Protecting Wireless Local Area Networks (WLANs)

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 can contribute to increased organizational productivity.

Small wireless devices are 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 regularly done on a desktop computer.

WLAN Technology

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.

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.

Implementing Security Throughout the WLAN Lifecycle
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. Weak authentication methods 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.

To help organizations improve their WLAN security, the National Institute of Standards and Technology (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.* For access to SP 800-153 and to other NIST publications with information about the security of wireless local area networks, the system development life cycle and the management of risks to systems, see http://csrc.nist.gov/publications/PubsSPs.html

What can organizations do to improve the security of their WLANs?

Employ standardized security configurations.
A standardized configuration for common WLAN components 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.
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 the use of only required protocols. In addition, 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 and enforce policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices.

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 apply appropriate security controls. 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.

Ensure that WLAN client devices and APs have configurations that are compliant with WLAN policies.
After WLAN security configurations are designed 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 the implementation and maintenance of WLAN security configurations 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 especially important for WLANs because of their exposure to increased risks. Organizations should continuously monitor their WLANs for both WLAN-specific and general (wired network) attacks. 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 or encryption key lengths. This monitoring 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 the use of unauthorized WLAN devices is a security concern.

Conduct regular technical security assessments of 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.

Mobile technology is changing the way that we work and interact with others. To achieve the cost savings and improved productivity benefits that mobile technology offers, organizations must take steps to secure their wireless networks, and limit their vulnerability to attacks.

This article was abridged and adapted from “Guidelines for Securing Wireless Local Area Networks (WLANs),” NIST ITL (Information Technology Laboratory) Bulletin, February 2012. 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.