April 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURING WIRELESS NETWORKS

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

Many users and organizations have found that wireless communications and devices are convenient, flexible, and easy to use. Wireless local area networks (WLANs) enable users with mobile devices that operate over radio frequencies to move from one place to another without being physically connected to a network. Portable computers, personal digital assistants (PDAs), and cell phones support the sharing of data and applications with network systems and other users with compatible devices, and provide access to network services such as wireless email, web browsing, and the Internet. Wireless communications can benefit organizations by reducing their wiring costs.

The mobile devices function within the range of the wireless network, usually limited to an area such as an office building or building complex. Since they transmit data through radio frequencies, wireless networks are open to intruders and especially vulnerable to security risks unless properly protected. Intruders have exploited the openness of wireless networks to access systems, destroy and steal data, and launch attacks that take over network bandwidth and deny service to authorized users.

Wireless Local Area Networks Standards and Security

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) issued Special Publication (SP) 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, in 2002. This guide assists organizations in implementing a family of voluntary industry standards developed by the Institute of Electrical and Electronics Engineers (IEEE) to define the characteristics, the transmission of data, and the security of wireless local area networks. In addition to the IEEE 802.11b and 802.11g standards, NIST SP 800-48 also discusses Bluetooth technology and wireless handheld devices such as text messaging devices, PDAs, and smart phones.

The IEEE 802.11 standards were based on a security method known as Wired Equivalent Privacy (WEP). Since this method had been subject to several well-documented security problems, the concerns about security led the standards developers to improve the security methodology with an amendment to the specifications (IEEE 802.11i).

The amendment introduces new security features to overcome the shortcomings of WEP and presents the concept of the Robust Security Network (RSN), a wireless security network with three main components:

- stations (STA) - wireless endpoint devices such as laptops, and wireless handheld devices such as PDAs, text messaging devices, and smart phones;

- access points (AP) - network devices that allow STAs to communicate over radio frequencies and to connect to another network, such as the organization's wired infrastructure; and

- authentication servers (AS) - WLAN components that provide authentication services to STAs.

Threats to WLANs often involve an attacker with access to the radio link between two STAs or between a STA and an AP. The RSN framework, as described in IEEE 802.11i, provides for the creation

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 8900, Gaithersburg, MD 20899-8900, 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 May 2006:

of Robust Security Network Associations (RSNAs). RSNAs are wireless connections that provide moderate to high levels of assurance against WLAN security threats through the use of a variety of cryptographic techniques.

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.

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*

ITL recently issued NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, to supplement NIST SP 800-48 and to assist organizations in establishing and maintaining robust security for WLANs using the new security features that were developed for IEEE 802.11i. Written by Sheila Frankel and Karen Scarfone of NIST and by Bernard Eydt and Les Owens of Booz Allen Hamilton, the guide includes an overview of wireless networking, focusing on the IEEE 802.11 family of WLAN standards. The publication explains the basic WLAN components and architectural models and provides an overview of WLAN security, including a review of the security features and weaknesses of the IEEE 802.11 specifications, and the features of the IEEE 802.11i amendment that improve WLAN security.

NIST SP 800-97 introduces the major security-related components that are defined in IEEE 802.11i and explains the security features and capabilities associated with the framework for RSNs. It provides extensive guidance on the planning and deployment of RSNs, the steps needed to establish RSNAs, data confidentiality and integrity protocols, and the cryptographic keys that are created and used by these protocols.

Other issues discussed include the five phases of operation that occur during RSN communications, starting with the discovery of a WLAN and ending in the termination of the connection; the types of frames used to carry information between RSN components; the flow of frames between components during each phase of RSN operation; and planning for the implementation of the Extensible Authentication Protocol (EAP). The EAP, which was designed to accommodate the use of new authentication methods as they are developed, should be used by organizations for most RSN deployments. Also discussed are the most common EAP methods, how organizations can select EAP methods appropriate to their environments, EAP security considerations, and the EAP architectural model and related support requirements.

A section of the guide focuses on validation testing of cryptographic products as required under Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and the certification requirements as applied to IEEE 802.11 wireless networks. This section also provides an overview of the security specifications developed by the Wi-Fi Alliance, a nonprofit industry consortium of WLAN equipment and software vendors, which conducts a certification program for WLAN products. The certifications help organizations select interoperable WLAN products that can support RSNs. Recommendations for best practices related to WLAN security are summarized, and planned extensions to IEEE 802.11 are discussed.

Extensive appendices to NIST SP 800-97 include an acronym list, references and other sources of information, as well as a listing of online resources that provide additional information about IEEE 802.11i specifications and IEEE 802.11i security.

NIST SP 800-97 is available from NIST's website at http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

Recommendations for Wireless Network Security

NIST recommends that organizations adopt the following practices to improve the security of their wireless networks:

Ensure that all WLAN components use Federal Information Processing Standards (FIPS)-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications.

The IEEE 802.11i amendment defines two data confidentiality and integrity protocols for RSNAs: Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). The guide discusses both protocols, as well as the cryptographic keys created and used by these protocols.

Federal agencies are required to use FIPS-approved cryptographic algorithms that are contained in FIPS-validated cryptographic modules. Only the CCMP uses a FIPS-approved core cryptographic algorithm, the Advanced Encryption Standard (AES), as specified in FIPS 197. Since CCMP provides stronger assurance than WEP and TKIP, federal agencies are advised to use CCMP for securing IEEE 802.11-based WLANs. Auxiliary security protection is required for legacy IEEE 802.11 equipment that does not support the use of the CCMP. Federal agencies should consult NIST SP 800-48 for specific recommendations for securing legacy IEEE 802.11 implementations.

Select IEEE 802.11 RSN authentication methods that meet the needs of the organization's computing environments.

The RSN specified in IEEE 802.11 uses the EAP for the authentication phase of establishing an RSNA. EAP supports a wide variety of authentication methods, also called EAP methods. These methods include authentication based on passwords, certificates, smart cards, and tokens. EAP methods also can include combinations of authentication techniques, such as using a certificate followed by a password, or the option of using either a smart card or a token for authentication. These options enable organizations to

integrate the EAP methods with other environments to which a WLAN might connect. Organizations have considerable discretion in choosing which EAP methods to employ; however, the choice of EAP method should be carefully considered since it can impact the protection provided by an RSN.

Because of the extensible nature of EAP, many EAP methods exist, and others are being developed. Some EAP methods may not satisfy the necessary security requirements for WLANs; for example, EAP methods that do not generate cryptographic keying material cannot be used for WLANs. In general, the current EAP methods that can satisfy WLAN security requirements are based on the Transport Layer Security (TLS) protocol. A primary distinction between TLS-based EAP methods is the level of public key infrastructure (PKI) support required; the EAP-TLS method requires an enterprise PKI implementation and certificates deployed to each STA, while most other TLS methods require certificates on each AS only. Organizations should use the EAP-TLS method whenever possible.

Because some EAP methods have not yet been adopted as voluntary industry standards and new methods are being developed, organizations are encouraged to obtain up-to-date information on EAP methods and standards when planning an RSN implementation, based on IEEE 802.11. See Appendix C of the guide for contact information. Additionally, organizations should ensure that the cryptographic modules implementing the TLS algorithm for each product under consideration have been FIPS-validated.

Before selecting WLAN equipment, organizations should review their existing identity management infrastructure, authentication requirements, and security policy to determine the EAP method or methods that are most appropriate in their environments. They should then acquire systems that support the chosen EAP methods, and implement and maintain them carefully. See the guide for detailed guidance on planning EAP implementations, the available EAP methods, how organizations can select EAP methods, and additional EAP security considerations.

Integrate existing authentication technology with the IEEE 802.11 RSN WLAN to the extent feasible.

Although the RSN framework supports the use of pre-shared keys (PSK), organizations should choose to implement the IEEE 802.1X standard and EAP for authentication instead of using PSKs because of the resources needed for proper PSK administration and the security risks involved. IEEE 802.1X and EAP authentication requires an organization to use an AS, which may necessitate the use of a PKI. An organization that already has implemented ASs for web, email, file and print services, and other authentication needs, should consider integrating this technology into its RSN solution. Most leading network operating systems and directory solutions offer the support needed for RSN integration.

Ensure that the confidentiality and integrity of communications between access points and authentication servers are sufficiently protected.

The data confidentiality and integrity protocol, such as CCMP, used by an IEEE 802.11 RSN protects communications between STAs and APs. However, IEEE 802.11 and its related standards do not cover protection of the communications between the AP and AS. Therefore, organizations deploying RSNs should ensure that communications between each AP and its corresponding ASs are protected sufficiently through the use of cryptography. Also, because of the importance of the ASs, organizations should pay particular attention to establishing and maintaining their security through operating system configuration, firewall rules, and other security controls.

Use technologies that have the appropriate security certification from NIST and interoperability certification from the Wi-Fi Alliance when IEEE 802.11 RSNs are established.

To implement IEEE 802.11 RSNs, organizations may need to update or replace existing IEEE 802.11 equipment and software that cannot support RSNAs. They may also need to purchase additional equipment. The Wi-Fi Alliance's Wi-Fi Protected Access 2 (WPA2) certification program facilitates the interoperability of WLAN products that implement IEEE 802.11i systems with similar equipment from other vendors. Federal agencies should procure WPA2 products that use FIPS-approved encryption algorithms and that have been FIPS-validated. Organizations that plan to use authentication servers as part of their IEEE 802.11 RSN implementations should procure products with the WPA2 Enterprise level certification. Also, because the WPA2 certification is expanded periodically to test for interoperability with additional EAP methods, organizations should obtain the latest WPA2 information before making procurement decisions.

Ensure that WLAN security considerations are incorporated into each phase of the WLAN life cycle in the establishment and maintenance of IEEE 802.11 RSNs.

Each of the phases of the life cycle in planning and implementing IEEE 802.11 RSNs has special considerations for WLAN security. The five-phase life cycle model for WLANs, which is briefly summarized below, is based on the model discussed in NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

- **Initiation Phase** includes the tasks that an organization should perform before it starts to design its WLAN solution: developing a WLAN use policy; performing a WLAN risk assessment; and specifying business and functional requirements for the solution, such as mandating RSNAs for all WLAN connections.

- **Acquisition/Development Phase** includes **Planning and Design**, and **Procurement**:

  - **Planning and Design** allows WLAN network architects to specify the technical characteristics of the WLAN solution, such as authentication methods, and the related network components, such as the firewall rules. The WLAN network architects should also conduct a site survey to help determine the architecture of the solution and how the WLAN should be integrated with the existing authentication

infrastructure, including the organization's PKI.

- **Procurement** involves specifying the number and type of WLAN components that must be purchased, the feature sets they must support such as FIPS-validated encryption modules, and any certifications they must hold such as WPA2 Enterprise.

- **Implementation** entails the configuration of procured equipment to meet operational and security requirements, and the installation and activation of the equipment on a production network, with the appropriate event logging procedures enabled.

- **Operations/Maintenance** includes carrying out security-related tasks that an organization should perform on an ongoing basis once the WLAN is operational, including patching, periodic security assessment, log reviews, and incident handling.

- **Disposition** encompasses the tasks that occur after a system or its components have been retired, including preserving information to meet legal requirements, sanitizing media that might contain sensitive material, and disposing of equipment properly.

Best Practice Recommendations

NIST SP 800-97 summarizes over 50 best practice recommendations for WLAN security, grouped by the life cycle phase for which each recommendation is most relevant. NIST encourages organizations to adopt these best practice recommendations. RSNs are complex, involving multiple devices, protocols, and standards. The recommendations are presented in a way to enable organizations to manage their WLANs and to take actions that will provide reasonable assurance that the WLANs are protected from most security threats. The recommendations should be particularly helpful to organizations that have made a decision to integrate WLAN technology into their computer networks and want to determine the best way to do it. The recommendations will help those organizations that are already managing WLANs, but are not satisfied with the level of security they provide. When they upgrade, replace, and configure their infrastructure, they should enhance security by supporting RSNs and other security controls.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are referenced in the security guide for wireless networks, as well as other security-related publications, see NIST's web page http://csrc.nist.gov/publications/index.html

Federal organizations should follow the guidance on general security controls that are discussed in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, for minimum management, operational, and technical security controls for information systems. This publication is available on the web page listed above.

For information about FIPS 140-2, lists of FIPS-approved cryptographic products, and NIST's Cryptographic Module Validation Program, see http://csrc.nist.gov/cryptval/140-2.htm.

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.

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.