National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-97

Establishing Wireless Robust Security Networks:

A Guide to IEEE 802.11i

Recommendations of the National Institute of Standards and Technology

---

Sheila Frankel
Bernard Eydt
Les Owens
Karen Scarfone

NIST Special Publication 800-97

Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

Recommendations of the National Institute of Standards and Technology

Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2007

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-97
Natl. Inst. Stand. Technol. Spec. Publ. 800-97, 162 pages (February 2007)

Acknowledgements

The authors, Sheila Frankel and Karen Scarfone of the National Institute of Standards and Technology (NIST), and Bernard Eydt and Les Owens of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Tim Grance, Lily Chen, Tim Polk and Randy Easter of NIST, and Alexis Feringa, Thomas Fuhrman, and Marc Stevens of Booz Allen Hamilton, for their keen and insightful assistance throughout the development of the document. The authors appreciate the detailed, perceptive in-depth comments provided by wireless experts Matthew Gast, Jesse Walker (Intel) and Nancy Cam-Winget (Cisco). The authors would also like to express their thanks to Bernard Aboba (Microsoft), Randy Chou (Aruba Networks), Ryon Coleman (3e Technologies), Paul Dodd (Boeing), Dean Farrington (Wells Fargo), Ben Halpert (Lockheed Martin), Criss Hyde, Timothy Kramer (Joint Systems Integration Command), W. J. Miller (MaCT), and Robert Smith (Juniper Networks) for their particularly valuable comments and suggestions.

Trademark Information

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

A wireless local area network (WLAN) enables access to computing resources for devices that are not physically connected to a network. WLANs typically operate over a fairly limited range, such as an office building or building campus, and usually are implemented as extensions to existing wired local area networks to enhance user mobility. This guide seeks to assist organizations in better understanding the most commonly used family of standards for WLANs—Institute of Electrical and Electronics Engineers (IEEE) 802.11—focusing on the security enhancements introduced in the IEEE 802.11i amendment. In particular, this guide explains the security features and provides specific recommendations to ensure the security of the operating environment.

Before IEEE 802.11i was finalized, IEEE 802.11 relied on a security method known as Wired Equivalent Privacy (WEP), which has several well-documented security problems. The IEEE 802.11i amendment introduces a range of new security features that are designed to overcome the shortcomings of WEP. It introduces the concept of a Robust Security Network (RSN), which is defined as a wireless security network that allows the creation of Robust Security Network Associations (RSNA) only. RSNAs are wireless connections that provide moderate to high levels of assurance against WLAN security threats through use of a variety of cryptographic techniques. This guide describes the operation of RSNs, including the steps needed to establish an RSNA and the flows of information between RSN components. The three types of RSN components are stations (STA), which are wireless endpoint devices such as laptops and wireless handheld devices (e.g. PDAs, text messaging devices and smart phones); access points (AP), which are network devices that allow STAs to communicate wirelessly and to connect to another network, typically an organization's wired infrastructure; and authentication servers (AS), which provide authentication services to STAs. STAs and APs are also found in pre-RSN WLANs, but ASs are a new WLAN component introduced by the RSN framework.

NIST recommends that Federal agencies implement the following recommendations to assist in establishing and maintaining robust security for their IEEE 802.11i-based WLANs. Personnel responsible for their implementation and maintenance should read the corresponding sections of the document to ensure they have an adequate understanding of important related issues.

This publication covers IEEE 802.11i-based wireless LANs only. It does not replace NIST Special Publication (SP) 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, which addresses IEEE 802.11b and 802.11g-based wireless LANs, Bluetooth implementations, and wireless handheld devices (e.g., text messaging devices, PDAs, smart phones). Organizations with existing IEEE 802.11b or 802.11g implementations should continue to use the recommendations in SP 800-48 to secure them; they should also review this publication to understand the new IEEE 802.11i technology and how it addresses the shortcomings of the Wired Equivalent Privacy (WEP) protocol used to secure IEEE 802.11b and 802.11g networks. Organizations that are considering the deployment of new wireless LANs should be evaluating IEEE 802.11i-based products and following the recommendations for IEEE 802.11i implementations in this publication.

Organizations should 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). This guide discusses both protocols at length, 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.[1] Of WEP, TKIP, and CCMP, only CCMP uses a core cryptographic algorithm that is FIPS-approved, the Advanced Encryption Standard (AES). For other security features, CCMP offers stronger assurance than WEP and TKIP. Accordingly, NIST requires the use of CCMP for securing Federal agencies' IEEE 802.11-based WLANs. For legacy IEEE 802.11 equipment that does not provide CCMP, auxiliary security protection is required; one possibility is the use of an IPsec VPN, using FIPS-approved cryptographic algorithms. NIST SP 800-48 contains specific recommendations for securing legacy IEEE 802.11 implementations.

Organizations should select IEEE 802.11 RSN authentication methods for their environment carefully.

IEEE 802.11 RSN uses the Extensible Authentication Protocol (EAP) for the authentication phase of establishing an RSNA. EAP supports a wide variety of authentication methods, also called EAP methods. They include authentication based on passwords, certificates, smart cards, and tokens. EAP methods also can include combinations of authentication techniques, such as a certificate followed by a password, or the option of using either a smart card or a token. This flexibility allows EAP to integrate with nearly any environment to which a WLAN might connect. Organizations have considerable discretion in choosing which EAP methods to employ; a poor EAP method choice or implementation could seriously weaken an IEEE 802.11 RSN's protections.

Because of the extensible nature of EAP, dozens of EAP methods exist, and others are being developed continually. However, many EAP methods do 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 are not yet official standards and new methods are being developed, organizations are encouraged to obtain the latest available information on EAP methods and standards when planning an IEEE 802.11 RSN implementation. Additionally, organizations should ensure that the cryptographic modules implementing the TLS algorithm for each product under consideration are 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, then purchase systems that support the chosen EAP methods, and implement and maintain them carefully. This publication provides detailed guidance on planning EAP implementations. It discusses the most common EAP methods, explains how organizations can select EAP methods, and examines additional EAP security considerations.

[1] Information about NIST's Cryptographic Module Validation program can be found at http://csrc.nist.gov/cryptval/140-2.htm. FIPS PUB 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) describes the generic security requirements; the implementation guide (http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf) includes specific implementation guidance for IEEE 802.11. Lists of FIPS-approved cryptographic products can be found at http://csrc.nist.gov/cryptval/140-1/1401val.htm.

Organizations should integrate their existing authentication technology with their 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 ASs for Web, e-mail, 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.

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

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 explicitly state that protection of the communications between the AP and AS is out of their scope. Therefore, organizations deploying RSNs should ensure that communications between each AP and its corresponding ASs are protected sufficiently through 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.

Organizations establishing IEEE 802.11 RSNs should use technologies that have the appropriate security certification from NIST and interoperability certification from the Wi-Fi Alliance.

To implement IEEE 802.11 RSNs, organizations may need to update or replace existing IEEE 802.11 equipment and software that cannot support RSNAs, as well as purchase additional equipment. The Wi-Fi Alliance, a non-profit industry consortium of WLAN equipment and software vendors, has established the Wi-Fi Protected Access 2 (WPA2) certification program to give consumers of WLAN products assurance that their IEEE 802.11i systems can interoperate with similar equipment from other vendors. Federal agencies should procure WPA2 products that use FIPS-approved encryption algorithms and 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.

Organizations should ensure that WLAN security considerations are incorporated into each phase of the WLAN life cycle when establishing and maintaining IEEE 802.11 RSNs.

This guide presents extensive guidance on IEEE 802.11 RSN planning and implementation. It describes a life cycle model for WLANs and presents best practice recommendations related to WLAN security for each phase in the life cycle. WLAN security considerations for each phase include the following:

- **Phase 1: Initiation**. This phase includes the tasks that an organization should perform before it starts to design its WLAN solution. These include 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.
- **Phase 2: Acquisition/Development.** For the purposes of this guide, the Acquisition/Development phase is split into the following two phases: