GCN
Government Computer News

NIST publishes security guidance for wireless links, industrial controls

10/02/08
By William Jackson

Sponsored By

The National Institute of Standards and Technology has released three information security documents in its 800 series of special publications; two final guidelines on information security assessment and Bluetooth security, and a draft of guidelines for security industrial control systems.

SP 800-121, Guide to Bluetooth Security, has been finalized and describes the security capabilities of Bluetooth technologies and gives recommendations on security them effectively. Bluetooth is an open standards protocol for personal area wireless networking commonly used to connect peripherals with desktop or handheld computing devices.

Much of SP 800-121 originally was included in a draft of NIST's SP 800-48 Revision 1, Wireless Network Security for IEEE 802.11a/b/g and Bluetooth. But because of comments received on that publication, the Bluetooth material has been placed in a separate publication. This document and SP 800-48 Revision 1, which was released in July, replace the original SP 800-48, which dates to 2002.

SP 800-115, Technical Guide to Information Security Testing and Assessment, provides guidance for planning and conducting tests, analyzing findings and developing mitigation strategies for risks that are identified. The document gives an overview of key elements of security testing, with the benefits and limitations of different technical testing techniques and recommendations for their use. It replaces SP 800-42, Guidelines on Network Security Testing, which was released in 2003.

For effective testing and assessment, NIST recommends that organizations:

- Establish an information security assessment policy to identify requirements for executing assessments and provide accountability topics to address organizational requirements, roles and responsibilities, adherence to an established assessment methodology, assessment frequency and documentation requirements.
- Implement a repeatable and documented assessment methodology. This enables organizations to maximize the value of assessments while minimizing possible risks introduced by certain technical assessment techniques. Minimizing risk caused by assessment techniques requires skilled assessors, comprehensive assessment plans, logging assessor activities, performing testing off-hours and conducting tests on duplicates of production systems. Organizations need to determine the level of risk they are willing to accept for each assessment and tailor their approaches accordingly.
- Determine the objectives of each security assessment. Because no individual technique provides a comprehensive picture of an organization's security when executed alone, organizations should use a combination of techniques. This also helps organizations to limit risk and resource usage.
- Analyze findings and develop risk mitigation techniques to address weaknesses. This includes conducting root cause analysis upon completion of an assessment to translate findings into actionable mitigation techniques.

A final draft of SP 800-82, Guide to Industrial Control Systems (ICS) Security, is being released for public comment. Its guidance includes recommendations for security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and other control system configurations such as Programmable Logic Controllers.

"These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems," the document says. Examples of use within the government include air traffic control and materials handling such as that done by the U.S. Postal Service.

As these once isolated systems are being replaced with standardized IT solutions with IP connections, the possibility of cyber vulnerabilities and exploitations rises. "While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments," NIST advises. "In some cases, new security solutions are needed that are tailored to the ICS environment."

Major security objectives for an ICS implementation recommended by NIST include:

- Restricting logical access to the ICS network and network activity. This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks.
- Restricting physical access to the ICS network and devices. A combination of physical access controls should be used, such as locks, card readers and/or guards.
- Protecting individual ICS components from exploitation. This includes deploying security patches as quickly as possible after testing under field conditions; disabling all unused ports and services; restricting ICS user privileges to those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible.
- Maintaining functionality during adverse conditions, providing a redundant counterpart for each critical component.
- Restoring a system after an incident. Incidents are inevitable and an incident response plan is essential.

This document is an update of the second draft, released in 2007. Comments should be sent by Nov. 30 to 800-82comments@nist.gov with "Comments SP 800-82" in the subject line.

© 1996-2008 1105 Media, Inc. All Rights Reserved.