that are vulnerable.

4. Use of inappropriate wireless communication. Lack of authentication in the 802.11 series of wireless communication protocols. Use of unsecured wireless communication for control system networks.

- Foundational

- Establish a policy on where wireless may be used in the system.
- Implement WEP.

- Intermediate

- Implement 802.1x device registration.

- Advanced

- Implement WPA encryption and 802.1x device registration along with unregistered device detection.
- Use PKI and certificate servers
- Use non-broadcasting SSIDs
- Utilize MAC address restrictions
- Implement 802.11i

5. Use of non-deterministic communication for command and control such as Internet based SCADA. Inadequate authentication of Control System communication protocol traffic.

- Foundational
 - Implement defense in depth architecture (e.g., multiple firewalls between control network and other networks).
- Intermediate
 - Implement technologies to enforce legitimate traffic.
- Advanced
 - Authenticate and validate control system communication.

6. Lack of mechanisms to detect and restrict administrative/maintenance access to control system components. Inadequate identification and control of modems installed to facilitate remote access. Poor Password standards and maintenance practices. Limited use of VPN configurations in control system networks.

- Foundational

- Perform background personnel checks on employees with access to sensitive systems. Ensure vendors and contractors have implemented similar procedures.
- Establish a policy for system access including password authentication. Change all default passwords. Do not allow unsecured modems.
- Use VPN technology when the Internet is used for sensitive communications.
- Ref: Securing Remote Access to Electronic Control and Protection Systems Guideline

- Intermediate

- Define levels of access based on need. Assign access level and unique identifiers for each operator. Log system access at all levels. Implement network IDS to identify malicious network traffic, scan systems for weak passwords, separate networks physically.

- Advanced

- Design access levels into the system restricting access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms. Use multi-factor authentication (e.g., two-factor, non-replayable credentials). Implement protocol anomaly detection and active response technology.

7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity among the volumes of appropriate control system traffic.

- Foundational

- Install monitoring technology, e.g., Intrusion Detection System (IDS) to log all existing and potential points of entry into the system. Preserve logs for subsequent analysis.

- Intermediate

- Install anomaly detection, actively monitor logs.

- Advanced

- Work with vendors to develop appropriate tools to identify inappropriate control systems traffic.

8. Dual use of critical control system low band width network paths for non-critical traffic or unauthorized traffic.

- **Foundational**
 - Define critical network paths.
 - Restrict or eliminate non-critical traffic on the control network.
 - Segregate functionality onto separate networks (e.g., do not combine email with control system networks).
- **Intermediate**
 - Implement IDS 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 and active response systems to enforce legitimate traffic.

9. Lack of appropriate boundary checks in control systems that could lead to “buffer overflow” failures in the control system software itself.

- Foundational
 - Actively monitor server status.
- Intermediate
 - Implement processes to automatically stop and restart services.
- Advanced
 - Enforce vendors' software development standards that incorporate secure software development techniques.

10. Lack of appropriate change management/change control on control system software and patches.

- Foundational

- Maintain a maintenance agreement with software vendors for update notification and distribution. Define change management process.

- Intermediate

- 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.

- Advanced

- Utilize a dual redundant or clustered system architecture that allows for rebootable updates without requiring system downtime. Actively scan resources to ensure security patches are installed. (Caution: procedures should be developed that will ensure on-line control systems are not compromised as a result of the scan.)