© Route66 | Dreamstime.com

Protecting Wireless Local Area Networks

Shirley Radack and Rick Kuhn, *National Institute of Standards and Technology*

Many government and private-sector organizations have implemented wireless local area networks (WLANs) that let staff members with wireless-enabled devices, such as smartphones, connect to the Internet and the organization's networks. The staff can use such devices for many tasks: to make and receive voice calls, send and receive text messages, manage information, send and receive email, browse the Web, store and modify documents, access data, and perform other tasks regularly done on a desktop computer. Wireless networks thus support a mobile workforce and can contribute to increased organizational productivity.

However, what should organizations do to improve the security of such WLANs?

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 and information systems. 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.

WLAN technologies are based on industry consensus-based standards developed by 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 smartphones, and *access points*, which logically connect client devices with a distribution system. The distributed system lets the client devices 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 access points and the distributed system and help administrators manage the WLAN infrastructure.

Implementing Security

WLAN security depends on how well all of the WLAN components—including the client devices, access points, and wireless switches—are secured throughout the WLAN life cycle. WLANs are frequently less secure than wired networks. The configuration of the WLANs might not include a strong process for authenticating users, making it easier for attackers within range of the WLAN to gain access to it. Weak authentication methods are often used because they're more convenient for the users and 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 project initiation to system development to final disposition. The system life cycle is a multistep process that starts with system initiation, analysis, design, and implementation, and continues through to system maintenance and disposal.

To help organizations improve their WLAN security, the National Institute of Standards and Technology (NIST) recently published *Guidelines for Securing Wireless*

Local Area Networks (WLANs): Recommendations of the National Institute of Standards and Technology.[1] For access to this and other NIST publications with information about WLAN security, the system development life cycle, and the management of system risks, see http://csrc.nist.gov/publications/PubsSPs.html.

Here, we summarize some of the recommendations from the new NIST guidelines to help organizations 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.

Organizations should consider the risks posed not only by the traditional form of dual connections but also by other forms involving multiple wireless networks.

Consider Other Networks

It's useful to consider both the security of the WLAN as well as how it might affect the security of other networks. A WLAN is usually connected to an organization's wired networks, and WLANs can 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 they should use only required protocols.

In addition, an organization should have separate WLANs if there's more than one security profile for WLAN usage. For example, an organization should have logically separated WLANs for external use (such as for guests) and for internal use. Devices on one WLAN shouldn't be allowed to connect to devices on a logically separated WLAN.

State Which Dual Connections Are Allowed

Organizations should 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 might 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 can't be sufficiently mitigated, then dual connections involving that network might pose too much risk, in which case the organization should consider prohibiting such connections.

Ensure Configurations Are Compliant

After WLAN security configurations are designed for client devices and access points, 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 client-device life cycles. 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 WLAN security configurations.

Perform Attack and Vulnerability Monitoring

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 doesn't 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 identify configuration issues related to WLAN devices. It's also useful when not all of the WLAN devices are under the organization's control—such as visitor laptops—or when the use of unauthorized WLAN devices is a security concern.

Conduct Regular Technical Security Assessments

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. IT

Acknowledgments

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

Reference

1. M. Souppaya and K. Scarfone, "Guidelines for Securing Wireless Local Area Networks (WLANs)," *NIST Information Technology Laboratory Bull.*, SP 800-153, Feb. 2012.

***Shirley Radack** is a guest researcher at the US National Institute of Standards and Technology. Contact her at shirley.radack@nist.gov.*

***Rick Kuhn** is a computer scientist at the US National Institute of Standards and Technology. Contact him at kuhn@nist.gov.*