ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY FOR WIRELESS NETWORKS AND DEVICES

Shirley Radack, Editor, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Many organizations and users have found that wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) devices have flexibility to move their laptop computers from one place to another within their offices while maintaining connectivity with the network. Wireless personal networks allow users to share data and applications with network systems and other users with compatible devices, without being tied to printer cables and other peripheral device connections. Users of handheld devices such as personal digital assistants (PDAs) and cell phones can synchronize data between PDAs and personal computers and can use network services such as wireless email, web browsing, and Internet access. Further, wireless communications can help organizations cut their wiring costs.

While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies, and are open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users. Another risk is the theft of the small and portable devices themselves.

NIST Guidance on Security of Wireless Networks and Devices

The National Institute of Standards and Technology, Information Technology Laboratory, has published recommendations to improve the security of wireless networks in NIST Special Publication (SP) 800-48, *Wireless Network Security, 802.11, Bluetooth, and Handheld Devices*. Written by Tom Karygiannis and Les Owens, NIST SP 800-48 discusses three aspects of wireless security:

- security issues associated with wireless local area networks (WLANs) that are based on Institute of Electrical and Electronics Engineers (IEEE) standards 802.11;
- security issues related to wireless personal area networks based on the Bluetooth specifications, which were developed by an industry consortium; and
- security of wireless handheld devices.

This ITL bulletin summarizes the publication, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

The publication includes checklists that organizations will find useful in assessing the security of their wireless networks and devices. The appendices contain information about wireless frequencies and applications, a glossary of terms used, and an explanation of acronyms and abbreviations. Also included are summaries of eight IEEE 802.11 standards, references to print and electronic sources of information, and information about wireless networking tools.

The Risk Environment

Wireless networks and handheld devices are vulnerable to many of the same threats as conventional wired networks. Intruders who gain access to information systems via wireless communications can bypass firewall protection. Once they have accessed systems, intruders can launch denial of service attacks, steal identities, violate the privacy of legitimate users, insert viruses or malicious code, and disable operations. Sensitive information that is transmitted between two

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since November 2001

❒ *Computer Forensics Guidance*, November 2001

❒ *Guidelines on Firewalls and Firewall Policy*, January 2002

❒ *Risk Management Guidance for Information Technology Systems,* February 2002

❒ *Techniques for System and Data Recovery*, April 2002

❒ *Contingency Planning Guide for Information Technology Systems*, June 2002

❒ *Overview: The Government Smart Card Interoperability Specification,* July 2002

❒ *Cryptographic Standards and Guidelines: A Status Report*, September 2002

❒ *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002

❒ *Security for Telecommuting and Broadband Communications*, November 2002

❒ *Security of Public Web Servers*, December 2002

❒ *Security of Electronic Mail*, January 2003

❒ *Secure Interconnections for Information Technology Systems*, February 2003

wireless devices can be intercepted and disclosed if not protected by strong encryption. Handheld devices, which are easily stolen, can reveal sensitive information.

Before establishing wireless networks and using handheld devices, organizations should use risk management processes to assess the risks involved, to take steps to reduce the risks to an acceptable level, and to maintain that acceptable level of risk. Using risk management processes, managers can protect systems and information in a cost-effective manner by balancing the operational and economic costs of needed protective measures with the gains in mission capability to be achieved through the application of new technology.

Wireless Technology and Standards

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Two standards for wireless technologies are discussed in NIST SP 800-48. One is the IEEE 802.11 group of standards for WLANs, which were developed by a voluntary industry standards committee. The IEEE 802.11 standards provide specifications for high-speed networks that support most of today's applications. The Bluetooth standard, which was developed by a computer and communications industry consortium, specifies how mobile phones, computers, and PDAs interconnect with each other, with home and business phones, and with computers using short-range wireless connections.

As wireless technology evolves, new devices are being developed to provide more features, functions, portability and ease of use. Mobile phones can provide multiple services including voice, email, text messaging, paging, web access, and voice recognition services. Newer mobile phones incorporate PDA, wireless Internet, email, and global positioning system (GPS) capabilities.

Recommendations for Secure Wireless Networks

The trends in use of information technology point to increased implementation of wireless communications networks and use of wireless devices. Each new development will present new security risks, which must be addressed to ensure that critical assets remain protected. Actions that organizations should take to protect the confidentiality, integrity, and availability of all systems and information include:

Assess risks, test and evaluate system security controls for wireless networks more frequently than for other networks and systems. Maintaining secure wireless networks is an ongoing process that requires greater effort than that required for other networks and systems.

Steps that can be taken to improve the management of wireless networks include:

- Maintain a full understanding of the topology of the wireless network.
- Label and keep inventories of the fielded wireless and handheld devices.
- Create backups of data frequently.
- Perform periodic security testing and assessment of the wireless network.
- Perform ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Apply patches and security enhancements.
- Monitor the wireless industry for changes to standards that enhance security features and for the release of new products.
- Monitor wireless technology for new threats and vulnerabilities.

Perform a risk assessment, develop a security policy, and determine security requirements before purchasing wireless technologies.

The risks associated with the use of wireless technologies are considerable, and many products provide inadequate protection. Organizations should plan to protect their essential operations before they adopt wireless technologies. Common administration problems include installing equipment with "factory default" settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or installing security architectures that are suitable to the wireless environment. The use of firewalls between wired and wireless systems should be considered. Other good practices are to block unneeded services and ports, and to use strong cryptography. Often the risks can be addressed, but the tradeoffs between technical solutions and costs must be considered as well. Organizations may want to postpone the installation of wireless networks until more robust, open, and secure products are available.

Organizations should perform security assessments prior to implementation of wireless technologies to determine the specific threats and vulnerabilities that wireless networks will introduce in their environments. In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

of security measures, and technical requirements. Once the risk assessment is complete, the organization can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing.

Effective risk management should be integrated into the System Development Life Cycle (SDLC) of an IT system. The SDLC includes five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. NIST has issued recommendations for conducting the risk management process in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. This document is available online at http://csrc.nist.gov/publications/nistpubs/index.html.

Maintain an awareness of the technical and security implications of wireless and handheld device technologies.

Wireless technologies present unique security challenges due in part to the relative immaturity of the technology, incomplete security standards, flawed implementations, limited user awareness, and lax security and administrative practices. In a wireless environment, data is broadcast using radio frequencies. As a result, data may be captured when it is broadcast. The distances needed to prevent eavesdropping vary considerably because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high-gain antennas. The safe distance can vary up to kilometers, even when the nominal or claimed operating range of the wireless device is less than a hundred meters.

Carefully plan for the installation of wireless technologies.

The security of wireless networks and devices should be considered from the initial planning stage because it is much more difficult to address security once deployment and implementation have occurred. A detailed, well-designed plan can point the way to better security decisions about configuring wireless devices and network infrastructure. The plan will support decisions concerning the tradeoffs between usability, performance, and risk.

Apply security management practices and controls to maintain and operate secure wireless networks.

Organizations should identify their information system assets, and develop, document and implement policies, standards, procedures, and guidelines to ensure confidentiality, integrity, and availability of information system resources. NIST recommends the following steps:

- The information system security policy should directly address the use of 802.11, Bluetooth, and other wireless technologies.
- Configuration/change control and management practices should ensure that all equipment has the latest software release, including security feature enhancements and patches for discovered vulnerabilities.
- Standardized configurations should be employed to reflect the security policy, and to ensure change of default values and consistency of operations.
- Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.
- Robust cryptography is essential to protect data transmitted over the radio channel, and theft of equipment is a major concern.

Physical controls should be implemented to protect wireless systems and information.

Adequate physical security measures include barriers, access control systems, and guards. Physical countermeasures can lessen risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices. The small size, relatively low cost, and constant mobility of handheld devices make them more likely to be stolen, misplaced, or lost, and the physical security controls that protect desktop computers do not offer the same protection for handheld devices.

Enable, use, and routinely test the inherent security features, such as authentication and encryption methods that are available in wireless technologies. Firewalls and other appropriate protection mechanisms should also be employed.

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. The security features available in wireless networks and devices may not be as comprehensive or robust as necessary. The security features provided in some wireless products may be weak; therefore, robust, well-developed, and properly implemented cryptography should be used to attain the highest levels of integrity, authentication, and confidentiality.

The built-in security features of Bluetooth and 802.11 networks can include data link level encryption and authentication protocols, and these features should be used as part of an overall defense-in-depth strategy. Although these protection mechanisms may have weaknesses, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks.

The data link level wireless protocol protects only the wireless subnetwork. Where traffic traverses other network segments, including wired segments or the organization's backbone network, other end-to-end

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

cryptographic protection may be required. Since there is still a residual risk when cryptography and other security countermeasures are used, it may also be necessary to provide strategically located access points, firewall filtering, and antivirus software.

Federal agencies must use Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules,* when they have determined that information must be protected by cryptography. Since the security protections in 802.11 and Bluetooth networks do not meet the requirements of FIPS 140-2, higher-level cryptographic protocols and applications should be used. These include secure shell (SSH), Transport-Level Security (TLS), or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the non-validated data link security protocols are used. Future wireless products are expected to offer data linked cryptographic services for FIPS 197, *Advanced Encryption Standard*. Such products, when validated for conformance with FIPS 140-2, should be considered for use when they become available.

NIST supports federal agencies and their use of cryptographic products through its Cryptographic Module Validation Program (CMVP), which validates cryptographic modules to FIPS 140-2, *Security Requirements for Cryptographic Modules*, and other FIPS cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information. Information about the CMVP is available at http://csrc.nist.gov/cryptval.

Summary

Organizations and individuals benefit when wireless networks and devices are protected. After assessing the risks associated with wireless technologies, organizations can reduce the risks by applying countermeasures to address specific threats and vulnerabilities. These countermeasures include management, operational, and technical controls. While these countermeasures will not prevent all penetrations and adverse events, they can be effective in reducing many of the common risks associated with wireless technology.

Additional Useful References

In addition to the references cited in this bulletin, organizations may find the following publications useful in planning, implementing, and maintaining wireless networks:

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance on general security procedures.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, provides details on access control issues, and developing and updating security plans.

NIST SP 800-31, *Intrusion Detection Systems (IDS)*, and NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, provide information on selection of security controls.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, gives information on coordinating contingency planning activities.

Guidance on physical security techniques is included in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*; and NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300
Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195