ITL BULLETIN FOR FEBRUARY 2012

GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS (WLANS)

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Many government and private sector organizations have implemented wireless local area networks (WLANs) that enable staff members with wireless-enabled devices, such as smart phones, to connect to the Internet and to the organization's networks. Wireless networks support a mobile workforce and increase the organization's flexibility.

Small wireless devices can be used for many tasks: making and receiving voice calls, sending and receiving text messages, managing information, sending and receiving electronic mail, browsing the web, storing and modifying documents, accessing data, and performing other tasks that are commonly done on a desktop computer. The Office of Management and Budget (OMB) recognized the benefits of mobility for federal workers in a January 2012 statement that supported increased mobility as a means for organizations to realize savings and to improve productivity.

Security of Wireless Networks

Wireless technologies use radio waves instead of direct physical connections to transmit data between networks and devices. Wireless networks, like other communications networks, are vulnerable to risks that could compromise the confidentiality, integrity, and availability of information systems and information. Attackers who gain unauthorized access to wireless networks can obtain sensitive information, conduct fraudulent activities, disrupt operations, and attack other networks and systems. Without proper security precautions, information can be intercepted and altered more easily than when transmitted through physical connections. To monitor traffic on a wired network, an attacker would have to gain physical access to the network or remotely compromise systems on the network; for a WLAN, an attacker simply needs to be within range of the wireless transmissions.

The U.S. Government Accountability Office (GAO) analyzed the security practices of federal government organizations that use wireless networks and technologies in a report, *Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk* (GAO-11-43, November 2010). The GAO recommended that federal agencies adopt additional security practices to protect their wireless networks, and that governmentwide oversight of wireless networks should be improved.

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST), which is responsible for developing standards and guidelines for information security under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, has issued many publications that explain secure wireless communications and that recommend good practices for protecting wireless transmissions. See the **For More Information** section below for a listing of some of NIST's wireless security-related publications.

To help federal organizations implement NIST's recommendations and improve their WLAN security, NIST recently published Special Publication (SP) 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs): Recommendations of the National Institute of Standards and Technology.* This new publication supplements the other NIST publications on the security of wireless local area networks and consolidates the key recommendations of the previous publications.

Wireless Local Area Networks (WLANs)

Wireless networking enables computing devices with wireless capabilities to use computing resources without being physically connected to a network. To communicate, the devices must be within a certain distance (known as the range) of the wireless network infrastructure. WLANs are groups of wireless networking devices within a limited geographic area, such as an office building, that exchange data through radio communications. WLANs are usually implemented as extensions to the organization's existing wired local area networks (LANs), supporting user mobility and access to the organization's wired networks.

WLAN technologies are based on industry consensus-based standards developed by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE 802.11 standard and its amendments provide technical specifications and security requirements for WLANs. Two basic components of WLANs are defined: client devices, such as laptops and smart phones, and access points (APs), which logically connect client devices with a distribution system (DS). The DS allows the client devices to communicate with the organization's wired LANs and external networks such as the Internet. Some WLANs also use wireless switches, which act as intermediaries between APs and the DS, and assist administrators in managing the WLAN infrastructure.

The security of the WLAN depends upon how well all of the WLAN components, including client devices, APs, and wireless switches, are secured throughout the life cycle of the WLAN. WLANs are frequently less secure than wired networks. The configuration of the WLANs may not include a strong process for the authentication of users; this makes it easier for attackers within range of the WLAN to gain access to it. These weak configurations are often used because they are more convenient for the users and the network administrators.

The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the initiation of a

project to develop a system to its disposition. The system life cycle is a multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system. NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* discusses the life cycle process.

NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs): Recommendations of the National Institute of Standards and Technology*

NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs),* was written by Murugiah Souppaya of NIST and Karen Scarfone of Scarfone Cybersecurity. The publication supplements other NIST publications on the security of wireless local area networks; it summarizes and strengthens recommendations to help organizations improve the security configuration and monitoring of their IEEE 802.11 wireless local area networks and their devices connecting to the networks. The recommendations included in SP 800-153 are applicable to the protection of unclassified wireless networks and of unclassified facilities that are within range of unclassified wireless networks.

SP 800-153 points readers to other NIST publications for additional information on system planning, development, and security activities. Federal organizations should follow the recommendations in other NIST publications, such as NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, and NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* In cases where there might be a conflict between recommendations in the publications cited here, the provisions of NIST SP 800-153 apply.

A section of the new guideline provides recommendations for WLAN security configuration, including configuration design, implementation, evaluation, and maintenance. Another section overviews the monitoring of WLAN security and provides guidelines concerning the selection of monitoring tools and the frequency of security monitoring. Information contained in the appendices includes a list of the major security controls for WLAN security that are incorporated in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; a list of acronyms and abbreviations used in the publication; and a list of references on issues related to WLAN security.

NIST SP 800-153 is available from the NIST web page here.

NIST's Recommendations for Improving WLAN Security

NIST recommends that organizations implement the following guidelines to improve the security of their WLANs:

• Employ standardized security configurations for common WLAN components, such as client devices and APs.

A standardized configuration provides a base level of security, reducing vulnerabilities and lessening the impact of successful attacks on the network. Standardized configurations can also significantly reduce the time and effort needed to secure WLAN components and verify their security, particularly if the configuration can be deployed and verified through automated means.

• Consider both the security of the WLAN and how the security of other networks may be affected by the WLAN, when developing plans for WLAN security.

A WLAN is usually connected to an organization's wired networks, and WLANs may also be connected to each other. The client devices of WLANs that need wired network access should be allowed access only to the necessary hosts on the wired network and to use only the required protocols. Also, an organization should have separate WLANs if there is more than one security profile for WLAN usage; for example, an organization should have logically separated WLANs for external use (such as guests) and for internal use. Devices on one WLAN should not be allowed to connect to devices on a logically separated WLAN.

• Implement policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the application of appropriate security controls.

A client device with dual connections is connected to both a wired network and a WLAN at the same time. If an attacker gains unauthorized wireless access to a dual-connected client device, the attacker could then use that access to attack resources on the wired network. Organizations should consider the risks posed not only by the traditional form of dual connections, but also by other forms involving multiple wireless networks. Client devices may be connected to multiple wireless networks simultaneously, such as cell phone, WiMAX, Bluetooth, and WLAN networks. Organizations should assess the risk of the possible combinations of network technologies for their WLAN client devices and determine how those risks should be mitigated. If the risks to one or more of the networks cannot be mitigated to an acceptable level, then dual connections involving that network may pose too much risk to the organization, and the organization should consider prohibiting such connections.

FISMA emphasizes a risk-based policy for cost-effective security. The changing technology environment accentuates the importance of active, continuous management of risks. NIST SP 800-53A Revision l, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans,* supports organizations in assessing the effectiveness of the security controls that are implemented in federal information systems. The selection and assessment of appropriate security controls are important steps in the comprehensive process of managing risks and maintaining effective security of those information systems. Appendix A of SP 800-153 lists the security controls that are applicable to WLAN security.

• Ensure that the organization's WLAN client devices and APs have configurations that are compliant with the organization's WLAN policies.

Ensure that security configurations for WLAN client devices and APs are maintained throughout their life cycle and are consistent with the organization's WLAN policies. After designing WLAN security configurations for client devices and APs, organizations should determine how the configurations will be implemented, evaluate the effectiveness of the implementations, deploy the implementations to the appropriate devices, and maintain the configurations and their implementations throughout the life cycles of client devices. Organizations should standardize, automate, and centralize their activities for WLAN security configuration implementation and maintenance as much as practical. This allows the implementation of consistent WLAN security throughout the enterprise; organizations will be able to detect and correct unauthorized changes to configurations, and to react quickly when newly identified vulnerabilities or recent incidents indicate a need to change the security configurations of WLANs.

• Perform both attack monitoring and vulnerability monitoring to support WLAN security.

Security monitoring is very important for all systems and networks, and it is especially important for WLANs because of the increased risks that they face. Organizations should continuously monitor their WLANs for both WLAN-specific and general (wired network) attacks. Organizations should do largely the same vulnerability monitoring for WLAN components that they do for any other software: identifying patches and applying them, and verifying security configuration settings and adjusting them as needed. These actions should be performed at least as often for WLAN components as they are for the organization's equivalent wired systems.

Attack monitoring should consider both passive and active attacks: in passive attacks, an unauthorized party monitors WLAN communications, but does not generate, alter, or disrupt WLAN communications; in active attacks, an unauthorized party generates, alters, or disrupts WLAN communications.

Vulnerability monitoring for WLANs involves analyzing WLAN communications and identifying policy violations, such as communications using the wrong protocols, encryption key lengths, etc. This process can help to identify configuration issues related to WLAN devices, and is useful when not all of the WLAN devices are under the organization's control, such as visitor laptops, and when unauthorized WLAN devices are a concern.

• Conduct regular periodic technical security assessments of the organization's WLANs.

Regular assessments should be performed at least annually to evaluate the overall security of the WLAN. In addition, organizations should perform periodic assessments at least quarterly unless their activities for continuous monitoring of WLAN security are

already collecting all of the necessary information about WLAN attacks and vulnerabilities needed for assessment purposes.

For More Information

Information about standards developed by the Institute of Electrical and Electronics Engineers (IEEE) is available here.

Government Accountability Office (GAO) Report 11-43, *Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk* (November 2010) is available here.

Office of Management and Budget, *The Mobile Opportunity* (January 12, 2012) is available here.

NIST publications that provide guidance and requirements for information system planning, configuration, and security for wireless devices include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
NIST Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*
SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*
SP 800-70 Revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*
SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
SP 800-115, *Technical Guide to Information Security Testing and Assessment*
SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*
SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

Security configuration checklists help organizations to automatically set and verify the appropriate security settings for different information technology products. NIST maintains the National Checklist Repository, a publicly available resource that contains information on a variety of security configuration checklists. For information about NIST's checklist program and the National Checklist Program Repository, see the NIST web page here.

To achieve adequate security, federal managers must actively manage the risks to their core missions and business functions, and to the information and information systems supporting those missions and functions. NIST developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level. The RMF is available here.

For information about NIST standards and guidelines, and related publications, see the NIST web page here.

For information about NIST's cybersecurity programs, see web page here.

ITL Bulletin Publisher: Elizabeth B. Lennon
Writer/Editor, Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov