

Top Ten Vulnerabilities of Control Systems

September 7, 2004, version

The following is a list of the top ten most common and threatening vulnerabilities to control systems. This list should be reviewed and updated periodically. Asset owners are encouraged to use this list in their risk management process to ensure that at a minimum they are addressing these types of vulnerabilities.

1. **Architectural Design Flaws** — poorly designed control networks that
 - a. fail to compartmentalize communication with the corporate network and other entities outside of the Control System;
 - b. fail to employ sufficient “defense in depth” mechanisms;
 - c. fail to restrict “trusted access” to the control network;
 - d. Excessively rely on “security through obscurity” as a defensive mechanism.
2. **Configuration Flaws** — Lack of understanding of proper control system configurations including configurations of embedded system devices. This lack of understanding contributes to the misconfiguration of operating parameters, and delays in implementation of software and firmware patches due to concerns of the unintended effects on operations. This requires the extensive testing of patches prior to implementation and may result in patches not being applied due to these unintended effects.
3. **Communication flaws** — Communication protocols were never designed with security in mind and therefore the protocols themselves typically lack any form of authentication. Hence if an adversary can gain access to the appropriate communication channel the control system devices will accept any command given in that protocol.
4. **Communication flaws** — Use of inappropriate wireless communication. Lack of authentication in the 802.11 series of wireless communication protocols, along with an unfixable fundamental flaw that allows a Denial of Service (DOS) make the 802.11 series of protocols unsuitable for control system communications. Lack of authentication and security in other wireless communication mechanisms increase the risk of an adversary gaining access to the communication channel. Use of unsecured wireless communication for control networks should be avoided.
5. **Communication flaws** — Use of non-deterministic communications for command and control, in particular internet based SCADA. The non-deterministic part means that you can not guarantee delivery, or in most cases the path taken by the communications. This increases the risk of critical control system communications failure. The use of the internet increases that risk, as it is a very adversary friendly environment, and attacks against other entities could greatly impact any control communications that uses this path or shares resources that touch the internet. For example, the slammer worm had a negative impact on a control communications channel due to a shared resource (router) that had control channels as well as internet channels.
6. **Access flaws** — Lack of defensive mechanisms to restrict administrative/maintenance access to control system components. Lack of control of Out of Band access (i.e., modems) in some cases installed by vendors (or others) to facilitate remote access without notifying security of these connections. Poor password capabilities — the device contains no passwords, default passwords, or only allows weak passwords (insufficient character sets and short length) and may not allow the owner of the device to change the passwords. Limited use of Virtual Private Network (VPN) in control systems due to key management and other maintenance issues (one

concern is that an incorrectly configured VPN or one in which the operator forgets how to properly operate could cause a DOS to the affected device).

7. **Forensic flaws** — Most control systems lack the capability to easily analyze data to determine if an intrusion has occurred. Very few of the devices in today's market have the capability to examine control system traffic and determine if the traffic is legitimate or unauthorized. (Note: the capability does exist in some equipment that would allow you to determine if the traffic is the proper format, and to some extent if the data is correct from a protocol standpoint. However there are no devices that would allow you to analyze and determine if the traffic is correct for "that timeframe/conditions of the grid").
8. **Communication Flaws** — Most control systems currently operate on low bandwidth communication paths. Dual use of these paths or unauthorized traffic on these paths (e.g., via worm, or non-prioritized download) may lead to loss of control of the affected devices. In some instances a loss of control may be as bad as compromise of the control device.
9. **Architectural Design Flaw** — Many control systems have not been developed to avoid standard IT problems e.g., lack of boundary checks (i.e.: control signal or data input is outside reasonable numerical bounds) in control systems could lead to "buffer overflow" attacks against the control system software itself. This forms an additional avenue of attack beyond the ones available due to the control system being "overlaid" onto a commercial operating system (Windows, Unix, Linux etc.,).
10. **Architectural Design Flaws** — Many control systems have insufficient defense mechanisms to protect against the installation and implementation of unauthorized software.