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

Special Publication 800-48
Revision 1 (Draft)

Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (DRAFT)

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Derrick Dicoi

NIST Special Publication 800-48
Revision 1 (Draft)

Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (Draft)

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Derrick Dicoi

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

August 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 800-48 Revision 1 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-48 Rev. 1, 96 pages (Aug. 2007)

Acknowledgments

The authors, Karen Scarfone of the National Institute of Standards and Technology (NIST) and Derrick Dicoi 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 Sheila Frankel, Tim Grance, and Tom Karygiannis of NIST, and John Padgette and Michael Bang of Booz Allen Hamilton, for their keen and insightful assistance throughout the development of the document. Additional acknowledgements will be added to the final version of the publication.

Acknowledgements, original version of the publication

The authors, Tom Karygiannis of NIST and Les Owens of Booz Allen Hamilton, wish to express their sincere thanks to numerous members of government, industry, and academia who have commented on this document. First, the authors wish to express their thanks to the staff at Booz Allen Hamilton who contributed to this document. In particular, their appreciation goes to Rick Nicholson, Brendan Goode, Christine Kerns, Sharma Aditi, and Brian Miller for their research, technical support, and contributions to this document. The authors express their appreciation to Bill Burr, Murugiah Souppaya, Tim Grance, Ray Snouffer, Sheila Frankel, and John Wack of NIST, for providing valuable contributions to the technical content of this publication. The authors would also like to express their thanks to security experts Russ Housley, Markus Jacobsson, Jan-Ove Larsson, Simon Josefsson, Stephen Whitlock, Brian Seborg, Pascal Meunier, William Arbaugh, Joesph Kabara, David Tipper, and Prashanth Krishnanmurthy for their valuable comments and suggestions. Finally, the authors wish to thank especially Matthew Gast, Keith Rhodes, and the Bluetooth Special Interest Group for their critical review and feedback during the public comments period. Contributions were also made by Rick Doten, Jerry Harold, Stephen Palmer, Michael D. Gerdes, Wally Wilhoite, Ben Halpert, Susan Landau, Sandeep Dhameja, Robert Moskowitz, Dennis Volpano, David Harrington, Bernard Aboba, Edward Block, Carol Ann Widmayer, Harold J. Podell, Pieter Kasselman, Rick E. Morin, Chall McRoberts, and Kevin L. Perez.

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

Wireless communications offer organizations and users many benefits, such as portability, flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot.

The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to an organization's systems and information, corrupt the organization's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use the organization's resources to launch attacks on other networks.

Specific threats and vulnerabilities to wireless networks include the following:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is transmitted without being encrypted (or that is encrypted with weak cryptographic techniques) may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Malware may corrupt data on a wireless device and subsequently be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activities.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

- Malicious entities may use rogue wireless networks deployed within an organization to gain access to the organization's network resources.
- Internal and client device-based attacks may be possible via ad hoc transmissions.

This document provides an overview of wireless networking technologies, and provides in-depth explanations of two wireless networking technologies commonly used in office environments and with today's mobile workforce: Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g and Bluetooth. This document seeks to assist organizations in reducing the risks associated with these forms of wireless networking.

This document is an update to the original version of NIST SP 800-48, which was released in November 2002. Since that time, IEEE 802.11i has been finalized as a replacement for IEEE 802.11a/b/g, and additional serious security flaws have been discovered in IEEE 802.11a/b/g. IEEE 802.11i has built-in features for providing robust security for wireless communications, including support for Federal Information Processing Standard (FIPS) validated cryptographic algorithms. Therefore, NIST recommends that organizations with existing IEEE 802.11a/b/g implementations develop and implement migration strategies to move to IEEE 802.11i because of its superior security.

In terms of wireless local area networks, this publication covers IEEE 802.11a/b/g only. It does not replace NIST Special Publication (SP) 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, which addresses IEEE 802.11i-based wireless LANs.[1] Organizations with existing IEEE 802.11i implementations should continue to use the recommendations in SP 800-97 to secure them. 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 SP 800-97.

NIST recommends the following actions for securing wireless technologies:

Organizations should be aware of the technical and security implications of wireless technologies.

Although wireless technologies offer significant benefits, they also provide unique security challenges over their wired network counterparts. The coupling of relative immaturity of the technology with poor legacy security standards, flawed implementations, limited user awareness, and lax security and administrative practices forms an especially challenging combination. In a wireless environment, data is broadcast through the air and organizations do not have physical controls over the boundaries of transmissions or the ability to use the controls typically available with wired connections. As a result, data may be captured beyond the physical location that the wireless network was intended to serve. Because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high-gain antennas, the distances necessary for positive control for wireless technologies to prevent eavesdropping can vary considerably.

Organizations should carefully plan the deployment of any wireless technology.

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Organizations are more likely to make better security decisions about configuring wireless devices and network infrastructure when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support the inevitable tradeoff decisions between usability, performance, and risk.

[1] NIST SP 800-97 is available at http://csrc.nist.gov/publications/nistpubs/.

Organizations should be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

Appropriate management practices are critical to operating and maintaining a secure wireless network. Security practices entail the identification of an organization's information system assets and the development, documentation and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources.

To support the security of wireless technology, the following security practices should be implemented:

- Organization-wide information system security policy that addresses the use of IEEE 802.11a/b/g, Bluetooth, and other wireless technologies
- Configuration/change control and management to ensure that equipment (such as APs) has the latest software release that includes security feature enhancements and patches for discovered vulnerabilities
- Standardized configurations to reflect the security policy, to ensure change of default values, and to ensure consistency of operation
- Security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" transmission, and that simple theft of equipment is a major concern).

Organizations should be aware that physical controls are especially important in a wireless environment.

Organizations should make sure that adequate physical security is in place. Physical security measures, including barriers, access control systems, and guards, are the first line of defense. Organizations must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices.

Organizations must enable, use, and routinely test the inherent security features, such as authentication and encryption, that exist in wireless technologies. In addition, firewalls and other appropriate protection mechanisms should be employed.

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. As with many newer technologies (and some mature ones), the security features available may not be as comprehensive or robust as necessary. Because the security features provided in some wireless products may be weak, to attain the highest levels of integrity, authentication, and confidentiality, organizations should carefully consider the deployment of robust, proven, and well-developed and implemented cryptography.

The built-in security features of Bluetooth or IEEE 802.11a/b/g should be used as part of an overall defense-in-depth strategy. Although these protection mechanisms have weaknesses described in this publication, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks. However, FIPS 140-2, *Security Requirements for Cryptographic Modules,* is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means. Legacy IEEE 802.11a/b/g and Bluetooth devices may not meet the FIPS 140-2 standard. Therefore, it will be necessary to employ higher-level cryptographic protocols and applications such as secure shell (SSH), Transport Layer Security (TLS), or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to

protect that information, regardless of whether the non-validated data link security protocols are used. However, new products are now available that meet the FIPS 140-2 security requirements; such products should be deployed and implemented as feasible.

Even when federally approved cryptography is used, additional countermeasures such as strategically locating APs, ensuring firewall filtering, and installing antivirus software are typically necessary. Organizations must be fully aware of the residual risk following the application of cryptography and all security countermeasures in the wireless deployment. For example, data link level wireless encryption protects only the wireless subnetwork and not the wired network. Where traffic traverses other network segments, including wired segments or the Internet backbone, higher-level FIPS-validated, end-to-end cryptographic protection may also be required.

Organizations should maintain their secure wireless networks on an ongoing basis.

Maintaining a secure wireless network and associated devices requires significant effort, resources, and vigilance and involves the following steps:

- Maintaining a full understanding of the topology of the wireless network
- Labeling and keeping inventories of fielded wireless devices
- Creating backups of data frequently
- Performing periodic security testing and assessment of the wireless network
- Performing ongoing, randomly timed security audits to monitor and track wireless devices
- Applying patches and security enhancements
- Monitoring the wireless industry for changes to standards that enhance security features and for the release of new products
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to provide organizations with guidance for establishing secure wireless networks. The document provides general information on wireless networks and wireless network security, and specific information on two widely used standards: Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g and IEEE 802.15.1, better known as Bluetooth. Details on securing other wireless networking technologies, such as those based on IEEE 802.11i, are outside the scope of this document. Recommendations for securely using external networks, such as public Internet access points, are also outside the scope of this document; see NIST Special Publication 800-46 version 2 for additional information.

1.3 Audience and Assumptions

This document covers details specific to wireless technologies and solutions. The document is technical in nature; however, it provides the necessary background to fully understand the topics that are discussed.

The following list highlights how people with differing backgrounds might use this document:

- Government managers (e.g., chief information officers, senior managers) who are planning to employ wireless networked computing devices in their organizations
- Systems engineers and architects who design and implement wireless networks
- System and network administrators who administer, patch, secure, or upgrade wireless networks
- Auditors, security consultants, and others who perform security assessments of wireless environments
- Researchers and analysts who are trying to understand the underlying wireless technologies

This document assumes that the readers have at least some operating system, networking, and security expertise. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to these technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information.

1.4 Document Organization

The rest of this document is composed of the following sections and appendices:

- Section 2 provides an overview of wireless technology.
- Section 3 discusses security in general for wireless technology.
- Section 4 examines pre-Robust Security Networks (RSN) IEEE 802.11 WLAN technology, including the benefits and security risks of IEEE 802.11a/b/g, and provides guidelines for mitigating those risks.
- Section 5 examines Bluetooth ad hoc network technology, including its benefits and security risks, and provides guidelines for mitigating those risks.
- Appendix A shows the frequency ranges of common wireless devices.
- Appendix B provides a glossary of terms used in this document.
- Appendix C lists the acronyms and abbreviations used in this document.
- Appendix D describes the differences between the various IEEE 802.11 standards.
- Appendices E and F provide lists of useful printed and online resources, respectively.

2. Overview of Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. The devices simply need to be within a certain distance (known as the *range*) of the wireless network infrastructure or wireless peer to communicate. Radio frequency (RF) transmissions are the means for transmitting data. Wireless technologies range from complex systems, such as cell phone networks and enterprise WLANs to simple devices such as wireless keyboards, mice, and microphones. This section presents a brief overview of wireless networks, devices, standards, and technologies.

2.1 Wireless Networks

There are many forms of wireless networks. A common way of categorizing wireless networks is to consider the relative range and complexity of each type of network. For the purposes of this publication, the major categories of wireless networking architectures are as follows:

- **Wireless personal area network (WPAN):** a small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables. For example, WPANs can provide print services or enable a wireless keyboard or mouse to communicate with a computer. Section 2.4 contains additional information on WPANs.
- **Wireless local area networks (WLAN)** are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility. More information on WLANs is presented in Section 2.3.
- **Wireless metropolitan area networks (WMAN)** can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas. For more information on WMANs, see Section 2.5.
- **Wireless wide area networks (WWAN)** connect individuals and devices over large geographic areas. WWANs are typically used for cellular voice and data communications, as well as satellite communications. Details on WWAN technologies and security are outside the scope of this publication.

Because there are so many types of wireless networks, it is not feasible for this publication to cover each type of wireless networking technology. This section of the publication provides a high-level overview of several of the most commonly used forms of WPANs, WLANs, and WMANs. The rest of the publication provides detailed information on one form of WLAN, IEEE 802.11a/b/g, and one form of WPAN, Bluetooth. Other forms of wireless networking are not covered in depth in this publication.

2.2 Common Wireless Network Components and Topologies

Although there are a number of wireless technologies and devices available on the market, a core set of wireless devices comprise most wireless networks. An overview of each of the core components is included in this section.

2.2.1 Client Devices

Client devices in wireless networks, also referred to as stations (STA), serve as wireless endpoint devices. Client devices enable end users to gain access and utilize resources provided by wireless networks. Common examples of client devices are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with wireless capabilities.

2.2.2 Access Points

An access point (AP) logically connects client devices (STAs) to one another and provides access to the distribution system (DS), if connected, which is typically an organization's enterprise wired network. An AP generally consists of a wired network port (e.g., RJ-45 port) and at least one radio to provide wireless connectivity. IEEE 802.11 based APs typically have coverage areas of up to 300 feet (approximately 100 meters), which primarily depends on a number of characteristics of the device and operating environment. Wireless APs provide users with a mobile capability by allowing users to freely move within an AP's coverage area while maintaining connectivity between the user's client device and the AP. Appropriately configured APs can be linked together using wired infrastructure to allow users to "roam" between APs within a building or campus deployment. APs are most often associated with WLANs, but are also used in some WPAN implementations.

2.2.3 Wireless Bridges

A wireless bridge links two wired networks generally operating at two different physical locations. Bridges are often used to connect two buildings or two networks where a wired link is not feasible or cost efficient. Wireless bridges are similar to APs, but generally only serve to provide point-to-point wireless links. However, some bridges also serve as APs; as an example, some APs use IEEE 802.11 b/g to provide client connectivity and IEEE 802.11a to support a bridge link. A sample use of a wireless bridge would be to connect two adjacent buildings to serve as a redundant backhaul link or serve as the primary backhaul link when wired connectivity is unavailable. Wireless bridges are typically used with WLANs.

2.2.4 Base Stations

A base station or radio transceiver is similar to an AP, but serves a WMAN. A base station is typically a two-way radio installed at a fixed location to provide wireless access. A base station generally covers a much larger physical area than an IEEE 802.11 AP and can serve significantly more clients. The specific range and client support vary by base station vendor and technology.

2.2.5 General Wireless Network Topologies

There are two types of general wireless network topologies, infrastructure and ad hoc. Infrastructure based networks encompass WLANs, cellular networks, and other network types. These types of networks require the use of an infrastructure device, an AP for example, to facilitate communication between client devices.

Ad hoc networks are designed to dynamically connect devices such as cell phones, laptops, and PDAs to each other without the use of any infrastructure devices. These networks are termed ad hoc or peer-to-peer (P2P) because of the network's dynamic topology. Whereas infrastructure networks use a fixed network infrastructure, ad hoc networks maintain dynamic network configurations, relying on peer devices to manage network communication; no infrastructure-based devices are involved in the network. Figure 2-1 illustrates an example of a device connected to infrastructure networks, while simultaneously serving as part of an ad hoc network. The three mobile devices in Figure 2-1—a mobile phone, a laptop

computer, and a PDA—are synchronizing data using Bluetooth technology, while the mobile phone is connected to a cellular network and the laptop computer is attached to an IEEE 802.11-based network.

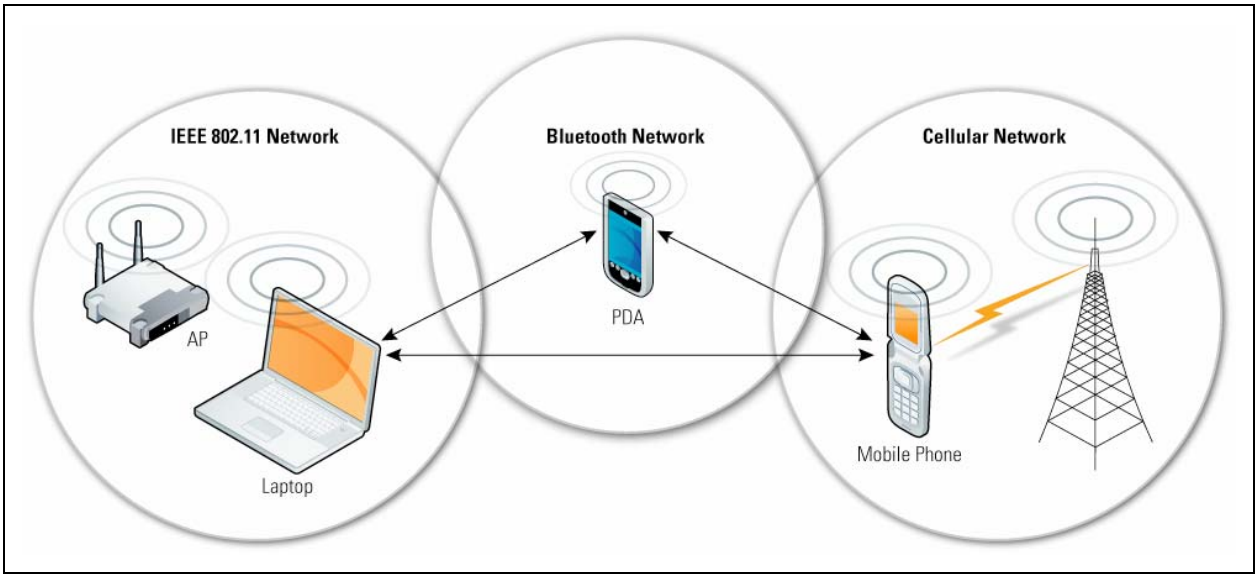

Figure 2-1. Notional Network Topologies

2.3 Wireless Personal Area Networks

WPANs are small-scale wireless networks that require little or no infrastructure. WPANs are typically used by a few devices in a single room to communicate without the need to physically connect devices with cables. A description of common WPAN technologies is included below.

2.3.1 Bluetooth

The Bluetooth specification was developed to facilitate wireless communications between small portable devices and led to the development of the IEEE 802.15.1 standard. Examples include synchronizing a PDA with a computer, providing print services, enabling a wireless keyboard or mouse to communicate with a computer, and allowing a wireless headset or earpiece to be used with a cell phone. All Bluetooth technologies operate at 2.4 GHz ISM band utilizing Frequency Hopping Spread Spectrum (FHSS) technology. Bluetooth v1.1 and v1.2 can achieve a maximum data rate of approximately 720 kilobits per second (Kbps); Bluetooth 2.0 + EDR can reach data rates of 3 Mbps. Section 5 provides detailed background and guidance on securing Bluetooth implementations.

2.3.2 Ultra-Wideband (UWB)

The standard defined in IEEE 802.15.3 is also known as High-Rate Ultrawideband (UWB). UWB is a low-cost, low power consumption standard that uses a wide range of GHz frequencies to avoid interference with other wireless transmissions. It can achieve data rates of up to 480 Mbps over short ranges and can support the full range of WPAN applications. One expected use of this technology is the ability to detect shapes through physical barriers such as walls and boxes, which could be useful for applications ranging from law enforcement to search and rescue operations.

2.3.3 ZigBee

ZigBee is the common name for IEEE 802.15.4, also known as Low-Rate Ultrawideband. ZigBee is a simple protocol for lightweight WPANs.[2] It is most commonly used for monitoring and control products, such as climate control systems and building lighting.

2.4 Wireless Local Area Networks

WLANs are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication. WLANs are usually implemented as an extension to existing wired local area networks to provide enhanced user mobility and network access. IEEE 802.11, also known as Wireless Fidelity (Wi-Fi)®, is the dominant family of WLAN standards, but other standards are also in use, such as High Performance Radio Local Area Network (HIPERLAN) from the European Telecommunications Standards Institute (ETSI). This section briefly describes the most commonly used forms of WLAN technologies: IEEE 802.11a, 802.11b, and 802.11g, collectively known as IEEE 802.11a/b/g; and IEEE 802.11i.

2.4.1 IEEE 802.11a/b/g

In 1997, IEEE ratified the IEEE 802.11 standard for WLANs. The IEEE 802.11 standard supports three transmission methods, including radio transmission within the 2.4 GHz Industrial, Scientific, and Medical (ISM) band. In 1999, IEEE ratified two amendments to the IEEE 802.11 standard—IEEE 802.11a and IEEE 802.11b—that define radio transmission methods and modulation techniques, and WLAN equipment based on IEEE 802.11b quickly became the dominant wireless technology. IEEE 802.11b equipment transmits in the 2.4 GHz band, offering data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance, throughput, and security features comparable to wired LANs. IEEE 802.11a operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) frequency band, delivering data rates up to 54 Mbps.

In 2003, IEEE released the IEEE 802.11g amendment, which specifies a radio transmission method that also uses the 2.4 GHz ISM band and can support data rates of up to 54 Mbps. Additionally, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products. Table 2-1 compares the basic characteristics of IEEE 802.11, 802.11a, 802.11b, and 802.11g. The typical ranges listed in the table will vary significantly in practice, depending on the operating environment (obstacles and material construction) and the equipment used. Outdoor ranges, with high-gain directional antennas, can exceed 20 miles.

Table 2-1. Summary of IEEE 802.11 WLAN Technologies

IEEE Standard or Amendment	Maximum Data Rate	Typical Range	Frequency Band	Comments
802.11	2 Mbps	Up to 91 meters (300 ft) indoors	2.4 GHz (ISM)	
802.11a	54 Mbps	Up to 91 meters (300 ft) indoors	5 GHz (UNII)	Not compatible with IEEE 802.11b
802.11b	11 Mbps	Up to 91 meters (300 ft) indoors	2.4 GHz (ISM)	Equipment based on IEEE 802.11b has been the dominant WLAN technology

[2] The ZigBee Alliance Web site (http://www.zigbee.org/) has additional information on ZigBee.

IEEE Standard or Amendment	Maximum Data Rate	Typical Range	Frequency Band	Comments
802.11g	54 Mbps	Up to 91 meters (300 ft) indoors	2.4 GHz (ISM)	Backward compatible with IEEE 802.11b

The IEEE 802.11 variants[3] listed in Table 2-1 all include security features known collectively as Wired Equivalent Privacy (WEP) that were developed to provide a level of security comparable to that of wired LANs. As described in Section 4, IEEE 802.11 configurations that rely on WEP have several well-documented security problems. The IEEE and the Wi-Fi Alliance acknowledged the scope of the problems and developed short-term and long-term strategies for rectifying the situation. In early 2003, the Wi-Fi Alliance, in coordination with the IEEE 802.11 Working Group, developed the Wi-Fi Protected Access (WPA) security enhancement to replace WEP. This was done as a stopgap measure until a robust IEEE 802.11 security standard could be developed and approved. In June 2004, the IEEE finalized the 802.11i amendment, which was designed to overcome the shortcomings of WEP, enhance WPA, and provide IEEE 802.11 based wireless networks with a robust security mechanism. IEEE 802.11i specifies security components that work in conjunction with all the IEEE 802.11 radio transmission standards and modulation techniques, such as IEEE 802.11a, 802.11b, and 802.11g; any future IEEE 802.11 standard will also be compatible with IEEE 802.11i. Sections 3 and 4 present additional information on WLAN security issues.

2.4.2 IEEE 802.11i / WPA2

The IEEE 802.11i standard is the sixth amendment to the original IEEE 802.11 standard. It includes many security enhancements that leverage mature and proven security technologies. For example, IEEE 802.11i references the Extensible Authentication Protocol (EAP) standard, which is a means for providing mutual authentication between wireless clients and the WLAN infrastructure, as well as performing automatic cryptographic key distribution. In addition, IEEE 802.11i employs accepted cryptographic practices, such as generating cryptographic checksums through hash message authentication codes (HMAC).

The IEEE 802.11i specification introduces the concept of a Robust Security Network (RSN). An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA). An RSNA is a logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, which is called the 4-Way Handshake. The handshake is a protocol that validates that both entities share a master key, synchronizes the installation of temporal keys, and confirms the selection and configuration of data confidentiality and integrity protocols. The master key, known as the pairwise master key (PMK), serves as the basis for the IEEE 802.11i data confidentiality and integrity protocols that provide enhanced security over the flawed WEP from earlier versions of IEEE 802.11.

WPA2 is the Wi-Fi Alliance interoperable specification for IEEE 802.11i. Organizations that are considering the deployment of new WLANs should be evaluating IEEE 802.11i/WPA2-based products and following the recommendations for IEEE 802.11i/WPA2 implementations presented in NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*.[4] The recommendations in NIST SP 800-97 should also be applied to existing IEEE 802.11i WLAN implementations.

[3] For information on other IEEE 802.11 amendments (e.g., 802.11e, 802.11n), visit http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm.

[4] NIST SP 800-97 is available at http://csrc.nist.gov/publications/nistpubs/.

2.4.3 Other IEEE 802.11 Standards

Sections 2.3.1 and 2.3.2 only include the major IEEE 802.11 access technologies and IEEE 802.11i, all other current and pending IEEE 802.11 amendments and standards are not included in these sections. For example, in November 2005, the IEEE ratified IEEE 802.11e, which provides quality-of-service (QoS) enhancements to improve the delivery of multimedia content over IEEE 802.11 based wireless networks. The IEEE 802.11n project is specifying IEEE 802.11 enhancements that will enable data throughput of at least 100 Mbps. Final working group approval of IEEE 802.11n is expected in 2008, with an interim Wi-Fi® certification some time in 2007; however, products based on the IEEE 802.11n draft are already available. Additional detail on these and other pending IEEE 802.11 standards is located in Appendix D.

2.5 Wireless Metropolitan Area Networks

WMANs can provide connectivity to users located in multiple facilities, generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas. The most commonly used standard for WMANs is IEEE 802.16, better known as World Interoperability for Microwave Access (WiMAX).[5] The two main types of WiMAX technology are described below.

2.5.1 Fixed WiMAX (IEEE 802.16-2004)

Fixed WiMAX, or IEEE 802.16-2004, is the standard for high-bandwidth broad coverage wireless technology. Fixed WiMAX uses Orthogonal Frequency Division Multiplexing (OFDM) to provide a non-line-of-sight (NLOS) wireless connectivity. WiMAX has a range of about 30 miles for line-of-sight (LOS) coverage, and about 5 miles for NLOS-based connectivity. The range of each of these types of networks depends on a number of environmental conditions. Fixed WiMAX operates within various GHz frequency bands and, based on optimal conditions, the technology can provide data rates up to 75 Mbps. The range and bandwidth of fixed WiMAX position this technology as an emerging backhaul or "last mile" type technology.

2.5.2 Mobile WiMAX (IEEE 802.16e-2005)

In December 2005, the IEEE ratified IEEE 802.16-2005, or Mobile WiMAX, as an amendment to the IEEE 802.16-2004 standard. The amendment added necessary specifications to the standard to add support for mobility. Mobile WiMAX will operate within various GHz frequency bands and employ the use of Orthogonal Frequency Division Multiple Access (OFDMA) for increased performance in NLOS environments, and scalable OFDMA (SOFDMA) to support scalable channel bandwidth. Both technologies serve as enablers to providing the mobile capability to IEEE 802.16e.

2.5.3 Other WMAN Technologies and Standards

Other WMAN technologies include the plethora of current cellular standards, which includes higher data rate 3G and emerging 4G technologies. Although cellular technology somewhat differs from other WMAN technologies, current cellular technologies are one of the best examples of WMANs implemented today. The IEEE is currently working to develop two additional wireless standards that will support WMAN capabilities. The IEEE 802.20 working group is working towards developing an additional WMAN standard to address broadband access for vehicular mobility, while the IEEE 802.11s working group is seeking to develop a mesh wireless standard utilizing IEEE 802.11 based technologies. However, ratification for each of these standards is still several years away. Other proprietary bridging,

[5] Information on the IEEE 802.16 working group is available at http://www.ieee802.org/16/.

point-to-point (PtP), and mesh technologies also exist that utilize microwave technologies, IEEE 802.11, Free Space Optics (FSO), and other technologies.

2.6 Summary

Table 2-2 summarizes the wireless networking architectures presented in Section 2, highlighting their typical applications and sample usage scenarios.

Table 2-2. Summary of Wireless Networking Architectures

Wireless Networking Architecture	Typical Application	Sample Usage Scenarios
WPAN	Short range ad hoc or peer-to-peer network configurations	• Used to pair a mobile device, such as a cellular phone, with a headset for hands-free communication or a laptop to transfer data • Bluetooth enabled mice and keyboards can be used instead of wired input devices
WLAN	Used to extend the range of a wired network or provide network access where wired connections are not feasible	• Deployed as an extension to an enterprise wired network to offer users mobile capability and access to network resources in conference rooms and other common areas where wired connections are not available • WLANs can be used to provide network access to users in temporary office environments in order to alleviate the burden and costs of deploying a wired network
WMAN	Provide high-speed data services to broad coverage areas, such as metropolitan environments	• Provide the capability to wirelessly link buildings within a campus type area on either a point-to-point or point-to-multipoint configuration • Used by cellular carriers to provide broadband data services to coverage areas that include a high number of mobile users
WWAN	Large scale wireless networks that support a broad footprint and a high number of users	• WWANs are best exemplified by cellular networks, including those that support high speed data transmissions

3. Overview of Wireless Network Security

This section provides a high-level overview of general wireless network security. The information in this section is intended to apply to many types of wireless networks. It first lists the security objectives for wireless networks and the most common threats against those objectives. Next, it discusses the high-level process for selecting security controls and highlights several types of controls commonly used to protect wireless communications. Finally, the section maps security-related considerations to the phases of the life cycle for wireless networks.

3.1 Security Needs for Wireless Networks

Wireless technologies typically need to support several security objectives. The most common security objectives for wireless networks are as follows:

- **Confidentiality—**ensure that communication cannot be read by unauthorized parties
- **Integrity—**detect any intentional or unintentional changes to data that occur in transit
- **Availability—**ensure that devices and individuals can access a network and its resources whenever needed
- **Access Control—**restrict the rights of devices or individuals to access a network or resources within a network**.**

The security objectives for wireless and wired networks are the same, as are the major high-level categories of threats that they face. Table 3-1 provides a list of these categories.

Table 3-1. Major Threats Against Network Security

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

Most threats against wireless networks involve an attacker with access to the radio link between wireless devices. Several of the threats listed in Table 3-1 rely on an attacker's ability to intercept and inject network communications. This highlights the most significant difference between protecting wireless and wired networks: the relative ease of intercepting wireless network transmissions and inserting new or altered transmissions from what is presumed as the authentic source. For a wired network, an attacker would have to gain physical access to the network or remotely compromise systems on the network; for a wireless network, an attacker simply needs to be within range of the wireless transmissions, making eavesdropping a particularly prevalent threat. (Some attackers use highly sensitive directional antennas,

which can greatly extend the effective range of the wireless network beyond the standard range.) Another consideration in threats against wireless networks is that in many cases, a wireless network is logically connected to a wired network, so the wireless network needs to be secured against both the threats that wired networks typically face and the threats that are specific to wireless networks.

In addition to eavesdropping, another common threat against wireless networks is the deployment of rogue wireless devices. For example, an attacker could deploy a device, most likely an AP, that has been configured to appear as part of an organization's wireless network infrastructure. This provides a backdoor into the wired network, bypassing perimeter security mechanisms, such as firewalls. Additionally, if clients inadvertently connect to the rogue device, the attacker can view and manipulate the clients' communications. DoS situations are another threat; examples are flooding (an attacker sends large numbers of messages at a high rate to prevent the wireless network from processing legitimate traffic) and jamming (a device emits electromagnetic energy on the wireless network's frequency to make it unusable). Jamming often occurs unintentionally; for example, microwave ovens, cordless phones, and other devices share bandwidth with certain wireless technologies, and the devices' operation can inadvertently make wireless networks in proximity unusable.

3.2 Security Controls for Wireless Networks

To mitigate the risks posed by these threats, organizations need to adopt security measures and practices that help bring risks to a manageable level. Organizations need, for example, to perform security assessments prior to implementation to determine the specific threats and vulnerabilities that wireless networks will introduce into their environments. In performing the assessment, organizations should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the organization can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing.

Organizations should develop their wireless network security controls based on existing guidance on security controls. FIPS Publication (PUB) 199 establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. NIST SP 800-53 provides recommendations for minimum management, operational, and technical security controls for information systems based on the FIPS PUB 199 impact categories.[6] The recommendations in NIST SP 800-53 should be helpful to organizations in identifying controls that are needed to protect networks and systems, which should be used in addition to the specific recommendations for wireless networks listed in this document. An explanation of securing laptops, PDAs, and other devices that use wireless networks is outside the scope of this guide.

Various operational and technical controls need to be implemented to protect a wireless network. For some network technologies, this is intended to be accomplished primarily through security features built into a wireless network standard; for other technologies, compensating controls need to provide all of the protection. Proprietary solutions are available that can be used to implement more robust security on legacy IEEE 802.11a/b/g WLANs. Commonly used types of security controls for wireless networks are as follows:

[6] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at http://csrc.nist.gov/publications/fips/. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, is available at http://csrc.nist.gov/publications/nistpubs/.

- **Encryption of communications.** Using cryptography to encrypt wireless communications prevents exposure of data through eavesdropping.[7]
- **Cryptographic hashes for communications.** Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit, either intentionally or unintentionally. This prevents masquerading and message modification attacks.
- **Device authentication and data origin authentication.** Authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading.
- **Replay protection.** There are several options to implement the detection of message replay, including adding incrementing counters, timestamps, and other temporal data to communications.
- **Physical security.** Limiting physical access within the range of the wireless network prevents some jamming and flooding attacks.
- **Wireless intrusion detection and prevention systems (IDPS).** Wireless IDPSs have the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Wireless IDPSs are most commonly used for IEEE 802.11a/b/g WLANs, but they are also available for Bluetooth networks, and they can also detect rogue networks that use uncommon frequencies, such as those used in other countries, in an attempt to avoid detection.[8]

In addition to these controls, organizations need to create a wireless network security policy that addresses each type of wireless network technology of interest. The policy should identify such things as who may or may not use the technology, who may install equipment, where the technology may be used, what the physical security requirements are for the technology, what types of information may or may not be sent and received through the technology, how security incidents should be reported, how wireless devices should be protected, how transmissions should be protected (e.g., encryption requirements), and how often the security of the implementation should be assessed. Organizations also need to ensure that all critical personnel are properly trained on the use of the wireless technology. Network administrators need to be fully aware of the security risks that the networks and associated devices pose, and they need to know what steps to take in the event of an incident. Users also need to be aware of their responsibilities in using wireless technologies.

3.3 Security in the Wireless Network Life Cycle

To be effective, wireless network security should be incorporated throughout the entire life cycle of wireless network solutions, involving everything from policy to operations. This section references a five-phase life cycle model to help organizations determine at what point in their wireless network deployments a recommended practice might be relevant. The model below is based on the model introduced in NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle.*[9] Organizations may follow a project management methodology or life cycle model that does not directly map to the phases in the model presented here, but the types of tasks in the methodology and their sequencing are probably similar. The phases of the life cycle are as follows:

---

[7] Federal agencies are required to use Federal Information Processing Standards (FIPS)-validated cryptography when protecting the confidentiality or integrity of data. The Cryptographic Module Validation Program (CMVP) performs validation testing of cryptographic modules. More information on cryptographic requirements is available at http://csrc.nist.gov/cryptval/.

[8] More information on wireless IDPS is available from NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, which is available at http://csrc.nist.gov/publications/nistpubs/.

[9] This document is available at http://csrc.nist.gov/publications/nistpubs/.

- **Phase 1: Initiation**. This phase includes the tasks that an organization should perform before it starts to design its wireless network solution. These include developing a wireless network use policy, performing a wireless network risk assessment, and specifying business and functional requirements for the solution.

- **Phase 2: Acquisition/Development.** For the purposes of this guide, the Acquisition/Development phase is split into the following two phases:

  - **Phase 2a: Planning and Design**. In this phase, wireless network architects specify the technical characteristics of the solution, such as authentication methods, and related network components, such as access control lists and firewall rules to segregate wireless network traffic from wired network traffic. The network architects should also conduct a site survey to help determine the architecture of the solution. A review of the wireless network should also be conducted to determine how it will be integrated with existing infrastructures, such as authentication servers and public key infrastructures (PKI).

  - **Phase 2b: Procurement**. This phase involves specifying the number and type of wireless network components that must be purchased, the feature sets they must support (e.g., FIPS-validated encryption modules), and any certifications they must hold.

- **Phase 3: Implementation**. In this phase, procured equipment is configured to meet operational and security requirements, and then installed and activated on a production network. Implementation includes altering the configuration of other security controls and technologies, such as security event logging, network management, AAA servers, and PKI.

- **Phase 4: Operations/Maintenance**. This phase includes security-related tasks that an organization should perform on an ongoing basis once the wireless network is operational, including patching, periodic security assessments, log reviews, and incident handling.

- **Phase 5**: **Disposition.** This phase encompasses 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 information, and disposing of equipment properly.

The details listed for these phases are most applicable to larger-scale wireless networks. For small implementations, such as most WPANs, the phases still apply but some details may not—for example, site surveys or integration with the wired network and security infrastructures may not be necessary.

4. Wireless Local Area Networks

This section provides a detailed overview of IEEE 802.11-based WLAN technology. The section includes introductory material on the history of IEEE 802.11 and provides other technical information, including IEEE 802.11 frequency ranges, data rates, network topologies, transmission ranges, and applications. Additionally, this section examines the security threats and vulnerabilities associated with WLANs and offers various means for reducing risks and securing WLAN environments.

4.1 Wireless Local Area Network Overview

WLAN technology and the WLAN industry date back to the mid-1980s when the Federal Communications Commission (FCC) first made the RF spectrum available to private industry. During the 1980s and early 1990s, growth was relatively slow. However, today WLAN technology is experiencing tremendous growth. The key reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standards. Table 4-1 provides some additional characteristics at a glance and serves as an introduction to the IEEE 802.11 standards and WLAN technology.

4.1.1 Brief History

WLAN technologies were first available in late 1990, when vendors began introducing products that operated within the 900 megahertz (MHz) frequency band. These solutions, which used non-standard, proprietary designs, provided data transfer rates of approximately 1 Mbps. This was significantly slower than the 10 Mbps speed provided by most wired local area networks (LAN) at that time.

In 1992, vendors began selling WLAN products that used the 2.4 GHz ISM band. Although these products provided higher data transfer rates than 900 MHz band products, they also used proprietary designs and had several problems that prohibited pervasive use. These WLANs were expensive, provided low data rates, were prone to radio interference, and were often designed to use proprietary RF technologies. The IEEE initiated the IEEE 802.11 project in 1990 with the objective to "develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." In 1997, IEEE first approved the IEEE 802.11 international interoperability standard. Then, in 1999, the IEEE ratified the IEEE 802.11a and the IEEE 802.11b wireless networking communication standards. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications. For the latest developments on the status of each specification, the reader is encouraged to refer to the IEEE 802.11 standards Web site[10] and Appendix D.

4.1.2 Frequency and Data Rates

The IEEE developed the IEEE 802.11 standards to provide standardized wireless networking technologies that would achieve speeds similar to traditional wired Ethernet networks. The popular IEEE 802.11b standard operates in the unlicensed 2.4 GHz ISM frequency band using a direct sequence spread-spectrum (DSSS) technology. The ISM band has become popular for wireless communications because it is unlicensed and available worldwide. The IEEE 802.11b WLAN technology permits data rates up to 11 Mbps. The IEEE 802.11a standard operates in the unlicensed 5 GHz UNII band using OFDM technology and provides data rates up to 54 Mbps. IEEE 802.11g is the latest IEEE 802.11 wireless access standard and also provides data rates up to 54 Mbps using OFDM technology. However, unlike IEEE 802.11a, IEEE 802.11g operates in the 2.4 GHz ISM band, making it backward compatible with IEEE 802.11b. Backward compatibility and a higher overall data rate were two major goals of the IEEE 802.11g standard

[10] See http://standards.ieee.org/getieee802 for the latest developments on the IEEE 802.11 standards.

working group. Table 4-1 below provides the data rates and frequency bands of the IEEE 802.11 based wireless access technologies. The operating ranges in Table 4-1 will vary significantly in practice, depending on the operating environment (obstacles and material construction) and the equipment used: outdoor ranges, with high-gain directional antennas, can exceed 20 miles. A summary of all of the various IEEE 802.11 standards is provided in Appendix D.

Table 4-1. Key Characteristics of IEEE 802.11 WLAN Access Technologies

Characteristic	IEEE 802.11	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a
Physical Layer	Frequency Hopping Spread Spectrum (FHSS) and Infrared (IR)	DSSS	OFDM and DSSS to support backwards compatibility with IEEE 802.11b	OFDM
Frequency Band	2.4 GHz (ISM band)	2.4 GHz (ISM band)	2.4 GHz (ISM band)	5 GHz (UNII band)
Maximum Data Rates	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Operating Range	Up to 91 meters (300 ft) indoors	Up to 91 meters (300 ft) indoors	Up to 91 meters (300 ft) indoors	Up to 91 meters (300 ft) indoors
Comments	Legacy technology that is minimally used.	Provides close to 10Base-T Ethernet speeds and is generally combined with IEEE 802.11g in product offerings as IEEE 802.11b/g.	Provides better than 10Base-T Ethernet speeds and is backwards compatible with IEEE 802.11b. Due to the backwards compatibility support and signal radio requirement, most wireless products now support IEEE 802.11b/g.	Provides better than 10Base-T Ethernet speeds and is not compatible with any other IEEE 802.11 access standard because it operates in the less crowded 5 GHz band.

4.1.3 IEEE 802.11 Network Components and Architectural Models

IEEE 802.11 has two fundamental architectural components, listed below. Additional WLAN components are outlined in Section 2.2.

- **Station (STA).** A *STA* is a wireless endpoint device. Typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with IEEE 802.11 capabilities.
- **Access Point (AP).** [11] An *AP* logically connects STAs with a distribution system (DS), which is typically an organization's wired infrastructure. APs can also logically connect wireless STAs with each other without accessing a distribution system.

The IEEE 802.11 standard permits STA to establish either ad-hoc/peer-to-peer (P2P) networks that allow STAs to communicate with one another or infrastructure networks that require STAs to use an AP to communicate. Infrastructure mode and ad hoc mode are the two basic network topologies defined in the

[11] Technically, APs are also STAs. Some literature distinguishes between AP STAs and non-AP STAs. In this document, the term STA refers to non-AP STAs only.

IEEE 802.11 standard. An infrastructure network can extend the range of a wired LAN by providing service to a much broader physical area or serve as a temporary or low-cost networking option in certain situations. The standard IEEE 802.11 wireless network architectures are outlined below and are discussed in more detail in Sections 4.1.3.1 and 4.1.3.2.

- **Ad Hoc Mode.** The *ad hoc mode* does not use APs. Ad hoc mode is sometimes referred to as peer-to-peer mode, because only STAs are involved in the communications.
- **Infrastructure Mode.** In *infrastructure mode*, an AP connects wireless STAs to each other or to a distribution system, typically a wired network. Infrastructure mode is the most commonly used mode for WLANs.

4.1.3.1 Ad Hoc Mode

The ad hoc mode (or topology) is depicted conceptually in Figure 4-1. This mode of operation, also known as *peer-to-peer mode*, is possible when two or more STAs are able to communicate directly to one another. Figure 4-1 shows three devices communicating with each other in a peer-to-peer fashion without any wireless infrastructure or wired connections. A set of STAs configured in this ad hoc manner is known as an *independent basic service set* (IBSS).

Today, a STA is most often thought of as a simple laptop with an inexpensive wireless network interface card (NIC) that provides wireless connectivity. However, as IEEE 802.11 and its variants continue to increase in popularity, many other types of devices could also be STAs, such as scanners, printers, and digital cameras. Figure 4-1 depicts a sample IBSS that includes a mobile phone, laptop, and a PDA communicating via IEEE 802.11 technology. The circle in Figure 4-1 represents the signal range of the devices, which is important to consider because this determines the coverage area within which the stations can remain in communication. A fundamental property of IBSS is that it defines no routing or forwarding, so all the devices must be within radio range of one another.

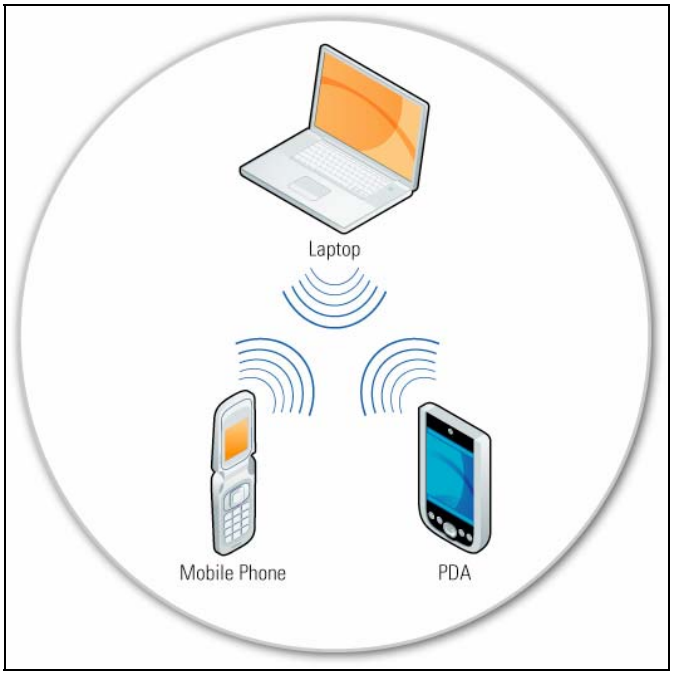

Figure 4-1. IEEE 802.11 Ad Hoc Mode Architecture

One of the key advantages of ad hoc WLANs is that theoretically they can be formed any time and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. In practice, many different types of ad hoc networks are possible, and the IEEE 802.11 specification allows many of them. An ad hoc network can be created for many reasons, such as supporting file sharing activities between two client devices. However, client devices solely operating in ad hoc mode cannot communicate with external wireless networks. A further complication is that an ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space.

4.1.3.2 Infrastructure Mode

In infrastructure mode, an IEEE 802.11 WLAN comprises one or more Basic Service Sets (BSS), the basic building blocks of a WLAN. A *BSS* includes an AP and one or more STAs. The AP in a BSS connects the STAs to the DS. The DS is the means by which STAs can communicate with an organization's wired LANs and external networks, such as the Internet. The IEEE 802.11 infrastructure mode is outlined in Figure 4-2 below by two BSSs connected to a DS.

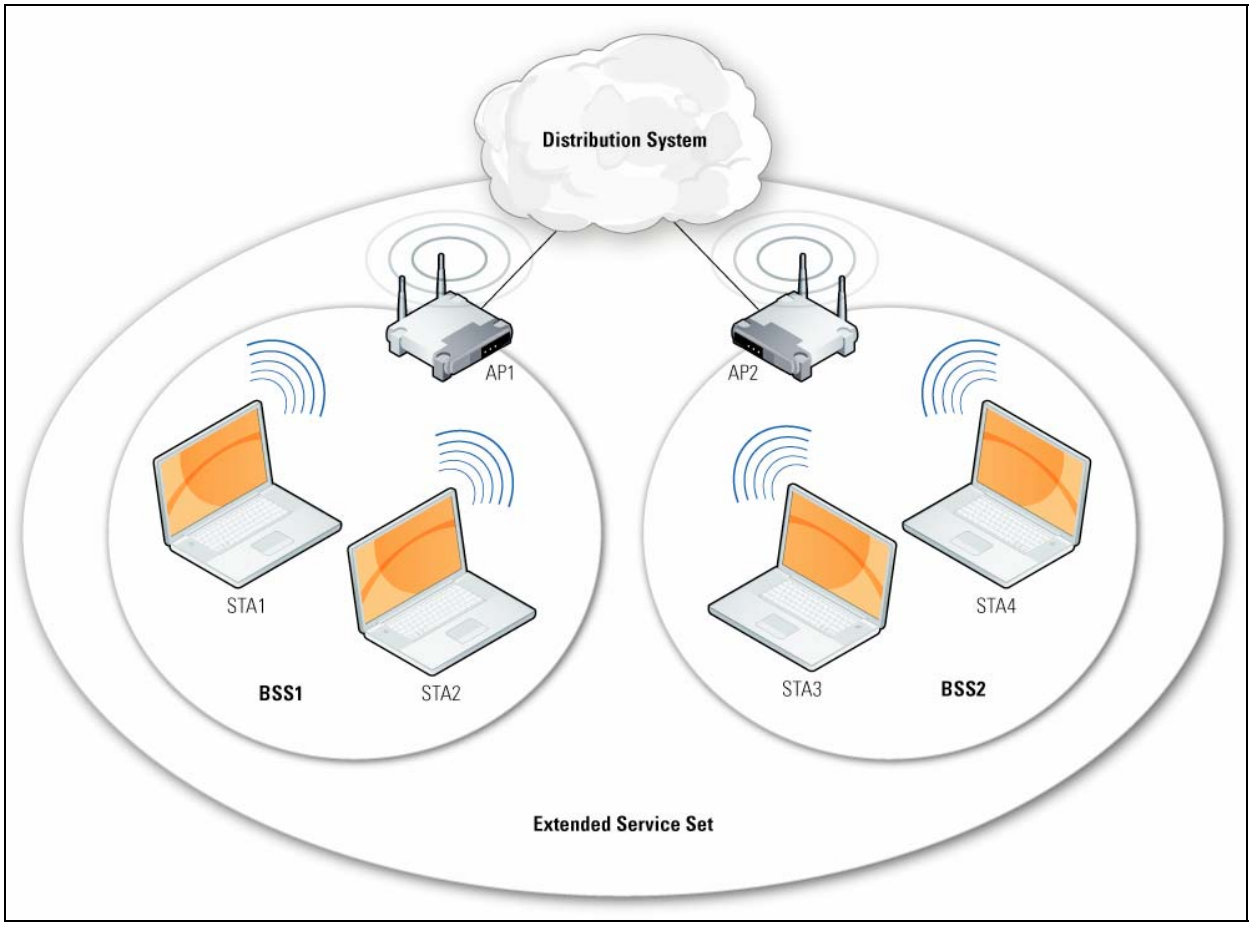

Figure 4-2. IEEE 802.11 Infrastructure Mode

The use of multiple APs connected to a single DS allows for the creation of wireless networks of arbitrary size and complexity. In the IEEE 802.11 specification, a multi-BSS network is referred to as an *extended service set* (ESS). Figure 4-3 conceptually depicts a network with both wired and wireless capabilities, similar to what would generally be deployed in an enterprise environment. It shows three APs with

corresponding BSSs, which comprise an ESS, The ESS is attached to the wired enterprise network or DS, which, in turn is connected to the Internet and other outside networks. This architecture could permit various STAs, such as laptops and PDAs, to access network resources and the Internet. Additionally, the use of an ESS provides the opportunity for IEEE 802.11 WLAN STAs to roam between APs while maintaining network connectivity.

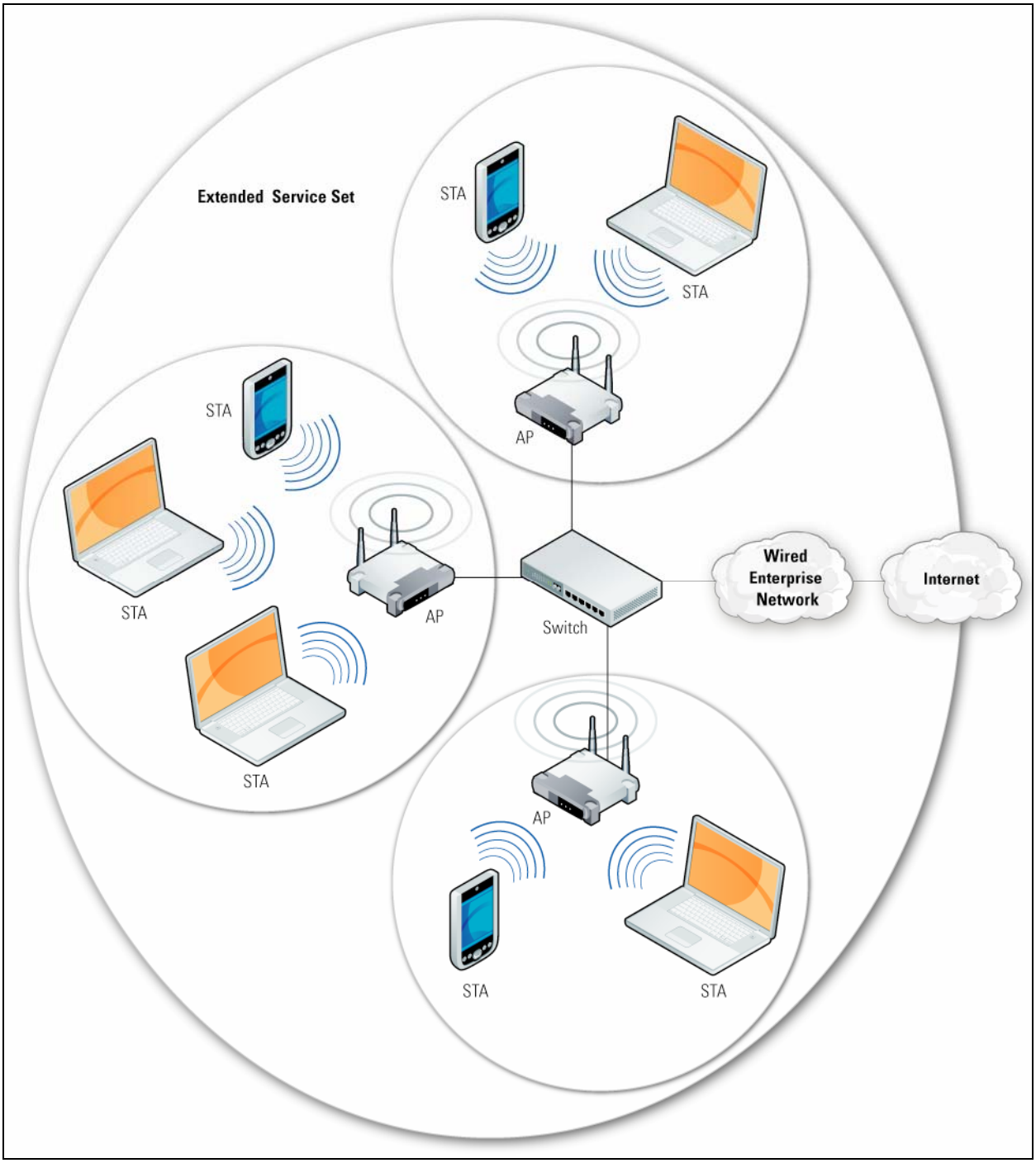

Figure 4-3. Extended Service Set in an Enterprise

4.1.4 Wireless Local Area Network Range and Use

The reliable coverage range for IEEE 802.11 WLANs depends on several factors, including data rate requirements and capacity, sources of RF interference, physical area characteristics, power, connectivity, and antenna usage. The typical range for connectivity of IEEE 802.11a/b/g equipment is up to 91 meters (about 300 ft.) indoors, with significantly greater ranges achievable outdoors. Increased power output and special high-gain antennas can increase the range of IEEE 802.11a/b/g devices to several miles.

APs may also provide a bridging function that connects two or more networks together and allows them to communicate via the wireless radio. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two wired LANs are connected to each other via each LAN's wireless bridging device. In multipoint bridging, one subnet on a wired LAN is connected to several other subnets on another wired LAN via each subnet's bridging device, eliminating the need for wired links. For example, if a computer on network A needed to connect to computers on networks B, C, and D, network A's wireless bridging device would connect to B's, C's, and D's respective wireless bridging devices.

Enterprises may use bridging to connect wired LANs between different buildings on corporate campuses. Bridging devices are typically placed on top of buildings to achieve greater antenna reception. Typical bridges may extend for several miles, but may vary depending on several factors including the specific receiver or transceiver being used, power-output, antenna type, and environmental conditions. Figure 4-4 illustrates a point-to-point wireless bridging between two wired LANs located in two separate buildings. In the example, wireless data is being transmitted from a client device in Building A to a client device in Building B, using each building's appropriately positioned bridging device to transmit and receive data between the two buildings. A client device in Building A connects to the wired enterprise network located in Building A, which then transmits any data intended for a client device in Building B over the wireless bridged link. Any data intended for a client device in Building A originating from a client device in Building B will be sent by Building B's wired LAN to the wireless bridging device and transmitted to Building A's wireless bridging device, which then passes the data on to Building A's wired enterprise network and finally to a client device in Building A. This sequence takes place for all data traversing the bridge link.

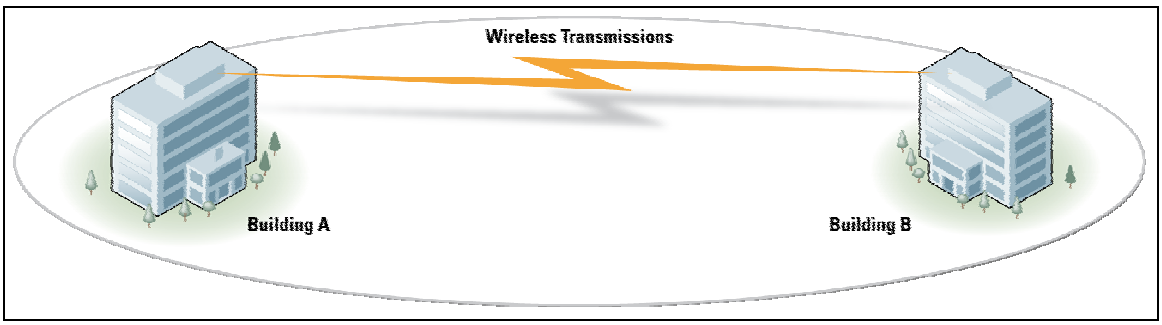

Figure 4-4. Access Point Bridging

4.2 Benefits of Wireless Local Area Networks

WLANs offer users and organizations a number of benefits, including the following four primary benefits:

- **User Mobility.** Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN and network resources.
- **Rapid Installation.** The time required for installation is reduced because network connections can be made without moving or adding wires or pulling them through walls or ceilings, or making modifications to the infrastructure cable plan. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules.
- **Flexibility.** Enterprises can also enjoy the flexibility of installing and removing WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, meeting, or Continuity of Operations (COOP) activities.
- **Scalability.** WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

Because of these fundamental benefits, the WLAN market has been increasing steadily over the past several years, and WLANs are still gaining in popularity. WLANs are now becoming a viable alternative to traditional wired solutions in some cases. For example, hospitals, universities, airports, hotels, and retail shops are using wireless technologies to conduct daily business operations.

4.3 Securing Non-IEEE 802.11i Wireless Local Area Networks

This section discusses the legacy security features included in the IEEE 802.11 standard, and does not include security recommendations for IEEE 802.11i capable networks. It provides an overview of the security features available in non-IEEE 802.11i WLANs in order to illustrate limitations, outline guidance, and provide motivation for use of the enhanced security recommendations. The IEEE 802.11 specification identifies several services to provide a secure communications link. The security services are provided largely by the Wired Equivalent Privacy (WEP), WPA, and WPA2 to protect link-level data during wireless transmission between clients and AP. WEP, WPA, and WPA2 do not provide end-to-end security; the protocol only provides limited security for the wireless link between the IEEE 802.11 AP and STA as shown in Figure 4-5.

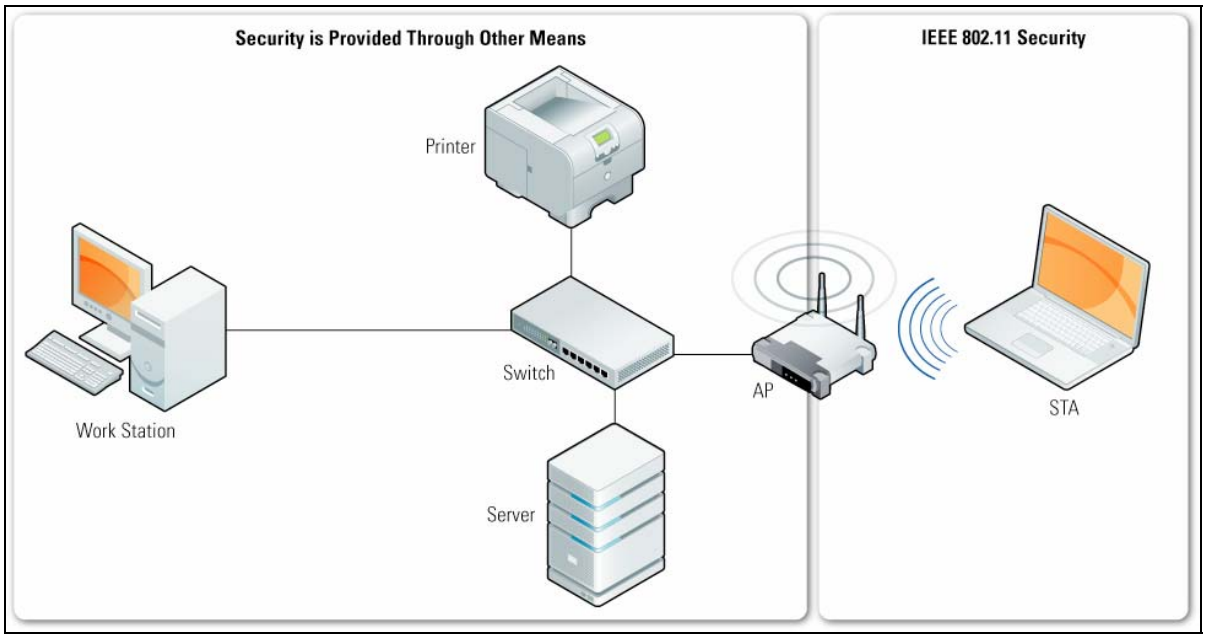

Figure 4-5. WEP Security of an IEEE 802.11 Network

Organizations that are considering the deployment of new WLANs or have WLANs capable of supporting IEEE 802.11i should follow the recommendations for IEEE 802.11i implementations presented in NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.*[12] The recommendations in NIST SP 800-97 should also be applied to existing IEEE 802.11i WLAN implementations.

4.3.1 Security Features of IEEE 802.11 Wireless Local Area Networks per the Standard

Although WEP has a number of known security vulnerabilities, the protocol was designed by the IEEE to provide the following three basic security services:

- **Authentication**—A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly.
- **Confidentiality—**Confidentiality, or privacy, through the use of encryption was a second goal of WEP. It was developed to provide the wireless networks with the same or similar privacy achieved by a wired network. The intent was to prevent information compromise from casual eavesdropping (passive attack).
- **Integrity**—Another goal of WEP was to provide a security service to ensure that messages are not modified in transit between wireless clients and APs in an active attack.

It is important to note that the standard did not address other security services such as audit, authorization, replay protection, key management, and nonrepudiation. The security services and vulnerabilities of IEEE 802.11 based security are described in greater detail below.

[12] NIST SP 800-97 is available at http://csrc.nist.gov/publications/nistpubs/.

4.3.1.1 Access Control and Authentication

The original IEEE 802.11 specification defines two means to validate the identities of wireless devices attempting to gain access to a WLAN, open system authentication and shared key authentication; neither of these alternatives is secure.[13] IEEE 802.11 implementations are required to support open system authentication; shared key authentication support is optional. Open system authentication is effectively a null authentication mechanism that does not provide true identity verification. In practice, a STA is authenticated to an AP simply by providing the following information:

- **Service Set Identifier (SSID) for the AP.** The *SSID* is a name assigned to a WLAN; it allows STAs to distinguish one WLAN from another. SSIDs are broadcast in plaintext in wireless communications, so an eavesdropper can easily learn the SSID for a WLAN. However, the SSID is not an access control feature, and was never intended to be used for that purpose.
- **Media Access Control (MAC) address for the STA.** A *MAC address* is a unique 48-bit value that is assigned to a particular wireless network interface by the network card's vendor. Many implementations of IEEE 802.11 allow administrators to specify a list of authorized MAC addresses; the AP will permit devices with those MAC addresses only to use the WLAN. This is known as *MAC address filtering.* However, since the MAC address is not encrypted, it is simple to intercept traffic and identify MAC addresses that are allowed past the MAC filter. Unfortunately, almost all WLAN adapters allow applications to set the MAC address, so it is relatively trivial to spoof a MAC address, meaning attackers can gain unauthorized access easily.

Additionally, the AP is not authenticated to the STA by open system authentication. Therefore, the STA has to trust that it is communicating to a trusted AP and not a rogue AP that is using the same SSID. Therefore, open system authentication does not provide reasonable assurance of any identities, and can be easily used by an attacker to gain unauthorized access to a WLAN or trick users into connecting to a malicious WLAN.

Shared key authentication was designed to be more robust than open system authentication, but in fact, it is equally insecure. As the name implies, shared key authentication is based on pre-shared secret cryptographic keys known as WEP keys, which are shared by legitimate STAs and APs. (WEP is described in more detail in Section 4.3.1.2.) Shared key authentication uses a simple challenge-response scheme based on whether the STA seeking WLAN access knows the WEP key. As shown in Figure 4-6, the STA initiates an Authentication Request with the AP, and the AP generates a random 128-bit challenge value and sends it to the STA. Using the WEP key, the STA encrypts the challenge and returns the result to the AP. The AP decrypts the result using the same WEP key and allows the STA access only if the decrypted value is the same as the challenge. The cryptographic computations are performed using the RC4 stream cipher algorithm, which generates a pseudo-random data sequence known as a *key stream*. To encrypt or decrypt data, the key stream is mathematically applied to the data.

[13] The shared key authentication scheme based on a unilateral challenge-response mechanism is typically referred to as WEP because it uses the WEP encryption for response computation. However, shared key authentication is actually a simple authentication scheme independent of WEP. Also, it does not work. WEP encrypts the response by XORing the challenge with a pseudo-random key stream generated using a WEP key. The attacker can XOR the challenge and the response to expose the key stream, which can subsequently be used to authenticate.

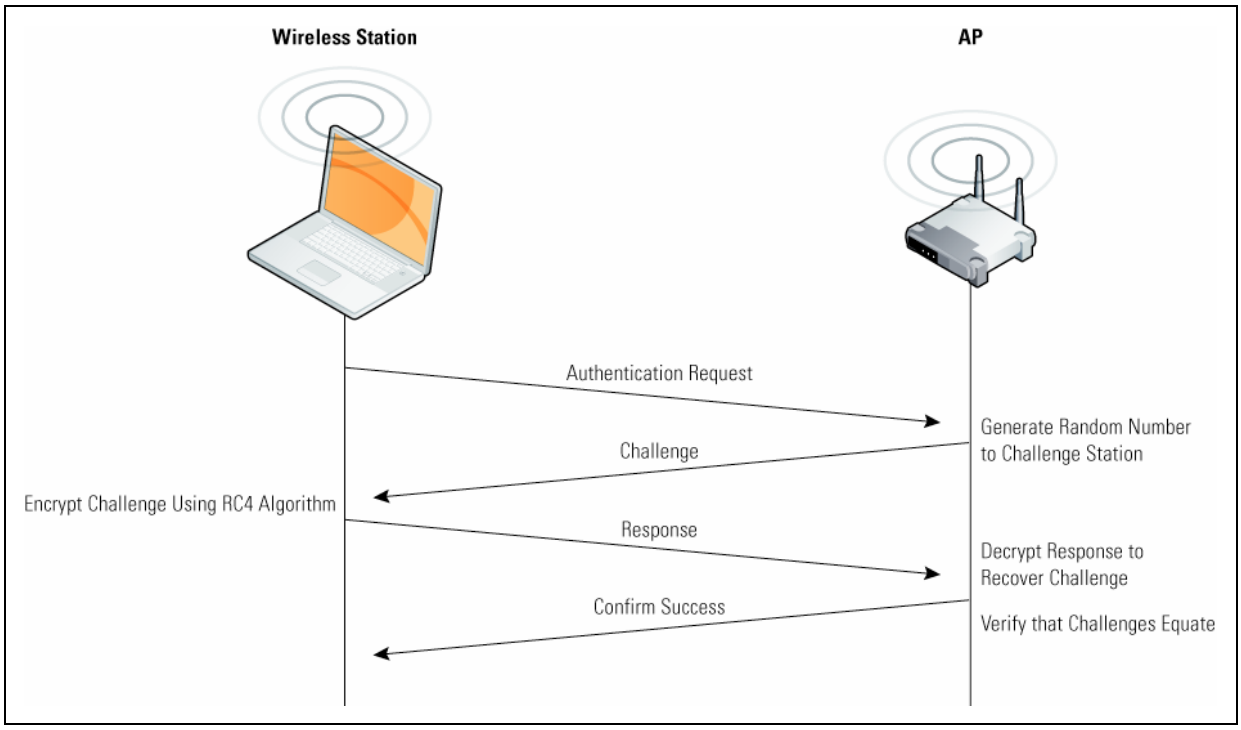

Figure 4-6. Shared Key Authentication Message Flow

Shared key authentication is still weak because the AP is not authenticated to the STA, so there is no assurance that the STA is communicating with a legitimate AP. Also, simple unilateral challenge-response schemes have long been known to be weak unless they are carefully designed with sufficient entropy in the challenge, keys of the appropriate length, a strong hash function, and secure protocol design. Although the challenge-response messages used for shared key authentication can prevent successful replay of authentication traffic, the challenge-response process can be compromised by methods such as man-in-the-middle attacks and off-line brute force or dictionary attacks.[14]

Additional vulnerabilities in IEEE 802.11's shared key authentication are known and documented. For example, an attacker can eavesdrop, capturing and viewing the cleartext challenge value and the encrypted response. The attacker can then analyze the two pieces of information to determine the WEP key stream. Some organizations prefer using open system authentication because shared key authentication provides so much information to eavesdroppers about the WEP key that it jeopardizes the confidentiality and integrity that should be provided to the communications by the WEP key. Another significant limitation of shared key authentication is that it authenticates the identity of devices but not users. If an attacker gains access to a STA containing a WEP key, the attacker can use that key on any other WEP-capable device to authenticate and gain access to the WLAN.

Another major problem with shared key authentication is that WEP-based IEEE 802.11 requires all devices on a WLAN to use the same WEP key or the same small set of keys. This reduces accountability and complicates troubleshooting and incident response efforts. If the WEP key is compromised, it needs to be replaced as quickly as possible to prevent further malicious acts, because WEP keys are used not

[14] Moreover, the IEEE 802.11 challenge-response scheme does not work properly. WEP encrypts the response by XORing the challenge with a pseudo-random key stream generated using a WEP key. The attacker can XOR the challenge and the response to expose the key stream, which can subsequently be used to authenticate.

only for access control, but also to protect confidentiality and integrity (as described in Sections 4.3.1.2 and 4.3.1.3). Unfortunately, IEEE 802.11 does not specify any support for key management. When a WEP key needs to be changed, the WLAN administrators have to implement their own methods for generating and distributing a new key. The key needs to be replaced on all STAs and APs, which is a manual process for many WLAN products. WLAN administrators also need to implement methods for archiving, auditing, and destroying keys. Key management problems often limit the scalability of IEEE 802.11 WLANs employing WEP.

In some cases, shared key authentication is weakened by implementations that use poor WEP keys. For example, some implementations use the WLAN product's default WEP key or set a trivial key, such as all zeroes or all ones. The key should be randomly generated[15] so that it is not easily decipherable. This will delay attackers that capture network traffic and perform dictionary attacks against it, hoping to find the key that decrypts the traffic successfully. WEP keys should be changed frequently to reduce the likelihood and impact of any key compromises.

4.3.1.2 Encryption/Privacy

The WEP protocol, part of the IEEE 802.11 standard, uses the RC4 stream cipher algorithm to encrypt wireless communications, which protects transmitted data from disclosure to eavesdroppers. The standard for WEP specifies support for a 40-bit WEP key only; however, many vendors offer non-standard extensions to WEP that support key lengths of up to 104 or even 232 bits. WEP also uses a 24-bit value known as an initialization vector (IV) as a seed value for initializing the cryptographic key stream. For example, a 104-bit WEP key with a 24-bit IV becomes a 128-bit RC4 key. Ideally, larger key sizes translate to stronger protection, but the cryptographic technique used by WEP has known flaws that are not mitigated by longer keys, because the key flaws are a result of the weak implementation of the IV and RC4 symmetric-key, stream cipher algorithm. WEP is applied to all data above the IEEE 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hypertext Transfer Protocol (HTTP). WEP is illustrated conceptually in Figure 4-7.

[15] For more information about the significance and requirements of random number generation, see RFC 4086, *Randomness Requirements for Security,* found at http://www.ietf.org/rfc/rfc4086.txt. A more technical approach can be found in NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* available at http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90_DRBG-June2006-final.pdf.

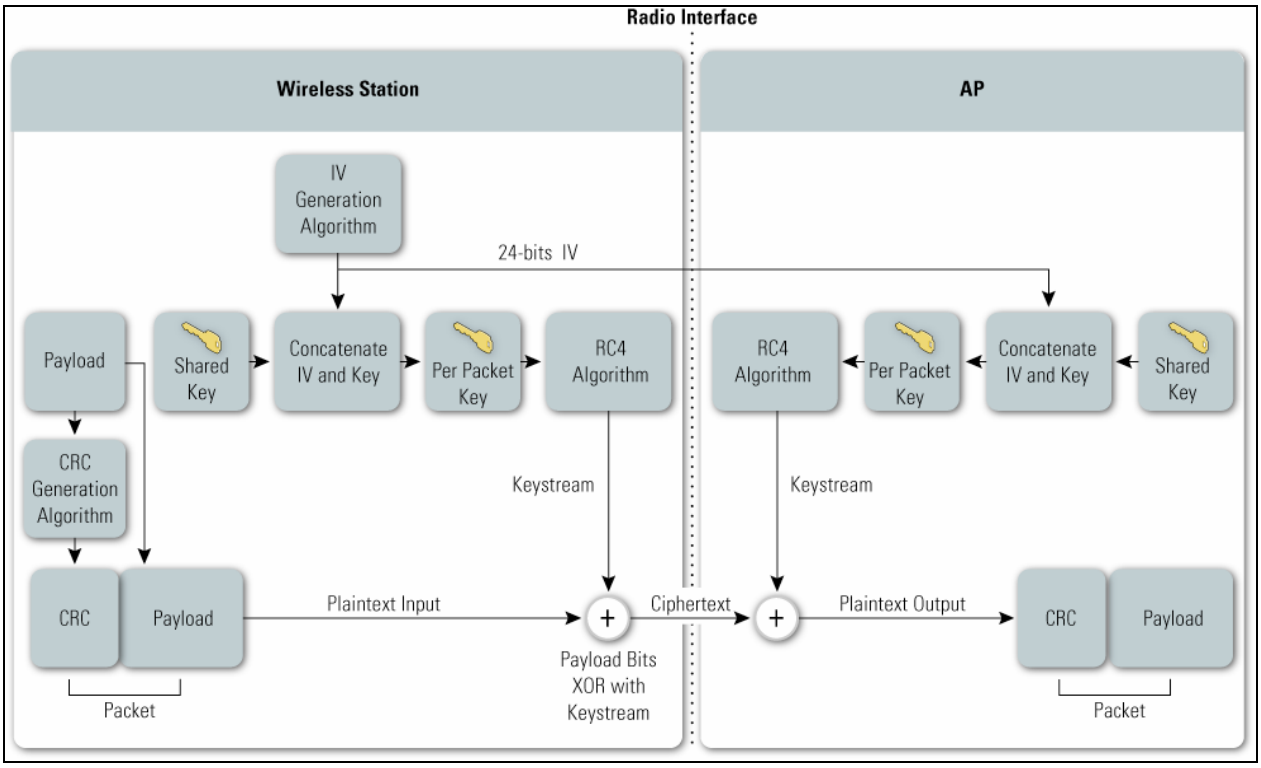

Figure 4-7. WEP Privacy Using RC4 Algorithm

Most attacks against WEP encryption have been based on IV-related vulnerabilities. For example, the IV portion of the RC4 key is sent in cleartext, which allows an eavesdropper that monitors and analyzes a relatively small amount of network traffic to recover the key by taking advantage of the IV value knowledge, the relatively small 24-bit IV key space, and a weakness in the way WEP implements the RC4 algorithm. Also, WEP does not specify precisely how the IVs should be set or changed, so some products use a static, well-known IV value or reset to zero. If two messages have the same IV, and the plaintext of either message is known, it is relatively trivial for an attacker to determine the plaintext of the second message. In particular, because many messages contain common protocol headers or other easily decipherable contents, it is often possible to identify the original plaintext contents with minimal effort. Even traffic from products that use sequentially increasing IV values is still susceptible to attack. There are less than 17 million possible IV values; on a busy WLAN, the entire IV space may be exhausted in a few hours. When the IV is chosen randomly, which represents the best possible generic IV selection algorithm, by the birthday paradox two IVs already have a 50% chance of colliding after about 2^{12} (or 4096) frames.

Another possible threat against confidentiality is network traffic analysis. Eavesdroppers might be able to gain information by monitoring which parties communicate at what times. Also, analyzing traffic patterns can aid in determining the content of communications; for example, short bursts of activity might be caused by terminal emulation or instant messaging, while steady streams of activity might be generated by video conferencing. More sophisticated analysis might be able to determine the operating systems in use based on the length of certain frames. Other than encrypting communications, IEEE 802.11, like most other network protocols, does not offer any features that might thwart network traffic analysis, such as adding random lengths of padding to messages or sending additional messages with randomly generated data.

Some WLAN devices can be upgraded through firmware to support WPA. WPA includes two main features: IEEE 802.1X and the Temporal Key Integrity Protocol (TKIP). The 802.1X port-based access control provides a framework to allow the use of robust upper layer authentication protocols. It also facilitates the use of session keys that allow the rotation of cryptographic keys. TKIP includes four new features to enhance the security of IEEE 802.11. TKIP extends the IV space, allows for per-packet key construction, provides cryptographic integrity, and provides key derivation and distribution. TKIP, through these features, provides protection against various security attacks discussed earlier, including replay attacks and attacks on data integrity. Additionally, it addresses the critical need to periodically change encryption keys. Again, the objective of WPA was to bring a standards-based interim security solution to the marketplace to replace WEP until the IEEE developed a new wireless security specification (IEEE 802.11i); however, WPA also has significant flaws and does not provide the level of security that IEEE 802.11i can. Table 4-2 below outlines the various IEEE 802.11 wireless security standards. Of the four standards shown in the table, only IEEE 802.11i using Counter Mode with Cipher Block Chaining MAC Protocol (CCMP) RSN has a cryptographic algorithm that is FIPS-approved.

Table 4-2. Summary of Data Confidentiality and Integrity Protocols

Security Feature	Manual WEP (pre-RSN)	Dynamic WEP (pre-RSN)	TKIP (RSN)	CCMP (RSN)
Core cryptographic algorithm	RC4	RC4	RC4	AES
Key sizes	40-bit or 104-bit (encryption)	40-bit or 104-bit (encryption)	128-bit (encryption), 64-bit (integrity protection)	128-bit (encryption and integrity protection)
Per-packet key	Created through concatenation of WEP key and the 24-bit IV	Derived from EAP authentication	Created through TKIP mixing function	Not needed; temporal key is sufficiently secure
Integrity mechanism	Enciphered CRC-32	Enciphered CRC-32	Michael MIC with countermeasures	CCM
Header protection	None	None	Source and destination addresses protected by Michael MIC	Source and destination addresses protected by CCM
Replay detection	None	None	Enforce IV sequencing	Enforce IV sequencing
Authentication	Open system or shared key	EAP method with IEEE 802.1X	EAP method with IEEE 802.1X or PSK	EAP method with IEEE 802.1X or PSK
Key distribution	Manual	IEEE 802.1X	IEEE 802.1X or manual	IEEE 802.1X or manual

4.3.1.3 Integrity

WEP performs data integrity checking for messages transmitted between STAs and APs. WEP is designed to reject any messages that have been changed in transit, such as by a man-in-the-middle attack. WEP data integrity is based on a simple encrypted checksum—a 32-bit cyclic redundancy check (CRC-32) computed on each payload prior to transmission. The payload and checksum are encrypted using the RC4 key stream before transmission. The receiver decrypts each transmission, recomputes the checksum on the received payload, and compares it with the transmitted checksum. If the checksums are not the same, the transmitted data frame has been altered in transit, and the frame is discarded. As with the

privacy service, unfortunately, the IEEE 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a "cryptographically secure" mechanism such as a hash or message authentication code.

The CRC-32 is subject to a number of security threats, including bit-flipping attacks, which occur when an attacker knows which CRC-32 bits will change when message bits are altered. WEP attempts to counter this problem by encrypting the CRC-32 to produce an integrity check value (ICV). The creators of WEP believed that an encrypted CRC-32 would be less subject to tampering. However, they did not realize that a property of stream ciphers such as WEP's RC4 is that bit flipping survives the encryption process—the same bits flip whether or not encryption is used. Therefore, the WEP ICV offers no additional protection against bit flipping.

Integrity should be provided by a cryptographic checksum rather than a CRC. Also known as keyed hashes or message authentication codes (MAC), cryptographic checksums prevent bit flipping attacks because they are designed so that any change to the original message results in significant and unpredictable changes to the resulting checksum. CRCs are generally more efficient computationally than cryptographic checksums, but are only designed to protect against random bit errors, not intentional forgeries, so they do not provide the same level of integrity protection.

Additionally, the IEEE 802.11 specification does not identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to individuals deploying WLANs. Key management (probably the most critical aspect of a cryptographic system) for IEEE 802.11 is left largely as an exercise for the administrators and users of the IEEE 802.11 network. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original IEEE 802.11 specification, a proper key management process to manage WEP-secured WLANs is extremely important. An enterprise that recognizes the need to change keys often and use random keys faces a formidable task in managing security of a large WLAN environment. For example, a large campus may have thousands of APs. Generating, distributing, loading, and managing keys for an environment of this size is a significant challenge.

4.3.2 Replay Protection

WEP implementation provides no protection against replay attacks because it does not include features such as an incrementing counter, timestamp, or other temporal data that would make replayed traffic easily detectable.

4.3.3 Availability

IEEE 802.11-based wireless access standards do not provide any additional mechanisms to prevent DoS attacks. Additionally, many of the physical security mechanism used to secure wired LANs are not feasible for WLANs because the RF signals from a WLAN propagate throughout free space.

4.3.4 Problems with the IEEE 802.11 Standard Security

This section discusses some known vulnerabilities in the security of the pre-RSN IEEE 802.11 WLAN standard. Several groups of computer security specialists have discovered security problems that let malicious users compromise the security of WLANs. These attacks on WLANs include both a variety of

passive attacks, such as packet capture or location tracking, and active attacks such as jamming and flooding.

A number of security problems have been identified with WEP, which include the following key problems:

- **Lack of Defined Key Management.** The lack of standardized key management and the use of static WEP keys pose a significant threat to WLANs. The lack of a standardized WEP key rotation is in part due to the lack of any key management provisions in the IEEE 802.11 standard or WEP protocol. Because of this, many users in a wireless network potentially use WEP keys for long periods of time, which is a well-known security vulnerability. The extensive use of WEP keys provides attackers with significant means to capture data in order to compute the WEP key and a larger pool of data to access or abuse with the stolen WEP key. Additionally, if a computer such as a laptop were to be lost or stolen, the key could become compromised, posing a significant risk to all devices using the same WEP key. Moreover, if every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks.

- **Weak IV.** The IV in WEP, as shown in Figure 4-8, is a 24-bit field sent in the cleartext portion of a message. This 24-bit string is used to initialize the key stream generated by the RC4 algorithm and is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for encrypting data, and the use of short IV increases the weakness of the entire encryption key because the IVs will repeat after a relatively short time in a busy network. Moreover, the IEEE 802.11 standard does not specify how the IVs are set or changed, leaving vendors responsible for implementation. Some vendors use the same IV or same IV scheme for each product, increasing the risk that all of the devices developed by a specific vendor will generate the same IV sequences or use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use collected data to easily decrypt the ciphertext.

- **Weak Encryption Keys.** The length of WEP keys is too short to provide an adequate level of security. When the IEEE developed WEP for the IEEE 802.11 standard, the organization thought that 40-bit encryption keys plus the 24-bit IV was strong enough. Additionally, defining smaller keys in the standard helped minimize export control issues. The fact that an eavesdropper knows 24 bits of every encryption key, combined with a weakness in the RC4 key schedule, allows an attacker to conduct a host of analytic attacks to decrypt captured packets after intercepting and analyzing only a relatively small amount of traffic.

- **Poor Integrity Protection.** The IEEE 802.11 protocol uses the CRC-32 algorithm to check the integrity of packets and acknowledge packets with the correct checksum, which is good for error detection but does not provide a strong level of integrity. The combination of non-cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as in the case of WEP. WEP fails to provide any level of cryptographic integrity protection. There are somewhat trivial attacks that can be conducted on WEP-encrypted packets where an attacker can alter the encrypted data and the CRC-32 in a way that prevents errors from being detected, thereby compromising the data. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection because of the possibility of interactions with other protocol levels that can give away information about ciphertext.

Because of the poor implementation of the cryptographic method in WEP, the problems would not be completely solved by merely increasing the length of the WEP key. Doing so will only yield a marginally longer time to decrypt packets. Additionally, it is important to note that WEP does not provide an acceptable level of wireless transmission security. Although outlined in the IEEE 802.11 standard, WEP should not be the sole security mechanism used in legacy wireless deployments. More robust wireless

security solutions, such as those outlined in NIST SP 800-97[16], or other security solutions should be implemented to provide wireless security. Because of the serious security flaws in IEEE 802.11a/b/g, NIST recommends that organizations with existing IEEE 802.11a/b/g implementations develop and implement migration strategies to move to IEEE 802.11i, which offers superior security.

Some of the problems associated with WEP and IEEE 802.11 WLAN security are summarized in Table 4-3.

Table 4-3. Key Problems with Existing IEEE 802.11 WLAN Security

Security Issue or Vulnerability	Remarks
1. Security features in products are not enabled by default.	The security features of WLAN devices often are not enabled when shipped, and users do not always enable or properly configure wireless devices when installed.
2. IVs are short, static, or weak.	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. The longer the key, the less likely a compromise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent a host of decryption attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of non-cryptographic integrity protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the client device is authenticated in a WLAN; therefore, a device that is stolen can access the wireless network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
11. The client does not authenticate the AP.	The client needs to authenticate the AP to ensure that it is legitimate and prevent the introduction of rogue APs.

[16] NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* is available at http://csrc.nist.gov/publications/nistpubs/.

4.4 Wireless Network Security, Vulnerabilities, and Threats

As the number of organizations that deploy wireless networks continues to grow, it becomes even more important to understand the vulnerabilities and threats facing IEEE 802.11 WLANs and implement appropriate security measures. Many organizations, including retail stores, hospitals, airports, and business enterprises, plan to capitalize on the benefits of wireless technology. However, although there has been tremendous growth and success in the wireless industry, certain precautions need to be taken to secure wireless networks. There have been numerous published reports and papers describing attacks on IEEE 802.11 wireless networks that expose organizations to security risks. This subsection briefly covers the vulnerabilities and threats facing IEEE 802.11-based wireless networks.

Network security attacks against WLANs are typically divided into two general categories:

- **Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content or actively attack or disrupt a WLAN. There are two types of passive attacks:
  - **Eavesdropping—**The attacker monitors wireless data transmissions between devices for message content, such as authentication credentials or passwords. An example of this attack is an attacker listening to transmissions on a WLAN between an AP and a client station.
  - **Traffic analysis (also known as traffic flow analysis)—**The attacker gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties. This is a more subtle method than eavesdropping.
- **Active Attack**—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack, but it may not be preventable. Active attacks may take the form of one of four types (or a combination thereof):
  - **Masquerading—**The attacker impersonates an authorized user to gain access to certain unauthorized privileges.
  - **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages posing as the legitimate user.
  - **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering the message.
  - **Denial of service (DoS)—**The attacker prevents or prohibits the normal use or management of a WLAN.

The threats associated with IEEE 802.11 are the result of one or more of these attacks. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

4.4.1 Loss of Confidentiality

Confidentiality is the information security property that ensures data is only available to authorized entities. This is generally considered a fundamental security requirement for most organizations. Due to the broadcast and radio nature of wireless technology, ensuring confidentiality is significantly more difficult in a wireless network than a wired network. Traditional wired networks provide inherent security through the use of a physical medium to which an attacker needs to gain access. Wireless networks propagate signals into space, making traditional physical security countermeasures less effective and

access to the network much easier, which increases the importance of adequate confidentiality on wireless networks.

Passive eavesdropping of native IEEE 802.11 wireless communications may cause significant risk to an organization. An adversary can scan RF signals and capture data traversing the wireless medium. Sensitive information including proprietary information, network IDs and passwords, and configuration data are some examples of data that may be captured. This risk is present because the IEEE 802.11 signals may travel beyond the intended physical service location, allowing attackers outside the physical confines of an office or building to eavesdrop on wireless networks. Additionally, attackers with specific equipment can capture data from wireless networks beyond the networks' normal operating range, again making confidentiality a critical security measure.

Eavesdropping performed with a wireless network analyzer tool or *sniffer*, which is free and readily available on the Internet, is particularly easy for two reasons: 1) confidentiality features of WLAN technology are frequently not enabled or not implemented properly, and 2) because of the numerous vulnerabilities in the IEEE 802.11 technology security, determined adversaries can compromise the system.

Wireless analyzers can take advantage of flaws in the key-scheduling algorithm that was provided for the implementation of RC4, which forms part of the original WEP standard. To exploit this weakness, the software passively monitors the WLAN data transmissions and computes the encryption keys after a variable number of network packets have been *sniffed*. On a highly saturated network, collecting the amount of data required to compute the WEP keys only takes several hours; if traffic volume is low, it may take up to one day. For example, a busy AP that is transmitting 3,000 bytes at 11 Mbps will exhaust the 24-bit IV space after approximately 10 hours.[17] If after ten hours the attacker recovers two ciphertexts that have been using the same key stream, both data integrity and confidentiality may be easily compromised. Advanced tools use methods to exploit the weakness in IEEE 802.11 security in less time. After the network packets have been received, the fundamental keys may be guessed in less than one second.[18] Once the malicious user knows the WEP key, he or she can read any packet traveling over the WLAN. These types of wireless sniffing tools are a major threat to wireless transmissions as they are widely available, easy to use, and can compute WEP keys quickly, which makes it essential for security administrators to implement secure wireless solutions.

Another risk to mobile and wireless devices is loss of confidentiality through simple eavesdropping of broadcast traffic. Ethernet hubs generally broadcast network traffic to all physical interfaces and connected devices, which leaves the broadcasted traffic vulnerable to unauthorized monitoring. For example, an AP connected to a port on an Ethernet hub that is broadcasting data traffic would broadcast all of the data traffic it received on the wired interface over the wireless interface. The use of the Ethernet hub infrastructure increases the risk that the AP may be broadcasting proprietary or sensitive data that was transmitted through the hub. Switches alleviate this concern in most cases by being configured to prohibit attached devices from intercepting data traffic to and from other devices. Consequently, organizations should use switches instead of hubs for connections to APs.[19]

WLANs risk loss of confidentiality following an active attack as well. Because sniffing software can obtain usernames and passwords as they are sent over a wireless connection, an adversary may be able to masquerade as a legitimate user and gain access to an organization's enterprise network through an AP. This could give the attacker access to internal network resources and sensitive data.

---

17 10 hours = (3,000 bytes x ((8 bits/byte) / (11 x 106 bits/sec)) x 24) = 36,600 seconds.)

18 For more information from AirSnort, visit their Web page at http://airsnort.shmoo.com/.

19 See Internet Security Systems, "Wireless LAN Security: 802.11b and Corporate Networks."

A malicious or irresponsible user could physically and surreptitiously insert a rogue AP into a closet, under a conference room table, or any other hidden area within a building. The rogue AP could then be used to allow unauthorized individuals to gain access to an enterprise network. As long as its location is in close proximity to the users of the WLAN, and it is configured to appear as a legitimate AP to wireless clients, the rogue AP may successfully convince wireless clients of its legitimacy and cause wireless clients to connect and transmit traffic to the rogue AP. In this scenario, an attacker can easily capture all of the data transmitted through the rogue AP, bypassing all wireless protocol confidentiality.

A malicious user can also gain access to the wired network through APs, which allows malicious users to bypass perimeter security mechanisms and gain access to the wired enterprise network without authorization. It is also important to note that rogue APs are not always deployed by malicious users. In many cases, rogue APs are deployed by users who want to take advantage of wireless technology without the approval of the IT department. Additionally, because rogue APs are frequently deployed without the knowledge of security administrators, these APs are often deployed without proper security configurations and pose significant security risks.

4.4.2 Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Because organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. For example, an attacker can compromise data integrity by deleting or modifying the data in an e-mail via the wireless system. This can be detrimental to an organization if important e-mail is widely distributed among e-mail recipients. Because the existing security features of the IEEE 802.11 standard do not provide strong message integrity, other kinds of active attacks that compromise system integrity are possible. The specific weaknesses of the CRC-32 integrity mechanism portion of WEP are outlined in Section 4.3.1.3.

4.4.3 Loss of Network Availability

A denial of network availability involves some form of DoS attack, such as jamming or flooding. Jamming occurs when a malicious user deliberately emanates an RF signal from a wireless device to overwhelm legitimate wireless devices and signals. Jamming may also be inadvertently caused by emissions from other legitimate devices operating within unlicensed spectrum, such as a cordless phone or microwave oven. Jamming results in a breakdown or complete loss of communications between legitimate wireless devices because signals are unable to be properly transmitted.

Attackers can also cause significant disruption to WLANs by initiating flooding attacks on APs and other wireless devices. This attack is initiated using specific software designed to transmit a large number of packets to an AP or other wireless device, causing the wireless devices to be overwhelmed by packets and cease normal operation. This type of attack can cause the WLAN to degrade to an unacceptable performance level or even fail completely. Non-malicious users can also cause a DoS by unintentionally monopolizing the capacity of a WLAN by downloading large files, effectively denying other users access to the network. As a result, organizational security policies should outline acceptable use and impose bandwidth control mechanisms.

Jamming and flooding threats are difficult to counter in any radio-based communications, thus the IEEE 802.11 standard does not currently provide any defense against them.

4.4.4 Other Security Risks

There are a number of additional security risks for wireless networks. One of the more prominent risks is posed by mobile users accessing enterprise resources through the use of public wireless networks. Conference centers, airports, hotels, and cafes commonly provide wireless networks for mobile users to connect to the Internet and subsequently to enterprise networks controlled by an organization. Third-party untrusted wireless networks do not offer the mobile user any control over the network infrastructure or operating environment. By connecting to enterprise networks via an untrusted third-party wireless network, mobile users may inadvertently pose significant vulnerabilities to an organization's enterprise network unless proper steps are taken to protect mobile users and the enterprise. Organizations should consider protecting mobile users and enterprise resources using an application layer security protocol such as Transport Layer Security (TLS) or other VPN security solutions to secure connections from unauthorized eavesdropping and access.

4.5 Risk Mitigation

Organizations can mitigate risks to WLANs by applying countermeasures to address specific threats and vulnerabilities. Management countermeasures combined with operational and technical countermeasures can be effective in reducing the risks commonly associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. However, this section does describe risk-mitigating steps organizations can take to reduce the risks posed by WLANs. Additionally, it should be clear that there is no "one size fits all solution" in terms of security. Also, security comes at a cost in terms of financial expenses related to security equipment, inconvenience, maintenance, and operation. Each organization needs to evaluate the acceptable level of risk based on numerous factors, which will affect the level of security implemented by the organization.

4.5.1 Management Countermeasures

An overarching security policy that addresses wireless technology is the cornerstone of management countermeasures, and is required to provide an adequate level of initial security. A security policy and the ability to enforce compliance are the foundations on which all other operational and technical countermeasures are rationalized and implemented. A WLAN security policy should include the following:

- Identify users or groups of users that are authorized to use organization-sanctioned WLANs
- Identify what type of access or services will be provided by a deployed WLAN
- Identify and describe the parties that are authorized and responsible for installing and configuring access points and other wireless equipment
- Provide limitations on the service area of WLANs and outline the mechanisms required to provide adequate physical security for wireless networks and devices
- Describe the type of information that may be sent over wireless links, including acceptable use guidelines
- Describe conditions under which wireless devices are allowed to be used and operated
- Define standard hardware and software configurations that must be implemented on all wireless devices to ensure the appropriate level of security

- Describe limitations on how and when the wireless device may be used, such as specific locations
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines for the protection of wireless clients to minimize/reduce theft
- Provide guidelines on the use of encryption and key management
- Describe organization actions that will be taken to address identified rogue or misconfigured devices
- Define the frequency and scope of wireless security assessments
- Describe actions or measures to address staff infringement on defined policy.

Trained and aware users serve as an important countermeasure; therefore, organizations should ensure that all IT staff and organization personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and wireless devices pose. They must work to ensure security policy compliance and be aware of the steps to take in the event of an attack.

4.5.2 Operational Countermeasures

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities providing wireless network connectivity need physical access controls. For example, photo identification, card badge readers, or biometric devices can be used to minimize the risk of improper physical penetration of facilities. External boundary protection can include locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorized access to wireless networking components such as wireless APs from outside the organization's secure facility. Additionally, security mechanisms should be put in place to prevent the theft, alteration, or misuse of wireless infrastructure placed throughout an enterprise. Network infrastructure is generally placed within a wiring or network closet, but because APs are dispersed throughout a physical location, each device needs to be locked and secured in an appropriate fashion.

It is important to consider the range of each AP that will be deployed as part of a WLAN environment. If the range extends beyond the physical boundaries of the building's walls, the extension creates a security vulnerability. An individual outside of the building, perhaps war driving, could eavesdrop on network communications by using a wireless device to capture wireless signals and data. A similar consideration applies to the implementation of building-to-building bridges. Ideally, the APs or bridges should be placed strategically within a building so that the range does not exceed the physical perimeter of the building and allow unauthorized personnel to eavesdrop near the perimeter. Organizations should use site survey tools to measure the range of AP devices, both inside and outside of the building where the wireless network is located. In addition, organizations should use wireless security assessment tools (e.g., vulnerability assessment) and regularly conduct scheduled security audits.

Site survey tools are extremely useful during the initial stages of WLAN development and for reassessing WLAN deployments. Site survey tools should be used by the appropriate individuals to design and deploy wireless networks. These tools measure and evaluate a number of WLAN characteristics, including signal strength, range, data rate, and other factors. These measurements can be used to map out the appropriate coverage area, capacity, and data rates for required WLAN usage. A proper site survey is important to ensure that signals for WLAN deployments do not extend beyond the appropriate service area to unrestricted areas, such as parking lots or public areas. During a deployment, administrators should take

every precaution to control WLAN signals, including the use of directional antennas to control RF emanations. Directional antennas do not protect network links, they merely help control coverage range by limiting signal dispersion.

Although mapping the coverage area may yield some advantage relative to security, it is not an absolute solution. There is always the possibility that an attacker might use a high-gain antenna from a relative distance to eavesdrop on the wireless network traffic. It should be recognized that only by using strong cryptographic means can a user gain any assurance against true eavesdropping adversaries.

4.5.3 Technical Countermeasures

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. These countermeasures include proper AP configurations (i.e., the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection and prevention systems (IDPS), encryption, smart cards, VPNs, public key infrastructure (PKI), and biometrics.

4.5.3.1 Access Point Configuration

Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption, reset functions, automatic network connection functions, access control lists (ACL), shared keys, and Simple Network Management Protocol (SNMP) agents eliminates many of the vulnerabilities inherent in a product's default configuration. Default configurations for APs are widely available via the Internet and are commonly exploited by attackers.

Updating administrator access. Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example of a default vulnerability of an AP. On some APs, the factory default configuration does not require a password or the default password is commonly known. Unauthorized users can easily gain access to the device if there is no password protection. Administrators should change default settings to reflect the organization's security policy, which should include the requirement for strong (i.e., an alphanumeric and special character string at least eight characters in length) administrative passwords. If the security requirement is sufficiently high, an organization should consider using an automated password generator. Additionally, the AP should lock the login screen after a specific number of failed attempts have been reached. A timeout feature should also be enabled to logout the user after a certain amount of inactivity occurs. An alternative to password authentication is two-factor authentication. One form of two-factor authentication uses a symmetric key algorithm to generate a new code every minute. This code is a one-time use code that is paired with the user's personal identification number (PIN) for authentication. Another example of two-factor authentication is pairing the user's smart card with the user's PIN. This type of authentication requires a hardware device reader for the smart card or an authentication server for the PIN. Several commercial products provide this capability. However, use of an automated password generator or two-factor authentication mechanism may not be worth the investment, depending on the organization's security requirements, number of users, and budget constraints. Given the need to ensure good password authentication and policies, it is important to note the critical importance of ensuring that the management interface has the proper cryptographic protection to prevent the unauthorized disclosure of the passwords over the management interface. Numerous mechanisms exist that can be used to ensure that encrypted access protects critical data in transit, such as Secure Shell (SSH) and SSL.

Establishing proper encryption settings. Encryption settings should be set to the strongest encryption available in the product. Despite the type of encryption available, the longest (i.e., strongest) unique key possible should be used. It is important to note that the client devices and APs must support the same

level and type of encryption, so client devices should also be reviewed to determine the level of encryption that can be deployed.

Controlling the reset function. The reset function poses a particular problem because it may allow an individual to negate any security settings that administrators have configured in the AP. A specific type of reset will return the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. On some devices, an individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing. If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel out any security settings on the device. The reset function, if configured to erase basic operational information such as IP address or keys, can further result in a network DoS, because APs may not operate without these settings. Having physical access controls in place to prevent unauthorized users from resetting APs can mitigate the threats. Organizations can detect threats by performing regular security audits. Additionally, resets can be invoked remotely over the management interface on some products. For this reason, there is a greater need to have proper password administration, configuration, and encryption on the management interface.

Using MAC ACL functionality. A MAC address is a hardware address that is intended to uniquely identify each network-based device. Networks use the MAC address to help regulate communications between different network devices. Many IEEE 802.11 product vendors provide capabilities for restricting access to the WLAN based on MAC ACLs that are stored and distributed across many APs. The MAC ACL grants or denies access to a computer using a list of permissions designated by MAC address. However, the MAC ACL does not represent a strong defense mechanism by itself. Because MAC addresses are transmitted in the clear from a wireless device to an AP, the MAC can be easily captured. Malicious users can spoof a MAC address by changing the actual MAC address on another computer to a MAC address that has access to the wireless network. This countermeasure may provide some level of security; however, users should use this with caution. This may be effective against casual eavesdropping but will not be effective against determined adversaries. Users may want to consider this as part of an overall defense-in-depth strategy—adding levels of security to reduce the likelihood of problems. However, users should weigh the administrative burden of enabling the MAC ACL (assuming they are using MAC ACLs) against the true security provided. In a medium-to-large network, the burden of establishing and maintaining MAC ACLs may exceed the value of the security countermeasure. Additionally, most products only support a limited number of MAC addresses in the MAC ACL. The size of the access control list may be insufficient for medium-to-large networks.

Changing the SSID. The SSID is an identifier that is sometimes referred to as the network name. Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. The SSID, typically a null-terminated ASCII string, has a range from 0 to 32 bytes (or characters). The default SSIDs used by many IEEE 802.11 WLAN vendors have been published and are well known to would-be adversaries, so the default SSID values of APs should be changed from the factory default to an unidentifiable value or non-discrete name to prevent easy identification by attackers. Although an equipped adversary can capture this identity parameter over the wireless interface, it should be changed to prevent unsophisticated adversary attempts to connect to the wireless network.

Maximize the beacon interval. The IEEE 802.11 standard specifies the use of "Beacon frames" to announce the existence of a wireless network. These beacons are transmitted from APs at regular intervals and allow a client station to identify and match configuration parameters to join a wireless network. APs may not be configured to suppress the transmission of the Beacon frames and their mandatory SSID field. However, the interval length may be set to its highest value, which results in approximately a 67 second interval. While the security improvement is marginal, it does make it somewhat more difficult to

passively locate a network because the AP is not transmitting as frequently. Using a longer Beacon interval forces an adversary to perform active scanning using Probe Request messages.

Using SNMP. Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP, SNMPv1 and SNMPv2, support only trivial authentication based on plaintext community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security, is highly recommended.[20] If SNMP is not required on the network, it should be disabled. If an organization must use a version of SNMP besides version 3, they must recognize and accept the risks. It is common knowledge that the default SNMP community string that SNMP agents commonly use is the word "public" with assigned "read" or "read and write" privileges. Using this well-known default string leaves devices vulnerable to attack. If an unauthorized user were to gain access and had read/write privileges, that user could write data to the AP, resulting in a data integrity breach. Organizations that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plaintext community strings and, as a result, are fundamentally insecure and are not recommended.

Using HTTP. Most wireless APs include an HTTP interface which provides administrators with a remotely accessible interface to manage device configuration. Normally, the only access control mechanism securing this interface is a user ID and password. In this case, any user with those credentials can re-configure the device to either provide no security or change the encryption key so that no authorized users can associate with the AP. Further, HTTP does not natively provide confidentiality security in the form of data encryption. It is recommended that HTTP interfaces be disabled once an AP is configured appropriately. If absolutely necessary, an HTTPS (using SSL) interface should be used with a strong password to help mitigate potential attacks.

Changing default channel and power output. Although not directly exploitable, the default channel and power output of APs should be configured appropriately. If two or more APs are located near each other, but are on different networks, a DoS can result from radio interference between the two APs if they are operating on the same or conflicting channels. Organizations that incur radio interference need to determine if one or more nearby AP(s) are using the same channel or a channel within five channels of their own and then choose a different channel. For example, channels 1, 6, and 11 can be used simultaneously by APs that are close to each other without mutual interference. Organizations must perform a site survey to discover any sources of radio interference. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP. Additionally, the power output of APs should be determined to minimize any unneeded channel overlap and to prevent the AP from providing too broad or limited a coverage area.

Using DHCP. Automatic network connections involve the use of the Dynamic Host Control Protocol (DHCP). DHCP automatically assigns IP addresses to devices that associate with an AP. For example, a DHCP server is used to manage a range of TCP/IP addresses for client laptops or workstations. After the range of IP addresses is established, the DHCP server dynamically assigns addresses to workstations as needed. The server assigns the device a dynamic IP address as long as the encryption settings are compatible with the WLAN. The threat with DHCP is that a malicious user could easily gain unauthorized access on the network with a laptop with a wireless NIC. Since a DHCP server will not necessarily know which wireless devices have access, the server will automatically assign the laptop a valid IP address. Risk mitigation involves disabling DHCP and using static IP addresses on the wireless

[20] See http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-rfc2570bis-03.txt for an explanation on why using SNMPv3 instead of SNMPv1 or SNMPv2 is strongly recommended.

network, if feasible. This alternative, like the MAC ACL countermeasure, may only be practical for relatively small networks, given the administrative overhead involved with assigning static IP addresses and the possible shortage of addresses. Statically assigning IP addresses to clients would also negate some of the key advantages of wireless networks, such as roaming or establishing ad hoc networks. Providing static IP addresses to client devices is a significant administrative task that should only be implemented if deemed necessary.

4.5.3.2 Wireless Client Device Security

Personal firewall. Resources on wireless networks have a higher risk of attack because they generally do not have the same degree of protection as internal resources. Personal firewalls increase device security by offering some protection against certain attacks.[21] Personal firewalls are software-based solutions that reside on a client device and are either client managed or centrally managed. Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage these solutions as opposed to leaving the management to the end user. Centrally managed solutions allow organizations to modify client firewalls to protect against known vulnerabilities and to maintain a consistent security policy for all remote users. Some of these high-end products also have VPN and audit capabilities. Although personal firewalls offer some measure of protection, they do not protect against advanced attacks. Depending on the security requirement, organizations may still need additional layers of protection.

Host-based intrusion detection and prevention systems (IDPS). A host-based IDPS provides complementary security services to personal firewalls. Host-based IDS software monitors and analyzes the internal state of a client device. The host-based IDS provide alerts or other responses when a system is not functioning as expected. Some products review logs to ensure that the system is performing as expected and that applications are not functioning unexpectedly, such as software applications inexplicably accessing or altering other portions of the system. Host-based IDS software also monitors network communications and reports or possibly blocks suspicious activity. As with all security solutions, proper installation and configuration determines the level of security provided by host-based IDS solutions. Some vendors bundle multiple software security packages; however, it is important that specific host-based functionality be included in any implemented client security solution.

Anti-virus. Anti-virus software is needed to assist in preventing the spread of viruses and worms between networked devices. Mobile and wireless client devices should have anti-virus software installed and consistently updated to ensure that the newest updates and signatures are loaded on the client device. Organizations should ensure that anti-virus software installed on client devices is properly configured to automatically receive updates to provide the most up-to-date virus security possible for client devices. Again, client device security solutions are now being bundled by vendors, so it is important that these bundled offerings be reviewed to ensure that all aspects of client security are addressed.

Disable radio. The IEEE 802.11 radio on all client devices should be disabled by default. This configuration is important to prevent client devices from being prone to attacks via the IEEE 802.11 wireless network interface when not in use. Users should manually have to engage the radio when they choose to establish a wireless connection. This will prevent wireless connectivity from ensuing without the user's knowledge, and provide additional security for the client device. However, users that enable the wireless interface for communication must ensure that the wireless network interface is disabled when not in use. Configuring all client devices to operate with the wireless interface disabled by default will help secure the client device, but will not completely mitigate potential wireless attacks on client devices.

---

[21] See case study on the use of firewalls on laptops for telecommuters at http://www.techrepublic.com/article.jhtml?id=r00520010328law01.htm.

Additionally, client devices should be configured not to allow the simultaneous use of more than one network interface.

Policy enforcement. Client devices should be configured to comply with implemented wireless policies. Policy enforcement and compliance for client devices comes in several forms. Devices can be configured according to policy, such as disabling services or altering default configurations. Additionally, policy-driven software solutions can be implemented on client devices to prevent or allow certain actions to take place only when specific parameters are met. This type of software assists in ensuring that client devices and users comply with defined policies. For example, policy-based software can prevent client devices from having more than one network interface enabled at a time.

Implementing data-at-rest. Data-at-rest solutions will secure data stored on the client device in the event the device is lost or stolen. Data-at-rest security solutions encrypt all or portions of the data stored on the client device's hard drive to ensure that unauthorized individuals cannot gain access to the data stored on the device. However, when an authorized user is logged into the device, the hard drive is no longer encrypted. Therefore, it is important that the other security measures outlined above be implemented to secure the client device during normal operation.

4.5.3.3 Software Patches and Upgrades

Vendors generally try to correct known software and hardware security vulnerabilities when they have been identified. These corrections come in the form of security patches, upgrades, or firmware updates. Network administrators need to regularly check with the vendor to see whether security patches and upgrades are available and apply them as needed. Also, many vendors have "security alert" e-mail lists to advise customers of new security vulnerabilities and attacks. Administrators should sign up to receive these critical alerts and have procedures and processes in place to implement updates. Lastly, administrators can check with the NIST National Vulnerability Database (NVD)[22] for a listing of all known vulnerabilities in the software or hardware being implemented. For specific guidance on implementing security patches, see NIST Special Publication 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*[23].

An example of a problem addressed in a patch is the RSA Security WEP security enhancement. In November 2001, RSA Security, Inc. developed a cryptographic technique to address some of the known security flaws in WEP. This enhancement, referred to as "fast packet keying," generates a unique key to encrypt each network packet on the WLAN. The Fast Packet Keying Solution uses a hashing technique that rapidly generates the per packet keys. The IEEE has approved the fast packet keying technology as one fix to the IEEE 802.11 protocol. Vendors have applied the fix to new wireless products and have developed software patches for many existing products.

Another example of a purpose of a patch is deploying WPA. WPA, which is promoted by the Wi-Fi Alliance, is an interim security solution that may not require a hardware upgrade in existing IEEE 802.11 equipment. WPA attempts to deliver enhanced protection to address some of the problems of WEP.

4.5.3.4 Authentication

In general, effective authentication solutions are a reliable way of permitting only authorized users to access a network. Authentication solutions include the use of usernames and passwords, smart cards,

[22] NVD is located at http://nvd.nist.gov/.

[23] NIST SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, is available at http://csrc.nist.gov/publications/nistpubs/

biometrics, PKI, or a combination of solutions (e.g., smart cards with PKI).[24] When relying on usernames and passwords for authentication, it is important to have policies specifying minimum password length, required password characters, and password expiration. Smart cards, biometrics, and PKI each have individual requirements that will be addressed in more detail later in this document.

At a minimum, all organizations should implement a strong password policy, regardless of the operational security level. Strong passwords are simply a fundamental measure in any environment. Organizations should also consider other types of authentication mechanisms if security levels warrant additional authentication. These mechanisms may be integrated into a WLAN solution to enhance the security of the system. However, users should be careful to fully understand the security provided by enhanced authentication.

There are a number of hardware mechanisms that can be used to provide an additional layer of authentication for logical network access, including access to WLANs. Some of the mechanisms that are currently deployed or may be deployed at organizations in the near future to provide an additional layer of authentication are public key infrastructure (PKI), biometrics, and smart cards.

PKI provides the framework and services for generating, distributing, controlling, and accounting for public key certificates. PKI provides the ability to encrypt files and applications, authenticate network transactions, as well as provide data integrity and nonrepudiation functionality. WLANs can integrate PKI for authentication and secure network transactions.

Smart cards provide added utility to PKI because the electronic certificates can be integrated into the memory of the smart cards, which allows a smart card to serve as both a token and a secure (tamper-resistant) means for storing cryptographic credentials. Smart cards are beneficial in environments requiring authentication beyond simple username and password. The portability of smart cards allows users to securely access network resources from various locations. As with most authentication solutions, smart cards may be integrated into a WLAN solution to enhance the security of the system. Network administrators and organization officials need to consider the complexity and cost of implementing and administering PKI before adopting this solution. For more information on smart cards, please see FIPS 201 and the NIST Personal Identity Verification (PIV) Project Web site.[25]

Organizations can also combine smart cards with biometrics to provide a more robust level of user authentication. Biometric devices include fingerprint/palm-print scanners, optical scanners (including retina and iris scanners), facial recognition scanners, and voice recognition scanners. Additionally, biometrics can be combined with VPN solutions to provide authentication and data confidentiality.

4.5.3.5 Wireless Intrusion Detection and Prevention Systems (IDPS)

A wireless intrusion detection and prevention system (IDPS) is an effective tool for determining whether unauthorized users or devices are attempting to access, have already accessed, or have compromised a wireless network. Wireless IDPS can also detect misconfigured wireless clients, rogue access points, ad hoc networks, and other possible violations of an organization's wireless networking policy.[26] Organizations with wireless LANs should consider implementing wireless IDPS solutions. For more information about wireless IDPS, see NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems*.

---

[24] See Federal Information Processing Standards Publication 196, *Entity Authentication Using Public Key Cryptography* at http://csrc.nist.gov/publications/fips/index.html.

[25] NIST Personal Identity Verification (PIV) Project homepage, http://csrc.nist.gov/piv-program/.

[26] Eavesdropping and other passive techniques cannot be identified by IDPS technologies.

4.5.3.6 Security Assessments

Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure WLANs remain secure.[27] It is important for organizations to perform regular audits using wireless network analyzers and other tools.[28] An analyzer, sometimes called a sniffer, is an effective tool to conduct security auditing and troubleshoot wireless network issues. Security administrators or security auditors can use network analyzers to determine if wireless products are transmitting correctly and on the correct channels. Administrators should periodically check within the office building space (and campus) for rogue APs and other unauthorized access. Organizations may also consider using an independent third party to conduct the security audits from an impartial perspective. Independent third-party security consultants may be more up-to-date on security vulnerabilities, well trained on security solutions, and better equipped to assess the security of a wireless network. An independent third-party audit, which may include penetration testing, will help an organization ensure that it has deployed a WLAN that is compliant with established security procedures and policies and that the system is up-to-date with the latest software patches and upgrades.[29] It is worth noting that organizations should take a holistic approach to the assessment process. It is important to ensure that the wireless portion of the network is secure, but it is also important for the wired portion to be secure.

4.5.3.7 Virtual Private Networks

A virtual private network (VPN) is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and IP information transmitted between networks. Because a VPN can be used over existing networks, such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. This is often less expensive than alternatives such as dedicated private telecommunications lines between organizations or branch offices. VPNs can also provide flexible solutions, such as securing communications between remote telecommuters and an organization's servers, regardless of where the telecommuters are located. A VPN can even be established within a single network to protect sensitive communications from other parties on the network, such as in a WLAN. A variety of VPN technologies currently exist, such as IPsec VPNs and SSL VPNs. As with other security technologies, Federal agencies must use VPNs that apply FIPS-approved encryption algorithms contained in validated cryptographic modules.[30]

An example of using an IPsec VPN with WLANs is depicted in Figure 4-8. As shown, the VPN tunnel is established between the wireless client (Laptop) and the VPN concentrator on the enterprise network edge. The wireless client in this scenario could be accessing an organization's network resources through an organization-deployed WLAN or a public WLAN for remote access connectivity. With an IPsec VPN, security services are provided at the network layer of the protocol stack, which will secure all applications and protocols operating at layer 3 and above. The VPN security services are independent of layer 2 wireless security and are recommended to be used with legacy or weak wireless security, such as WEP. As a defense-in-depth strategy, if a VPN is in place, an organization can consider having both VPN

---

[27] For more information on network security, see NIST SP 800-42, *Guideline on Network Security Testing* (http://csrc.nist.gov/publications/nistpubs/)

[28] Some wireless IDPS sensors are mobile and have wireless network analyzer capabilities so that they can be used to perform audits of wireless networking.

[29] See "Clinic: What are the biggest security risks associated with Wireless technology? What do I need to consider if my organization wants to introduce this kind of technology to my corporate LAN?", 2001, at http://www.itsecurity.com/.

[30] More specific information and guidance on IPsec VPNs is available in NIST SP 800-77, *Guide to IPsec VPNs,* which is available at http://csrc.nist.gov/publications/nistpubs/.

security and wireless security applied. With a configuration as in Figure 4-8, the VPN encrypts (and otherwise protects) the transmitted data to and from the wired network over the WLAN.[31]

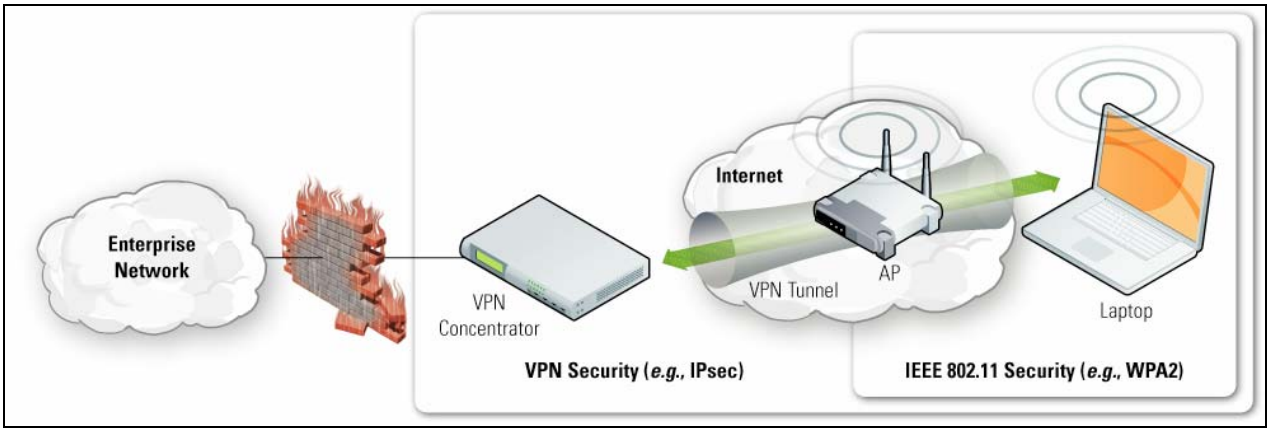

Figure 4-8. VPN Usage Over an IEEE 802.11 WLAN

It is important to understand that VPNs do not remove all risk from networking. While VPNs can greatly reduce risks, particularly for communications that occur over public networks, they cannot eliminate all risks for such communications.

4.6 Wireless Local Area Network Security Checklist

Table 4-4 presents guidelines and recommendations for creating and maintaining a secure IEEE 802.11 wireless network. For each recommendation or guideline, a justification column with a narrative is provided that addresses the security need, requirements, or justification for that recommendation. Additionally, with each recommendation and justification, a checklist with three columns is provided. The first column, the "Recommended Practice" column, if checked, means this is recommended for all organizations. The second column, the "Should Consider" column, if checked, means the recommendation is something that an organization should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some sort of additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the "Should Consider" column is checked, organizations need to carefully consider the option and weigh the costs versus the benefits. The last column, "Status", is intentionally left blank to allow organization representatives to use this table as a true checklist. For instance, an individual performing a wireless security audit in an IEEE 802.11 environment can quickly check off each recommendation for the organization.

[31] See "Identifying the Weakest Link," *Wireless Internet Magazine*, November/December 2001, at http://www.wirelessinternetmag.com/.

Table 4-4. Wireless Local Area Network Security Checklist

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
Management Recommendations					
1.	Develop an organization security policy that addresses the use of wireless technology, including IEEE 802.11.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable architecture, implementation, and uses for IEEE 802.11 wireless technologies.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.	✓		
3.	Perform a risk assessment to understand the value of the assets in the organization that need protection.	Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.	✓		
4.	Ensure that the client devices and APs support firmware upgrades so that security patches may be deployed as they become available (prior to purchase).	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist) to fully understand the wireless network security posture.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the organization.	The external boundaries should be secured to prevent malicious physical access to an organization's information system infrastructure such as a fence or locked doors.	✓		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
8.	Complete a site survey to measure and establish the AP coverage for the organization.	Proper placement of APs will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes AP locations, determines coverage areas, assigns radio channels to each AP, and ensures that the coverage range does not expose APs to potential malicious activities.	✓		
9.	Take a complete inventory of all APs and IEEE 802.11 wireless devices.	A complete inventory list of APs and IEEE 802.11 wireless devices can be referenced when conducting an audit for unauthorized use of wireless technologies.	✓		
10.	Ensure that wireless networks are not used until they comply with the organization's security policy.	Security policy enforcement is vital for ensuring that only authorized APs and IEEE 802.11 wireless devices are operating in compliance with the organization's wireless security policy.	✓		
11.	Position APs on the interior of buildings instead of near exterior walls and windows.	Deploying APs near exterior walls and windows increases the risk of eavesdropping by potential external malicious users from beyond the physical confines of a building or office. It is important to position APs wisely to balance security and coverage.	✓		
12.	Place APs in secured areas to prevent unauthorized physical access and manipulation.	APs and other network infrastructure should be deployed to secure areas, such as a network closet, or contained in secure enclosures to prevent unauthorized access by potential malicious users.	✓		
Technical Recommendations					
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	By empirically testing the AP coverage range, a level of risk associated with the access range by potential malicious users can be better understood.	✓		
14.	Make sure that APs are turned off when they are not used (e.g., after hours and on weekends).	Shutting down APs when not in use minimizes potential exposure to malicious activity.	✓		
15.	Make sure that the reset function on APs is used only when needed and is only invoked by authorized personnel.	The reset function allows an individual to negate any security settings administrators have configured on an AP.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
16.	Restore the APs to the latest security settings when the reset functions are used.	Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.	✓		
17.	Change the default SSID on the APs.	Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to IEEE 802.11 networks using the default SSID.	✓		
18.	Validate that the SSID character string does not reflect the organization's name (division, department, street, etc.) or products.	The SSID should be somewhat difficult for malicious users to use to determine the organization that owns the AP.	✓		
19.	Ensure that AP channels are different from nearby APs to prevent interference.	Radio interference between APs can result in a DoS. Therefore, using channels in a different range ensures service availability.	✓		
20.	Understand and make sure that all default parameters are changed.	Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.	✓		
21.	Disable all insecure and nonessential management protocols on the APs.	Management protocols that are enabled on APs but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an AP.	✓		
22.	Enable the strongest available security features of the WLAN product, including encryption and authentication (e.g., FIPS-approved cryptographic algorithms).	Enabling built-in security features provides greater security than the default settings.	✓		
23.	Ensure that encryption key sizes are at least 128 bits or as large as possible.	Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit key provides an "intractable" key space against cryptanalysis, if the algorithm and implementation are sound.	✓		
24.	If shared keys are employed, make sure that default shared keys are periodically replaced by more secure unique keys.	Changing default shared keys periodically decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
25.	Install a properly configured firewall between the wired infrastructure and the wireless network.	A firewall can enforce a security policy on the information flow between the wired network and the wireless network.	✓		
26.	Install antivirus software on all wireless clients.	Antivirus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.	✓		
27.	Install personal firewall software on all wireless clients.	Personal firewalls help to protect the client device against attacks.	✓		
28.	Disable file sharing on wireless clients.	Malicious users can potentially exploit wireless clients enabled for file sharing.	✓		
29.	Deploy MAC access control lists.	The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.		✓	
30.	Use Layer 2 switches in lieu of hubs for AP connectivity.	The use of layer 2 switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.	✓		
31.	Deploy a VPN, such as IPsec, for additional security of wireless communications.	The use of VPNs provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.		✓	
32.	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirement and overhead cost related to processor capability.	✓		
33.	Fully test and deploy software patches and upgrades on a regular basis.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.	✓		
34.	Ensure that all APs have strong administrative passwords.	Administrator passwords on APs should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
35.	Ensure that all passwords are being changed regularly.	Passwords should be changed regularly to reduce the risk of a compromised password being exploited.	✓		
36.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.	Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.		✓	
37.	Ensure that the "ad hoc mode" for IEEE 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or select an alternate product.	The "ad hoc mode" for IEEE 802.11 can be exploited. Users of hosts with "ad hoc mode" enabled may unintentionally allow users to inadvertently or maliciously connect to those systems.	✓		
38.	Use static IP addressing on the network.	Using static IP addressing makes it more difficult for a hostile user to connect to the network.		✓	
39.	Enable user authentication mechanisms for the management interfaces of the AP.	User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.	✓		
40.	Ensure that management traffic destined for APs is on a dedicated wired subnet.	Passing management traffic over an "out of band' network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.	✓		
41.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	SNMPv3 has enhanced security features relative to its predecessor SNMP protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of APs.	✓		
Operational Recommendations					
42.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	Organizations that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Organizations should use SNMPv3.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
43.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	AP management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.	✓		
44.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	Using a local serial port interface for AP configuration ensures that sensitive management information does not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.		✓	
45.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.	Use of authentication mechanisms such as RADIUS and Kerberos can improve security and simplify user management.		✓	
46.	Deploy a wireless IDPS to detect suspicious behavior or unauthorized access and activity.	A wireless IDPS can detect and respond to potential malicious activities.		✓	
47.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.		✓	
48.	Deploy an IEEE 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.		✓	
49.	Enable utilization of key-mapping keys (IEEE 802.1X) rather than default keys so that sessions use distinct encryption keys. This type of security can be implemented through the use of IEEE 802.11i based FIPS 140-2 validated Level 2 encryption modules.	The use of distinct encryption keys provides more security than default keys and reduces the risk of key compromise.	✓		
50.	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.	✓		
51.	Designate an individual to track the progress of IEEE 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.	An appointed individual designated to track the latest technology enhancements, standards, and risks will help to ensure the continued secure implementation of wireless technology.		✓	

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
52.	Develop and implement a migration plan to upgrade or replace the existing WLAN infrastructure to support FIPS 140-2 validated IEEE 802.11i security.	Upgrade or replace firmware and hardware as required to support FIPS 140-2 validated IEEE 802.11i security, which is superior to IEEE 802.11a/b/g security.	✓		
53.	When disposing APs that will no longer be used by the organization, clear AP configuration to prevent disclosure of network configuration, keys, passwords, etc.	Sensitive or proprietary configuration settings should be cleared from access points before removing them from use or disposing to prevent inadvertent disclosure of the information to potentially malicious users.	✓		
54.	Enable the logging feature on APs to support logging and review the logs on a regular basis.	Ensure that the APs are set to perform logging. Also, review of audit and logging data helps to ensure user accountability. AP logs should be enabled and regularly reviewed for malicious activity.	✓		

5. Overview of Bluetooth Technology

This section expands on the Bluetooth information in Section 2, providing more in-depth detail on Bluetooth technology. The benefits, architecture, functionality, security vulnerabilities, and other aspects of Bluetooth are outlined in this section. The information provided in each sub-section serves to form a cohesive, foundational set of information regarding Bluetooth technology.

5.1 Bluetooth Overview

Bluetooth is an open standard for short-range RF communication. Bluetooth technology is used primarily to establish WPANs, commonly referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of devices, from cellular phones to automobiles. This allows users to form ad hoc and P2P networks between an increasing number of devices in order to transfer voice and data. Bluetooth is touted as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis, known as *piconets*. Piconets are comprised of two or more Bluetooth wireless devices in close physical proximity that are operating on the same channel and using the same frequency hopping sequence. Examples of piconets are Bluetooth-based connections between a cellular phone and a Bluetooth-enabled ear bud or PDA. As with other types of ad hoc networks, Bluetooth network topologies are often established on a temporary and changing basis.

5.1.1 Brief History

Bluetooth technology was originally conceived by Ericsson in 1994 and in 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Interest Group (SIG), which is a not-for-profit trade association developed to drive the development of Bluetooth products and serve as the governing body for Bluetooth specifications. The SIG began as a means to monitor the development of the radio technology and the creation of a global open standard. Today more than 6,000 companies are part of the Bluetooth SIG, comprising leaders in the telecommunications and computing industries that are driving the development and promotion of Bluetooth technology. Bluetooth was originally designed primarily as a cable replacement protocol for wireless communications, but Bluetooth is now being integrated into a broad range of consumer devices to enhance wireless connectivity. Examples of these devices are cellular phones, PDAs, laptops, automobiles, PC cards, printers, and headsets. Bluetooth is standardized within the IEEE 802.15 Working Group for Wireless Personal Area Networks that formed in early 1999 as IEEE 802.15.1-2002.[32] The Bluetooth SIG Web site serves as a good resource for Bluetooth-related information and provides numerous links to other Web sites with additional information.[33]

5.1.2 Frequency and Data Rates

Like the IEEE 802.11b/g WLAN standard, Bluetooth is designed to operate in the unlicensed 2.4 GHz–2.4835 GHz ISM frequency band. Numerous technologies operate in this band, making it somewhat crowded in the sense of wireless transmissions. Bluetooth uses Gaussian Frequency Shift Keying (GFSK) modulation and employs frequency hopping spread spectrum (FHSS) technology for all transmissions. FHSS is used to reduce interference and transmission errors, as well as provide a mild level of transmission security. Through the use of FHSS technology, communications between Bluetooth devices utilize 79 different radio channels by hopping frequencies about 1600 times per second. A channel is used for 625 microseconds, followed by a hop designated by a pre-determined pseudo-random sequence to

[32] For more information, see the IEEE Web site at http://grouper.ieee.org/groups/802/15/.
[33] For more information, see the Bluetooth Web site at http://www.bluetooth.com/.

another channel for another 625 microsecond transmission; this process is repeated continuously as part of the frequency hopping sequence.

The combination of a frequency-hopping scheme and radio link power control provide Bluetooth with some additional, albeit small, protection from eavesdropping and malicious access. The frequency-hopping scheme, primarily a technique to avoid interference, makes it slightly more difficult than direct sequence spread spectrum technologies, like IEEE 802.11, for an adversary to locate and capture Bluetooth transmissions. Using the power control feature appropriately forces any potential adversary to be in relatively close proximity to pose a threat to an established Bluetooth piconet.

Bluetooth version 1.1, outlined in the IEEE 802.15.1-2002 standard, and version 1.2 outline transmission speeds of up to 1 Mbps and achieve throughput of approximately 720 kbps. Bluetooth version 2.0 + Enhanced Data Rate (EDR) outlines data rates up to 3 Mbps and throughputs of approximately 2.1 Mbps.

Some of the key characteristics of Bluetooth technology are summarized in Table 5-1.

Table 5-1. Key Characteristics of Bluetooth Technology

Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 – 2.4835 GHz (ISM band).
Hop Frequency	1600 hops/second
Data Rate	v1.1 and v1.2 – 1 Mbps max user data rate v2.0 + EDR – 3 Mbps max user data rate
Data and Network Security	Three modes of security (none, service level, and link level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge-response for authentication, PIN-derived keys, and limited management.
Operating Range	About 9 meters (30 feet); can be extended to 91 meters or more
Throughput	v1.1 and v1.2 – 720 Kbps v2.0 + EDR – 2.1 Mbps
Positive Aspects	No wires and cables needed to transmit data between devices.
Negative Aspects	Possible interference with other ISM band technologies. Relatively low data rates. Signals leak outside desired boundaries.

5.1.3 Bluetooth Architecture and Components

Bluetooth permits devices to establish either P2P networks or infrastructure networks based on fixed Bluetooth APs, which facilitate communication between Bluetooth devices. This document focuses on ad hoc network topology piconets, which are much more prevalent than infrastructure-based Bluetooth networks. Ad hoc networks were developed to provide easy connection establishment between mobile devices that are in the same physical area (e.g., in the same room). In this architecture, Bluetooth-enabled client stations that are grouped into a single geographic area can be networked without the use of any infrastructure devices. A Bluetooth client is simply a device with a Bluetooth radio and software incorporating the Bluetooth protocol stack and interfaces.

The Bluetooth specification provides separation of duties for performing stack functions amongst a host and a controller. The host functions could be performed by a computing device like a laptop or desktop. The controller functions could be performed by an integrated or external (e.g., USB) Bluetooth dongle.

The controller is responsible for the lower stack layers including the Radio, Baseband, and Link Manager Protocol (LMP). The host is responsible for the higher layer protocols such as L2CAP and SDP. The host and controller send information to each other using the Host Controller Interface (HCI).

The basic Bluetooth topology is depicted in Figure 5-1. In Bluetooth piconets, one device serves as the master, with all other devices operating in the same piconet acting as slaves. Bluetooth piconets can scale to include up to seven slave devices.

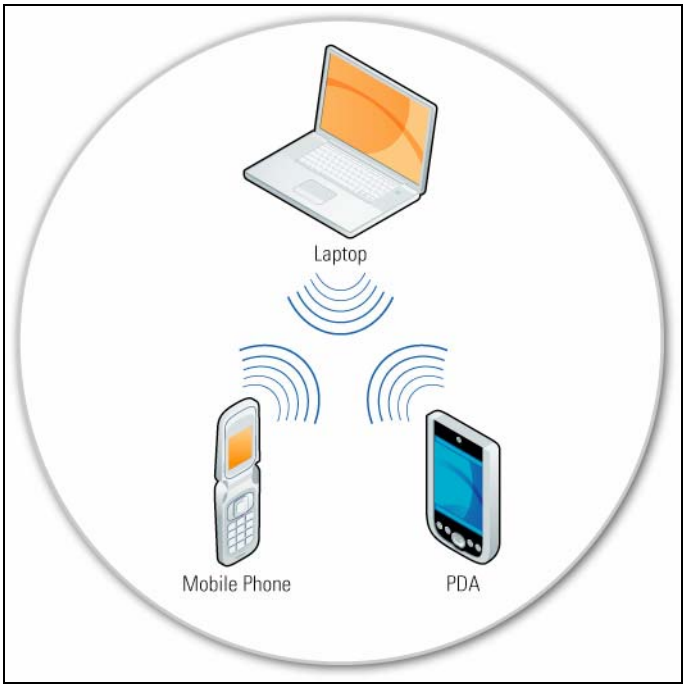

Figure 5-1. Bluetooth Ad Hoc Topology

The master device controls and establishes the network (including defining the network's hopping scheme). Although only one device may serve as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. Time division multiplexing (TDM) allows a device to perform both roles simultaneously. This series of piconets, often referred to as *scatternets*, allows several devices to be networked over an extended distance. This relationship also allows for a dynamic topology that may change during any given session, as a device moves toward or away from the master device in the network, the topology, and therefore the relationships of the devices in the immediate network may change. An example of a scatternet is depicted in Figure 5-2 through the connection of three separate piconets, Bluetooth Piconets 1, 2, and 3.

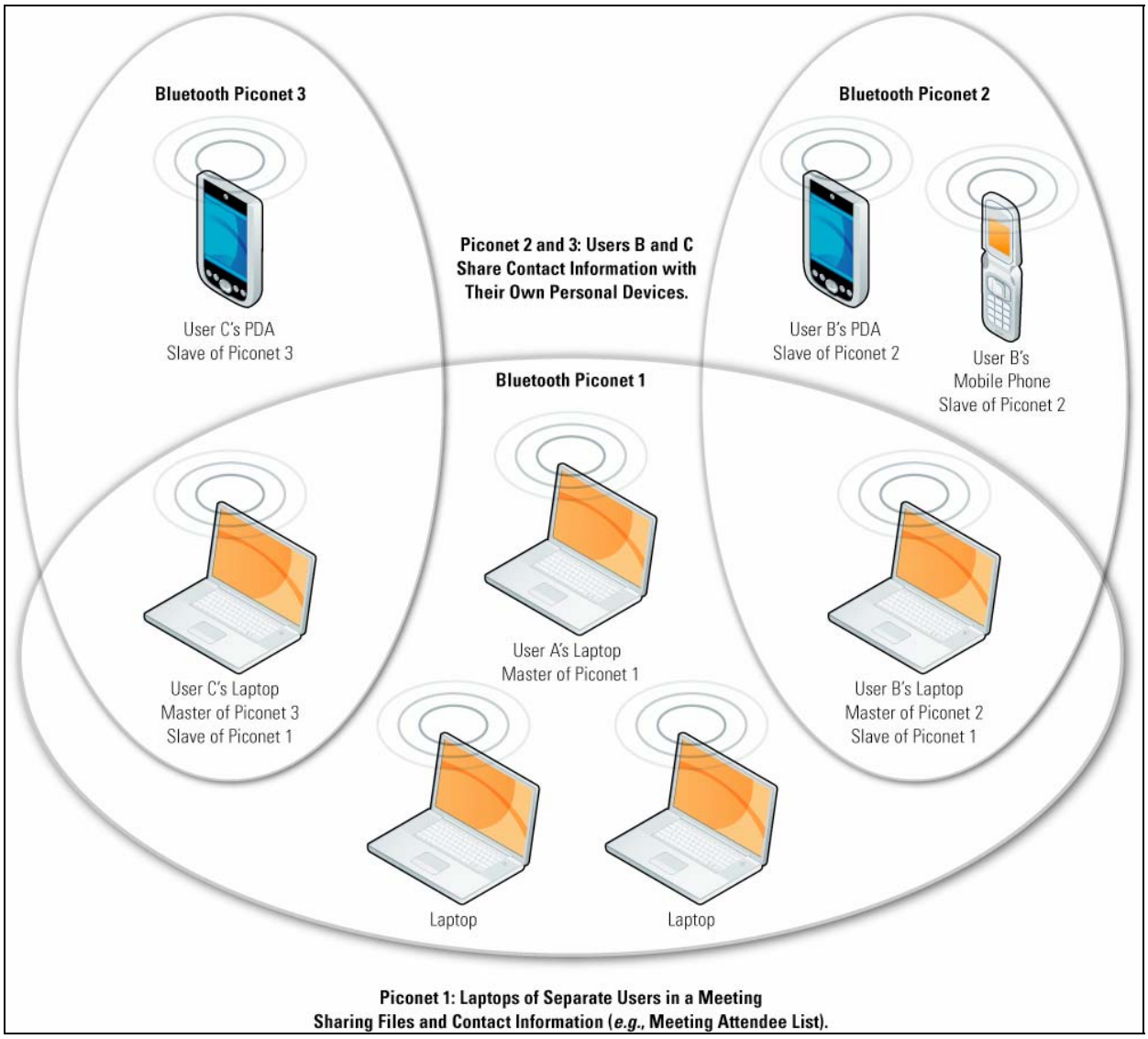

Figure 5-2. Bluetooth Networks (multiple scatternets)

Routing capabilities supported by Bluetooth networks control the changing network topologies of piconets and scatternets and assist in controlling the flow of data between networked devices, which supports the dynamic topology of Bluetooth networks.

Bluetooth uses a combination of packet-switching technology and circuit-switching technology. The use of packet switching in Bluetooth allows devices to route multiple packets of information over the same data path. This method does not consume all the resources of a data path, therefore allowing Bluetooth devices to maintain data flow throughout a scatternet.

5.1.4 Range

The range of Bluetooth devices is characterized by three different classes that define power management. Table 5-2 summarizes the three classes, including their power levels in milliwatts (mW) and decibels referenced to one milliwatt (dBm), and their operating ranges in meters (m). Most mobile phones are Class 2 devices, while Bluetooth USB adapters, headsets, and other Bluetooth enabled devices operate in

Classes 1-3. As with the data rates, it is anticipated that even greater distances will be achieved in the future.

Table 5-2. Bluetooth Device Classes of Power Management

Type	Power	Power Level	Operating Range (Designed)	Sample Devices
Class 1 Devices	High	100 mW (20 dBm)	Up to 91 meters (300 feet)	Bluetooth adapters (USB, headsets, and others)
Class 2 Devices	Medium	2.5 mW (4 dBm)	Up to 9 meters (30 feet)	Mobile devices and Bluetooth adapters, Smart Card Readers
Class 3 Devices	Low	1 mW (0 dBm)	Up to 1 meter (3 feet)	Bluetooth adapters

5.2 Benefits of Bluetooth

Bluetooth technology's ad hoc network topology offers communication flexibility and scalability between mobile devices. Efficiencies and cost savings attributed to the use of Bluetooth are attractive to both home and enterprise users. Bluetooth technology offers a number of key benefits, some of which are outlined below.

- **Cable replacement —** Bluetooth technology replaces cables for a variety of device connections. This includes cables traditionally used for peripheral devices (e.g., mouse and keyboard computer connections), printers, and wireless headsets and ear buds that interface with PCs or mobile phones.
- **Ease of file sharing** — Bluetooth enabled devices can easily form ad hoc wireless networks to support file sharing capabilities between multiple Bluetooth devices. For example, participants of a meeting with Bluetooth-compatible laptops could establish a piconet and share files with each other.
- **Wireless synchronization** — Bluetooth provides automatic synchronization between Bluetooth-enabled wireless devices. For example, contact information contained in electronic address books and date books as well as email can be synchronized between PDAs, laptops, mobile phones, and other devices via the use of Bluetooth.
- **Internet connectivity—**Bluetooth is supported by a variety of devices and applications. Some of these devices include mobile phones, PDAs, laptops, desktops, and fixed telephones. Internet connectivity is possible when these devices and technologies join to share capabilities. For example, a laptop, using a Bluetooth connection, can request a mobile phone to establish a dial-up connection; the laptop can then access the Internet through the connection established by the mobile phone.

5.3 Bluetooth Security

This section provides an overview of the security mechanisms included in the Bluetooth standard. An overview of the inherent Bluetooth security features is outlined to better illustrate limitations and provide a motivation for some of the recommendations for enhanced security. Security for the Bluetooth radio path is depicted in Figure 5-3.

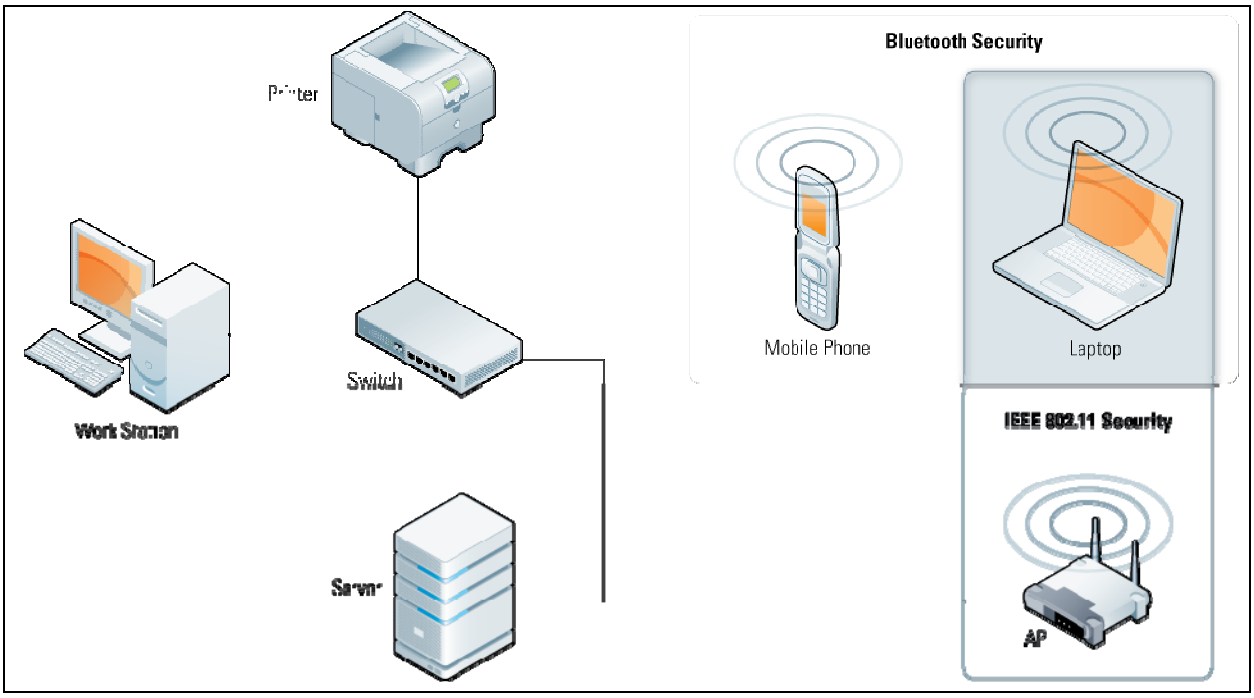

Figure 5-3. Bluetooth Air-Interface Security

As shown in Figure 5-3, Bluetooth security is only provided between the mobile phone and laptop, while IEEE 802.11 security protects the wireless link between the laptop and the AP. However, additional security would be required to secure the wired-side data transfers. Link authentication and encryption may be provided, but true end-to-end security is not possible without providing higher layer security solutions in addition to the security features included in the Bluetooth specification and IEEE 802.11 standard.

The following are the three basic security services defined by the Bluetooth standard:

- **Authentication**—A goal of Bluetooth is the identity verification of communicating devices. This security service addresses the question "Do I know with whom I am communicating?" This service provides an abort mechanism if a device cannot authenticate properly. This is device authentication only: user authentication is not provided by Bluetooth natively.
- **Confidentiality**—Confidentiality, or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by eavesdropping (passive attack). This service, in general, addresses the question "Are only authorized devices allowed to view my data?"
- **Authorization**—A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question "Has this device been authorized to use this service?"

The three security services offered by Bluetooth and details about the modes of security are described below. Bluetooth does not address other security services such as audit and non-repudiation. If these other security services are needed, they must be provided through additional means.

5.3.1 Security Features of Bluetooth Standard

Bluetooth has three different modes of security. Each Bluetooth device must operate in one of the following modes:

- **Security Mode 1**—Non-secure mode
  - No security is enabled
- **Security Mode 2**—Service level enforced security mode
  - Security mechanisms are not applied until after connection establishment
  - Allows for varying level of access defined by policy
- **Security Mode 3**—Link level enforced security mode
  - Security mechanisms are initiated before connection establishment

In Security Mode 1, a Bluetooth enabled device will not initiate any security procedures. In this non-secure mode, the security functionality (authentication and encryption) is bypassed, leaving the device and connections susceptible to attackers. In effect, Bluetooth devices operating in Mode 1 are in a "promiscuous" mode and do not employ any mechanisms to prevent other Bluetooth enabled devices from establishing connections.

In Security Mode 2, the service level enforced security mode, security procedures are initiated after channel establishment at the Logical Link Control and Adaptation Protocol (L2CAP) level. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to specific services and devices. The centralized security manager maintains policies for access control and interfaces with other protocols and device users. Varying security policies and "trust" levels to restrict access may be defined for applications with different security requirements operating in parallel. Therefore, it is possible to grant access to some services without providing access to other services. In this mode, the notion of authorization—the process of deciding if a specific device is allowed to have access to a specific service—is introduced. It is important to note that the authentication and encryption mechanisms used for Security Mode 2 are implemented at the LMP/Baseband layer (below L2CAP) just as with Security Mode 3.

In Security Mode 3, the link-level security mode, a Bluetooth device initiates security procedures before the channel is established. Bluetooth devices operating in Security Mode 3 require security procedures for all services or applications attempting to connect to the device. This mode supports authentication (unidirectional or mutual) and encryption. The authentication and encryption features are based on a separate secret key that is shared by connected devices, once the connection has been established.

Each of the following sections highlights a specific security component included in the Bluetooth standard. This section includes detail on Bluetooth bonding and link establishment, authentication, confidentiality, and other Bluetooth security mechanisms.

5.3.1.1 Link Key Generation—Bluetooth Bonding

According to the Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when users enter an identical PIN into one or both devices, depending on the configuration and device type. The PIN entry, device association, and key derivation are depicted

conceptually in Figure 5-4. The "E_x" boxes represent encryption algorithms that are used during the Bluetooth device association and key derivation processes. More details on the Bluetooth authentication and encryption procedures are outlined in Sections 5.3.1.2 and 5.3.1.3.

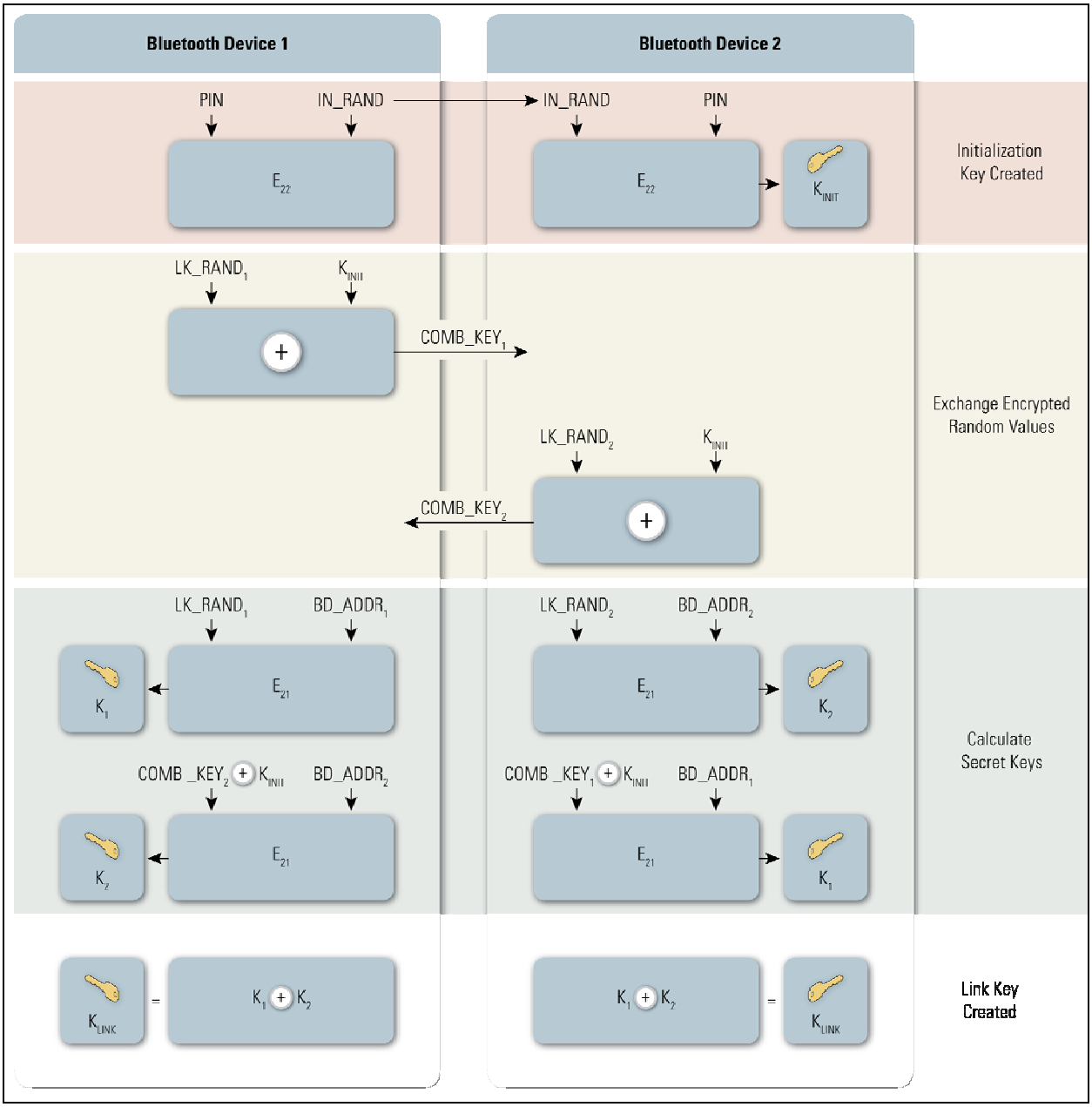

Figure 5-4. Bluetooth Key Generation from PIN

After initialization is complete, devices automatically and transparently authenticate and initiate the encryption procedure to secure the wireless link, if encryption is enabled. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4-digit PIN may be

sufficient for low-risk situations; however, a longer PIN should be used for devices that require a higher-level of security.[34]

5.3.1.2 Authentication

The Bluetooth authentication procedure is in the form of a "challenge-response" scheme. Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The claimant is the device attempting to prove its identity, and the verifier is the device validating the identity of the claimant. The challenge-response protocol validates devices by verifying the knowledge of a secret key—a Bluetooth link key. The challenge-response verification scheme is depicted conceptually in Figure 5-5. As shown, one of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier).

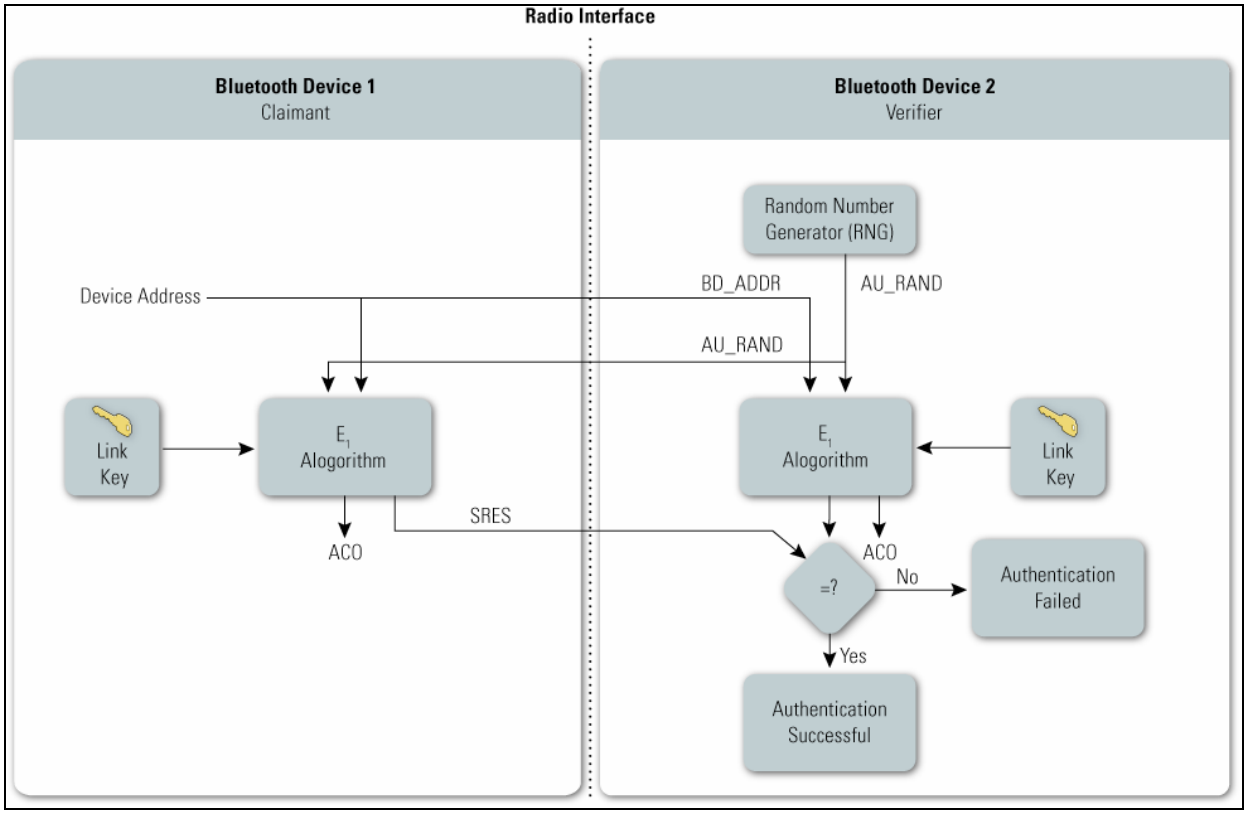

Figure 5-5. Bluetooth Authentication

The steps in the authentication process are the following:

Step 1. The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.

Step 2. The claimant uses the E_1 algorithm to compute an authentication response using his Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E_1 output will be used for authentication purposes. The remaining bits of the 128-bit output are known as the

[34] Bluetooth Security White Paper is available at http://www.bluetooth.com/.

Authentication Ciphering Offset (ACO) value, which will be used later to create the Bluetooth encryption key.

Step 3. The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier.

Step 4. The verifier compares the SRES from the claimant with the value that it computed.

Step 5. If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication has failed.

Step 6. For mutual authentication, the devices switch roles as claimant and verifier and repeat steps 1 through 5 above.

For mutual authentication, the above process is repeated with the verifier and claimant switching roles.

If authentication fails, a Bluetooth device will wait an interval of time before a new attempt is made. This time interval will increase exponentially to prevent an adversary from attempting to gain access by defeating the authentication scheme through trial-and-error with different keys. However, it is important to note that this "suspend" technique does not provide security against sophisticated adversaries performing offline attacks to exhaustively search PINs. The Bluetooth standard allows both uni-directional and mutual authentication to be performed. The E_1 authentication function used for the validation is based on the SAFER+ algorithm.[35]

Each Bluetooth device has a unique 48-bit address, which can be obtained through a device inquiry process. However, the private key, or link key, is not a public parameter. The link key is derived during initialization and is never disclosed outside the Bluetooth device nor transmitted over wireless links. However, the link key is passed in the clear from the host to the controller (e.g. PC to USB dongle) if the host is used for key storage. The random challenge, which is a public parameter part of the authentication process, is designed to be different on every transaction. The random number is derived from a pseudo-random process within the Bluetooth device. The cryptographic response is public as well and part of the encryption establishment process. The following are five key components of Bluetooth security:

- **Bluetooth Device Address**—A unique 48 bit address that is used to identify a Bluetooth-enabled device; also referred to as BD_ADDR
- **Random Challenge**—A 128-bit random number challenge (AU_RAND) used as part of the authentication process
- **Authentication Response (SRES)**—The response computed by the E_1 algorithm using the address, link key, and random challenge as inputs
- **Link Key—**A 128-bit secret key that is used by two devices to complete the authentication process
- **Encryption Key**—A shared secret key from 8 to 128 bits long that is used to encrypt data transfer as defined by Security Mode 2 or 3.

[35] A family of SAFER algorithms was developed by James Massey and used in Cylink Corporation products. SAFER stands for Secure And Fast Encryption Routine. The SAFER algorithms are iterated block ciphers (IBC). In an IBC, the same cryptographic function is applied for a specified number of rounds.

5.3.1.3 Confidentiality

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

- **Encryption Mode 1**—No encryption is performed on any traffic.
- **Encryption Mode 2**—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.
- **Encryption Mode 3**—All traffic is encrypted using an encryption key based on the master link key.

Encryption Modes 2 and 3 use the same encryption mechanism.

As shown in Figure 5-6, the encryption key provided to the encryption algorithm is produced using an internal key generator (KG). This key generator produces stream cipher keys based on the link key, a 128-bit random number (EN_RAND), and the ACO value. The ACO parameter, a 96-bit authenticated cipher offset, is another output produced during the authentication procedure shown in Figure 5-5. As mentioned above, the link key is the 128-bit secret key that is held in the Bluetooth devices and is not accessible to the user. Moreover, this critical security element is never transmitted outside the Bluetooth device.

The Bluetooth encryption procedure is based on a stream cipher, E_0. A key stream output is exclusive-OR-ed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR).[36] The encrypt function takes the following as inputs; the master identity (BD_ADDR), the 128-bit random number (EN_RAND), a slot number, and an encryption key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet, therefore the ciphering engine is also reinitialized with each packet, although the other variables remain static.

[36] LFSRs are used in coding (error control coding) theory and cryptography. LFSR-based key stream generators (KSGs), comprised of exclusive-OR gates and shift registers, are common in stream ciphers and are very fast in hardware.

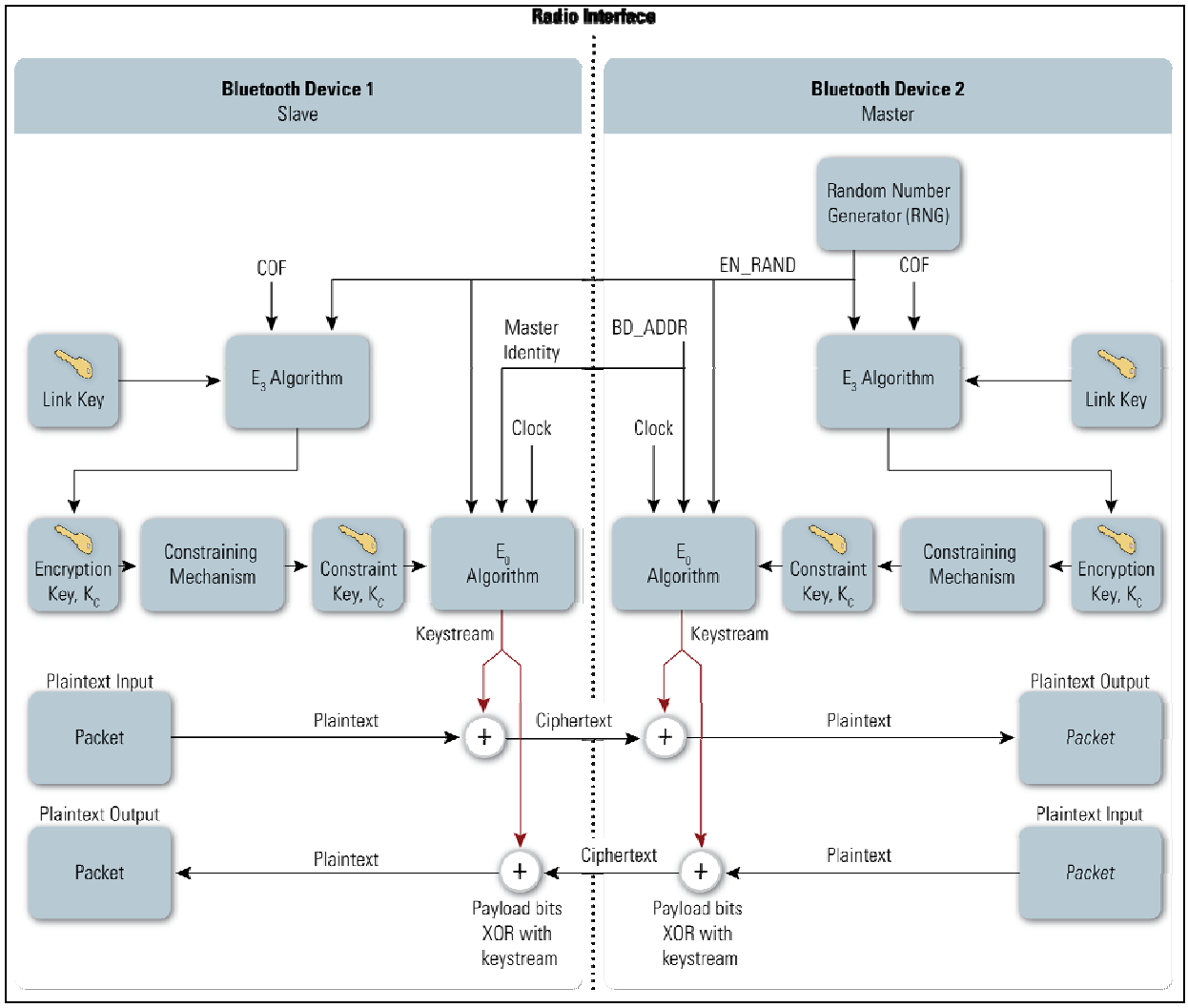

Figure 5-6. Bluetooth Encryption Procedure

The encryption key (K_C) is generated from the current link key and may vary from 8 bits to 128 bits. The negotiation process occurs between master devices and slave devices. During negotiation, a master device makes a key size suggestion for the slave. They initial key size suggested by the master is preset in its silicon by the manufacturer and is not always 128-bit. In product implementations, a "minimum acceptable" key size parameter can be set to prevent a malicious user from driving the key size down to the minimum of 8 bits, making the link insecure.

5.3.1.4 Trust Levels, Service Levels, and Authorization

In addition to the three security modes, Bluetooth allows two levels of trust and three levels of service security. The two Bluetooth levels of trust are "trusted" and "untrusted." Trusted devices have a fixed relationship with another device and have full access to all services. An untrusted Bluetooth device does not have an established relationship with another Bluetooth device, which results in the untrusted device receiving restricted access to services. Three levels of security have been defined for Bluetooth services. These levels are designed to allow the requirements for authorization, authentication, and encryption can be configured and altered independently.

The security levels can be described as follows:

- **Service Level 1—**Requires authorization and authentication. Automatic access is granted only to trusted devices; untrusted devices need manual authorization.
- **Service Level 2—**Requires authentication only; authorization is not necessary. Access to an application is allowed only after an authentication procedure.
- **Service Level 3—**Open to all devices, with no authentication required. Access is granted automatically.

Associated with these levels are the following security controls to restrict access to services: authorization required (this always includes authentication), authentication required, and encryption required (link must be encrypted before the application can be accessed).

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can get access only to specific services. It is important to understand that Bluetooth core protocols can only authenticate devices and not users. However, it is possible to initiate user-based access in an alternative manner. The Bluetooth security architecture (through the security manager) allows applications to enforce more granular security policies. The link layer, at which Bluetooth specific security controls operate, is transparent to the security controls imposed by the application layers. Thus it is possible to enforce user-based authentication and fine-grained access control within the Bluetooth security framework.

5.4 Bluetooth Security Problems

This section provides an overview of some of the known problems with Bluetooth. The Bluetooth security checklist addresses these vulnerabilities.

Table 5-3. Key Problems with Existing (Native) Bluetooth Security

	Security Issue or Vulnerability	Remarks
1	**Strength of the challenge-response pseudo-random generator is not known.**	The Random Number Generator (RNG) may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
2	**Short PINs are allowed.**	Weak PINs, which are used for the generation of link and encryption keys, can be easily guessed. Increasing the PIN length in general increases the security. People have a tendency to select short PINs.
3	**Lack of PIN management.**	Establishing PINs in large Bluetooth networks with many users may be difficult. Scalability problems frequently yield security problems.
4	**Encryption key length is negotiable.**	A standards group needs to develop a more robust initialization key generation procedure.
5	**Unit key is reusable and becomes public once used.**	Use a unit key as input to generate a random key. Use a key set instead of only one unit key.
6	**The master key is shared.**	A standards group needs to develop a better broadcast keying scheme.
7	**No user authentication exists.**	Only device authentication is provided. Application-level security and user authentication can be employed.

	Security Issue or Vulnerability	Remarks
8	**Attempts for authentication are repeated.**	A standards group needs to develop a limit feature to prevent unlimited requests. The Bluetooth specification requires a time-out period between repeated attempts that will increase exponentially.
9	**E_0 stream cipher algorithm is weak.**	A standards group needs to develop a more robust encryption procedure.
10	**Unit key sharing can lead to eavesdropping.**	A corrupt user may be able to compromise the security between two other users if the corrupt user has communicated with either of the other two users. This is because the link key (unit key), derived from shared information, has been disclosed.
11	**Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.**	Once the BD_ADDR is associated with a particular user, that user's activities could be logged, resulting in a loss of privacy.
12	**Device authentication is simple shared-key challenge-response.**	One-way-only challenge-response authentication is subject to man-in-the-middle attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that users and the network are legitimate.
13	**End-to-end security is not performed.**	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. Applications software above the Bluetooth software can be developed.
14	**Security services are limited.**	Audit, nonrepudiation, and other services are not part of the standard. If needed, these can be developed at particular points in a Bluetooth network.
15	**Discoverable and/or connectable devices are prone to attack**	Any device that must go into discoverable mode in order to pair should only do so for a minimal amount of time. A device should never be in discoverable mode all the time.

5.5 Bluetooth Security, Vulnerabilities, and Threats

Bluetooth offers several benefits and advantages, but the benefits of Bluetooth are not provided without risk. Bluetooth technology and enabled devices are susceptible to the general wireless threats outlined in Section 3, but are also threatened by more specific Bluetooth related attacks. These, more specific Bluetooth based vulnerabilities are outlined below.

- **Bluesnarfing** - Bluesnarfing enables attackers to gain access to a Bluetooth enabled device. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device and even the device's international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user's device to the attacker's device. This type of attack requires specific software and exploits a firmware flaw in older devices.

- **Bluejacking** - Bluejacking is an attack commonly conducted on Bluetooth-enabled mobile devices, such as cell phones, smart phones, and PDAs. A Bluejacking attack is initiated by an attacker sending unsolicited messages to a user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they are used to entice the user to respond in some fashion or add the new contact to the device's address book. This sort of message sending attack resembles spam and

phishing attacks conducted on email users. Bluejacking can cause harm when a user initiates a response to a Bluejacking message that is sent with a harmful purpose.

- **Bluebugging** - Bluebugging exploits a security flaw in Bluetooth enabled device firmware to gain access to the device and its commands. This attack uses the commands of the device without informing the user, allowing the attacker access to data, place phone calls, eavesdrop on phone calls, send messages, and exploit other services or features offered by the device. The firmware flaw exploited by Bluebugging is generally found in older devices and can potentially be mitigated with firmware upgrades.

- **Car Whisperer** - Car whisperer is a software tool developed by European security researchers that exploits a key implementation issue in hands-free Bluetooth car-kits installed in automobiles. The car whisperer software allows an attacker to send to or receive audio from the car-kit. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop) from the microphone in the car.

- **Denial of Service** – Like other networking technologies, Bluetooth is susceptible to DoS attacks. However, these types of attacks differ in regards to Bluetooth as they are not only directed at making a device's Bluetooth interface unusable, but also can be used to drain the mobile device's battery. These types of attacks are not significant and due to the proximity required for Bluetooth use can easily be averted by simply walking away, along with other mitigation techniques.

- **Fuzzing Attacks** – Commercial Bluetooth fuzzers are available that can cause problems from degradation of service to device reset. Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. When a device's response is slowed or otherwise stopped by these attacks, this is an indication that a potential serious vulnerability exists in the protocol stack. It is important the vendors test the robustness of their Bluetooth stack implementation before making their products available.

5.6 Risk Mitigation and Countermeasures

Although Bluetooth is susceptible to a number of general wireless threats and specific Bluetooth threats, countermeasures can be taken to mitigate known risks. This section outlines Bluetooth countermeasures that are in addition to the authentication, authorization, and confidentiality security mechanisms described in Section 5.3 regarding Bluetooth security. These additional countermeasures include various operational methods and additional software and hardware that go beyond the security structure of the Bluetooth standard. General mitigation techniques for wireless devices can be found in Section 3; specific Bluetooth countermeasures are included in this section.

The first line of defense is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth-enabled devices. Organizations using Bluetooth technology need to establish and document security policies that address the use of Bluetooth-enabled devices and users' responsibilities. Organizations should include awareness-based education to support staff understanding and knowledge of Bluetooth. Policy documents should include a list of approved uses for Bluetooth, the type of information that may be transferred over established Bluetooth networks, and any disciplinary actions that may result from misuse. The security policy should also specify a proper password usage scheme. General guidelines for developing security policies can be obtained from NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*.[37]

The general obscurity and mobility of Bluetooth enabled devices increases the difficulty of employing traditional security measures. However, a number of countermeasures can be enacted to secure Bluetooth

[37] NIST SP 800-100, *Information Security Handbook: A Guide for Managers* is available at http://csrc.nist.gov/publications/nistpubs/.

devices, ranging from distance and power output to general operation practices. Outlined below are several countermeasures that can be employed to secure Bluetooth devices and communications.

Authentication. Bluetooth devices can store and automatically access link keys, outlined in Section 5.3, from memory and automatically pair with certain devices. Incorporating application-level software that requires password authentication to secure the device will add an extra layer of security. Again, passwords are fundamental measures, adding an extra layer of security. Additional authentication mechanisms, such as biometrics and smart cards, can be used to provide strong authentication to Bluetooth devices. More details on authentication mechanisms are included in Section 4.5.3.4.

Encryption. Higher layer encryption (especially FIPS 140-2 validated) will also add an additional layer of security. Bluetooth PIN cracking tools are readily available that make current native encryption mechanisms breakable. Employing stronger encryption techniques over the native encryption (e.g., at the RFCOMM layer) will further protect the data in transit.

Disable Bluetooth. Bluetooth capabilities should be disabled on all Bluetooth devices, except when the user explicitly enables Bluetooth to establish a trusted connection. As a secondary procedure, operational Bluetooth interfaces should be configured in non-discoverable mode, which prevents visibility to other Bluetooth devices.

PIN Length. The PIN on Bluetooth devices should be changed to at least an eight character alphanumeric PIN code, if possible. This will increase the security of the pairing function and increase the PIN identification difficulty. According to the Bluetooth specification, the Bluetooth PIN is not a value that comes with a device, except for some devices that do not support a user interface and are configured by the vendor with fixed PINs—PINs that are provided by the device manufacturer that cannot be changed. In this case, although weak, the use of a fixed PIN is acceptable for devices that do not have a user interface.

Pairing Security. Bluetooth devices should be paired in a private physical setting to minimize the risk of eavesdropping or other potential attacks. Users should never respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the user's devices.

Pairing Management. In the event a Bluetooth capable device is lost or stolen, users should immediately unpair the missing device from all other Bluetooth devices with which it was previously paired. This will prevent an attacker from using the lost or stolen device to access another trusted Bluetooth device owned by the user.

Non-Discoverable Mode. The default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names. Again, disabling the Bluetooth interface when not in use and operating the Bluetooth device only in non-discoverable mode will increase the operational security of Bluetooth devices. It is important that devices remain in a non-discoverable and non-connectable state except as needed to make trusted connections.

Spatial Distance. Establishing spatial distance requires setting the power requirements low enough to prevent a device from having sufficient power to be detected from outside a physical area (e.g., outside the office building). This spatial distance in effect creates a more secure perimeter. Currently, Bluetooth devices have a useful range of approximately three feet (with a class 3 device). Organizations with requirements for high levels of security may restrict unauthorized personnel from using PDAs, laptops, and other electronic devices within the secure perimeter for added security.

Transmission Control. Users should not accept transmission of any sorts from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the

number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept transmission from these trusted devices.

Additionally, Bluetooth-enabled devices, as with all other wireless devices, should follow the security guidelines described in Sections 4.5.3.2 and 4.5.3.3, which includes outlining the use of personal firewalls, software patches, antivirus protection, policy enforcement, and data-at-rest security.

5.7 Bluetooth Security Checklist

Table 5-4 provides a Bluetooth security checklist. The table presents guidelines and recommendations for creating and maintaining a secure Bluetooth wireless network. For each recommendation or guideline, a justification column lists areas of concern for Bluetooth devices, the security threats and vulnerabilities associated with those areas, risk mitigations for securing the devices from these threats, and vulnerabilities. Additionally, with each recommendation and justification, a checklist with three columns is provided. The first column, the "Recommended Practice" column, if checked, means that this entry represents something recommended for all organizations. The second column, the "Should Consider" column, if checked, means that the entry's recommendation is something that an organization should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the "Should Consider" column is checked, organizations should carefully consider the option and weigh the costs versus the benefits. The last column, "Status", is intentionally left blank to allow organization representatives to use this table as a true checklist. For instance, an individual performing a wireless security audit in a Bluetooth environment can quickly check off each recommendation for the organization, asking, "Have I done this?"

Table 5-4. Bluetooth Security Checklist

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
Management Recommendations					
1	Develop an organization security policy that addresses the use of wireless technology including Bluetooth technology.	A security policy is the foundation on which other countermeasures (operational and technical) are rationalized and implemented. A documented security policy allows an organization to define acceptable implementations and uses for Bluetooth technology.	✓		
2	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (i.e., Bluetooth).	A security awareness program helps users to establish good security practices in the interest of preventing inadvertent or malicious intrusions into an organization's automated information system.	✓		
3	Perform a risk assessment to understand the value of the assets in the organization that need protection.	Understanding the value of organizational assets and the level of protection required enables the engineering of a wireless solution that provides an appropriate level of security.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
4	Perform comprehensive security assessments at regular intervals to fully understand the wireless network security posture.	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.	✓		
5	Ensure that the wireless "network" is fully understood. With piconets forming scatter-nets with possible connections to IEEE 802.11 networks and connections to both wired and wireless wide area networks. An organization must understand the overall connectivity. Note: a device may contain various wireless technologies and interfaces.	A thorough understanding of the functionalities and configurations of the deployed wireless network technologies allows an organization to identify possible risks and vulnerabilities. These risks and vulnerabilities can then be addressed in the wireless security policy and enforced appropriately.	✓		
6	Ensure external boundary protection is in place around the perimeter of the building or buildings of the organization.	To prevent malicious physical access to an organization's information system infrastructure, the external boundaries should be secured through means such as a fence or locked doors.	✓		
7	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	Identification badges or physical access cards should be deployed to ensure that only authorized personnel have physical access to a facility.	✓		
8	Ensure that handheld or small Bluetooth devices are protected from theft.	The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.	✓		
9	Ensure that Bluetooth devices are turned off during all hours when they are not used.	Shutting down Bluetooth devices when not in use minimizes exposure to potential malicious activities.	✓		
10	Take a complete inventory of all Bluetooth-enabled wireless devices.	A complete inventory list of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.	✓		
11	Study and understand all planned Bluetooth-enabled devices to understand any security idiosyncrasies or inadequacies.	An understanding of the security implications of Bluetooth will help the organization better address the associated risks.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
Technical Recommendations					
12	Change the default settings of the Bluetooth device to reflect the organization's security policy.	Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the company security policy.	✓		
13	Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.	Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users.	✓		
14	Ensure that the Bluetooth "pairing" environment is secure from eavesdroppers (i.e., the environment has been visually inspected for possible adversaries before the initialization procedures during which key establishment occur).	The key establishment is a vital security function and requires that users maintain a security awareness of possible eavesdroppers.	✓		
15	Choose PIN codes that are sufficiently random and avoid all weak PINs.	PIN codes should be random so that they would not be easily guessed by malicious users.	✓		
16	Choose PIN codes that are sufficiently long.	PIN codes with maximum lengths of 16 bytes make them more resistant to brute force attacks.	✓		
17	Ensure that no Bluetooth device is defaulting to the zero PIN.	Bluetooth devices defaulting to the zero PIN (e.g., 0000) essentially provide no security.	✓		
18	Configure Bluetooth devices to delete PINs after initialization to ensure that PIN entry is required every time and that the PINs are not stored in memory after power removal.	Requiring PIN entry after re-initialization prevents the possibility of a PIN being recovered from the memory of a stolen device.	✓		
Operational Recommendations					
19	Ensure that combination keys are used instead of unit keys.	The use of shared unit keys can lead to successful man-in-the-middle attacks.	✓		
20	Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).	Link encryption should be used to secure all data transmissions during a Bluetooth connection.	✓		
21	Ensure that encryption is enabled on every link in the communication chain.	Every link should be secured because one unsecured link results in compromising the entire communication chain.	✓		
22	Make use of Security Mode 2 in controlled and well-understood environments.	Security Mode 2 provides authorized access to services.	✓		

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
23	Ensure device mutual authentication for all accesses.	Mutual authentication is required to provide verification that all devices on the network are legitimate.	✓		
24	Enable encryption for all broadcast transmissions (Encryption Mode 3).	Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.	✓		
25	Configure encryption key sizes to the maximum allowable.	Using maximum allowable key sizes provides protection from brute force attacks.	✓		
26	Establish a “minimum key size” for any key negotiation process.	Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. Preferably 128-bit key sizes should be used.	✓		
27	Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.	Authenticating users to a portable Bluetooth device is a good security practice in the event the device is stolen, which provides a layer of protection for an organization’s Bluetooth network.	✓		
28	Use application-level (on top of the Bluetooth stack) encryption and authentication for highly sensitive data communication.	Application-level encryption and authentication provide security on top of the Bluetooth link encryption; the overlay increases the security of communication.		✓	
29	Use smart card technology in the Bluetooth network to provide key management.	The use of smart card technology can simplify the distribution and management of keys while maintaining strong security.		✓	
30	Install antivirus software on intelligent, Bluetooth-enabled hosts.	Antivirus software should be installed on a Bluetooth-enabled host to insure that known viruses are not introduced to the Bluetooth network.	✓		
31	Fully test and deploy Bluetooth software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should be fully tested before implementation to ensure that they work.	✓		
32	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong authentication mechanisms can minimize the vulnerabilities associated with passwords and PINs.		✓	
32	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or network-based agents) deployed on the wireless network can detect and respond to potential malicious activities.		✓	

	Security Recommendation	Security Need, Requirement or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
34	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements prior to implementation.	✓		
35	Designate an individual to track the progress of Bluetooth security products and standards (perhaps via the Bluetooth SIG) and the threats and vulnerabilities with the technology.	An appointed individual designated to track the latest technology enhancements, standards (perhaps via Bluetooth SIG), and risks will help to ensure the continued secure use of Bluetooth.		✓	
36	Wait until future releases of Bluetooth technology incorporate fixes to the security features or offer enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the Bluetooth products with major security vulnerabilities that have not been fixed.		✓	

Appendix A—Common Wireless Frequencies and Applications

EM Band Designation	Frequency Range	Wireless Device/Application
VLF: Very Low Frequency	9 kHz–30 kHz	Pipeline inspection gauges (20 kHz) Submarine communication devices (<30 kHz)
LF: Low Frequency	30 kHz–300 kHz	Submarine communications and ocean depth measurement devices (<50 kHz) RFID (125-134.2 kHz, 140-148.5 kHz)
MF: Medium Frequency	300 kHz–3 MHz	AM radio stations (535 kHz–1 MHz)
HF: High Frequency	3 MHz – 30 MHz	RFID (13.56 MHz) CB radios (~27 MHz)
VHF: Very High Frequency	30 MHz–300 MHz	FM radio stations (88-108 MHz) Amateur radio (50-54 MHz, 144-148 MHz, 222-225 MHz) Military VHF-FM (30-88 MHz) VHF TV channels 2–13, NTSC Standard (54-72 MHz, 76-88 MHz, 174 MHz–216 MHz) Garage door openers (~40 MHz) Standard cordless telephones (40 MHz–50 MHz) Alarm Systems (~40 MHz) Paging Systems (50 MHz–300 MHz)
UHF: Ultra High Frequency	300 MHz–3 GHz	Paging systems (300 MHz–500 MHz) RFID (902-928 MHz) UHF TV channels 14-69 (470-806 MHz) Satellite radio (2.310-2.360 GHz) Bluetooth/ IEEE 802.15.1 devices (2.4-2.4835 GHz) Wi-Fi/ IEEE 802.11x (2.4-2.5 GHz ISM Bands) ZigBee/ IEEE 802.15.4 devices (2.4 GHz, 915 MHz, 868 MHz ISM Bands)
SHF: Super High Frequency	3 GHz–30 GHz	Wireless USB/ IEEE 802.15.3a (3.1-10.6 GHz) WirelessHD (3.1-10.6 GHz) WiBree (2.4 GHz ISM Band) UWB/ IEEE 802.15.4a (3.1 – 10.6 GHz) Wi-Fi/ IEEE 802.11a (5.15-5.875 GHz ISM Bands) WiMAX / IEEE 802.16x (2-11 GHz, 10-66 GHz) LMDS (26 GHz, 29 GHz, 31.0-31.3 GHz)
EHF: Extremely High Frequency	30 GHz–300 GHz	Wi-Fiber (71-76 GHz, 81-86 GHz, 92-95 GHz)
IR: Infrared	300 GHz	Remote controls for home audio-visual components IR links for peripheral devices PDA and cellular telephone IR links

Appendix B—Glossary of Terms

Selected terms used in the publication are defined below.

Access Point (AP): A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Ad Hoc Network: A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station.

Base Station: A two-way radio installed at a fixed location to provide wireless access for WMAN clients.

Claimant: The Bluetooth device attempting to prove its identity to the verifier during the Bluetooth connection process.

Flooding: An attacker sending large numbers of wireless messages at a high rate to prevent the wireless network from processing legitimate traffic.

Infrared (IR): An invisible band of radiation at the lower end of the electromagnetic spectrum. It starts at the middle of the microwave spectrum and extends to the beginning of visible light. Infrared transmission requires an unobstructed line of sight between transmitter and receiver. It is used for wireless transmission between computer devices, as well as for most handheld remotes for TVs, video, and stereo equipment.

Infrastructure Network: A wireless network that requires the use of an infrastructure device, such as an access point or a base station, to facilitate communication between client devices.

Jamming: A device emitting electromagnetic energy on a wireless network's frequency to make it unusable.

Media Access Control (MAC): A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.

Piconet: A small Bluetooth network created on an ad hoc basis that includes two or more devices.

Range: The maximum possible distance for communicating with a wireless network infrastructure or wireless client.

Robust Security Network (RSN): A wireless security network that only allows the creation of Robust Security Network Associations (RSNA).

Robust Security Network Association (RSNA): A logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, also known as the four-way handshake.

Scatternet: A series of piconets that allows several devices to be networked over an extended distance.

Service Set Identifier (SSID): A name assigned to a WLAN that allows stations to distinguish one WLAN from another.

Station (STA): A client device in a wireless network.

Verifier: The Bluetooth device that validates the identity of the claimant during the Bluetooth connection process.

Wired Equivalent Privacy (WEP): A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. However, WEP is no longer considered viable encryption mechanism due to known weaknesses.

Wireless Bridge: A device that links two wired networks, generally operating at two different physical locations, through wireless communications.

Wireless Local Area Network (WLAN): A group of wireless AP and associated infrastructure within a limited geographic area, such as an office building or building campus, that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility.

Wireless Metropolitan Area Network (WMAN): A wireless network that provides connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

Wireless Personal Area Network (WPAN): A small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.

Wireless Wide Area Network (WWAN): A network that connects individuals and devices over large geographic areas. WWANs are typically used for cellular voice and data communications, as well as satellite communications.

Wireless Technology: A technology that enables one or more devices to communicate without physical connections.

Appendix C—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the publication are defined below.

3G	Third Generation
ACL	Access Control List
ACO	Authenticated Cipher Offset
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CCK	Complementary Code-Keying
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CRC	Cyclic Redundancy Check
dBm	Decibels referenced to one milliwatt
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Control Protocol
DoD	Department of Defense
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EDR	Enhanced Data Rate
EM	Electromagnetic
ESS	Extended Service Set
ETSI	European Telecommunications Standard Institute
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
GFSK	Gaussian Frequency Shift Keying
GHz	Gigahertz
HCI	Host Controller Interface
HIPERLAN	High Performance Radio Local Area Network
HMAC	Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
IBSS	Interdependent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	Internet Packet Exchange
IR	Infrared
ISM	Industrial, Scientific, and Medical
IT	Information Technology
ITL	Information Technology Laboratory
IV	Initialization Vector
Kbps	Kilobits per second
KG	Key Generator
KHz	Kilohertz
KSG	Key Stream Generator
L2CAP	Logical Link Control and Adaptation Protocol
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LFSR	Linear Feedback Shift Register
MAC	Medium Access Control
Mbps	Megabits per second
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple Input, Multiple Output
mW	Milliwatt
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NLOS	Non-Line-of-Sight
NVD	National Vulnerability Database
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OMB	Office of Management and Budget
P2P	Peer to Peer
PAN	Personal Area Network
PBCC	Packet Binary Convolutional Coding
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PHY	Physical Layer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPTP	Point-to-Point Tunneling Protocol
PtP	Point-to-Point
QoS	Quality of Service

RADIUS	Remote Authentication Dial-in User Service
RF	Radio Frequency
RNG	Random Number Generator
RSA	Rivest-Shamir-Adelman
RSN	Robust Security Network
RSNA	Robust Security Network Association
SIG	Special Interest Group
SNMP	Simple Network Management Protocol
SOFDMA	Scalable Orthogonal Frequency Division Multiple Access
SP	Special Publication
SRES	Signed Response
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmission Power Control
UNII	Unlicensed National Information Infrastructure
USB	Universal Serial Bus
UWB	Ultrawideband
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIDPS	Wireless Intrusion Detection and Prevention System
WIMAX	World Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks
WWAN	Wireless Wide Area Network

Appendix D—Summary of IEEE 802.11 Standards

Table D-1 provides a summary of the various IEEE 802.11 standards. Each of the standards outlined in the table below include a description, purpose keywords and remarks about the standard, and estimated product availability.

Table D-1. Summary of IEEE 802.11 Standards

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11a	A physical layer standard that operates in the 5 GHz UNII radio band. It specifies eight available radio channels (in some countries, 12 channels are permitted). The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Higher Performance.** In most office environments, the data throughput will be greater than for IEEE 802.11b. In addition, the greater number of non-overlapping radio channels (eight as opposed to three) provides better protection against possible interference from neighboring access points.	This standard was completed in 1999. Products are available now.
802.11b	This is a physical layer standard in the 2.4 GHz ISM radio band. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Performance.** Installations may suffer from speed restrictions in the future, as the number of active users increase, and the limit of three non-overlapping channels may cause interference from neighboring access points.	This standard was completed in 1999. Wide varieties of products have been available since 2001.
802.11d	This standard is supplementary to the Media Access Control (MAC) layer in IEEE 802.11 to promote worldwide use of IEEE 802.11 WLANs. It will allow APs to communicate information on the permissible radio channels with acceptable power levels for user devices. The IEEE 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use.** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	This standard was completed in 2001. Products are available now.
802.11e	This standard is supplementary to the MAC layer to provide QoS support for WLAN applications. It will apply to IEEE 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QoS for data, voice, and video applications.	**Quality of service.** This standard provides some useful features for differentiating data traffic streams. It is essential for future audio and video distribution.	This standard was completed in 2005. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11f	This is a "recommended practice" document that aims to achieve AP interoperability within a multi-vendor WLAN network. The standard defines the registration of APs within a network and the interchange of information between access points when a user is handed over from one AP to another.	**Interoperability.** This standard will work to increase vendor interoperability, reduce vendor lock-in, and allow multi-vendor infrastructures.	This recommended practice was completed in 2003. Products are available now.
802.11g	This is a physical layer standard for WLANs in the 2.4 GHz ISM radio band. The maximum link rate is 54 Mbps per channel whereas IEEE 802.11b offers 11 Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with IEEE 802.11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Higher Performance with IEEE 802.11b backward compatibility.** This standard provides speeds similar to IEEE 802.11a and backward compatibility with IEEE 802.11b.	This standard was completed in 2003. Products are available now.
802.11h	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance.** This is necessary for products to operate in Europe. Completion of IEEE 802.11h will provide better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by ETSI. Although European countries such as the Netherlands and the United Kingdom are likely to allow the use of 5 GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003 or later.	This standard was completed in 2003. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11i	This standard is supplementary to the MAC layer to improve security. It applies to IEEE 802.11 physical standards a, b, and g. It provides improved security over Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of IEEE 802.11i.	**Improved security.** 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), using AES. Federal agencies are required to use FIPS-validated cryptographic modules.[38] NIST SP 800-97 contains specific recommendations and guidance for IEEE 802.11i.	This standard was completed in 2004. Products are available now.
802.11k	This standard defines Radio Resource Measurement enhancements to provide management and maintenance interfaces to higher layers for mobile WLANs.	**Resource Radio Management** This standard will enable seamless Basic Service Set (BSS) transitions between WLANs through the discovery of the best available AP and improve network traffic by distributing users to under-utilized APs.	This standard is expected to be finalized by the second half of 2007.
802.11m	This is a supplementary maintenance standard to the IEEE 802.11-1999 (reaff. 2003) standard	**Editorial Maintenance** This initiative is to perform editorial maintenance, corrections, improvements, clarifications, and interpretations to the IEEE 802.11-1999 (reaff. 2003) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications standard.	
802.11n	This standard investigated the possibility of improving the 802.11 standard to provide high throughput at a theoretical 540 Mbps.	**Increased Data Throughput** The purpose of this standard is to improve the IEEE 802.11 WLAN user experience by providing significantly higher throughput using multiple-input multiple output (MIMO) antennas/receivers and different coding schemes.	This standard is expected to be completed in 2008.

[38] 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.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11p	This standard is an amendment of IEEE 802.11 to support communication between vehicles and the roadside and between vehicles while operating at speeds up to a minimum of 200 km/h for communication ranges up to 1000 meters. The amendment will support communications in the 5 GHz bands; specifically 5.850-5.925 GHz band within North America with the aim to enhance the mobility and safety of all forms of surface transportation, including rail and marine. Amendments to the PHY and MAC will be limited to those required to support communications under these operating environments within the 5 GHz bands. This standard is also referred to as the Wireless Access for Vehicular Environment (WAVE).	**Wireless Access for Vehicles** This standard amends the existing IEEE 802.11 standard to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments, and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50ms).	This standard is scheduled to be completed in April 2009.
802.11r	This standard is supplementary to the IEEE 802.11 Medium Access Control (MAC) layer and creates improvements to minimize or eliminate the amount of time data connectivity between the Station (STA) and the Distribution System (DS) during a Basic Service Set (BSS) transition.	**Fast BSS Transitions** This standard improves Basic Service Set (BSS) handoffs within IEEE 802.11 networks. This is a critical component to support real time constraints imposed by applications such as Voice over Internet Protocol (VoIP).	This standard is scheduled to be completed in 2007.
802.11s	This standard defined the IEEE 802.11 Extended Service Set (ESS) Mesh with an IEEE 802.11 Wireless Distribution System (WDS) using the IEEE 802.11 MAC/PHY layers that supports both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies.	**ESS Mesh Networking** This standard provides a protocol for auto-configuring paths between Access Points (AP) over self-configuring multi-hop topologies in a Wireless Distribution System (WDS) to support both broadcast/multicast and unicast traffic in an ESS Mesh using the four-address frame format or an extension.	This standard is scheduled to be completed in 2008.
802.11t	This is a “recommended practice” and will provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of IEEE 802.11 WLAN devices and networks at the component and application level as a recommended practice.	**Wireless Performance Protection** To enable testing, comparison, and deployment planning of IEEE 802.11 WLAN products so that performance and products specifications can be captured through common and accepted set of performance metrics, measurement methodologies and test conditions.	This recommended practice is scheduled to be completed in 2008.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11u	This standard is an amendment the IEEE 802.11 MAC and PHY to support InterWorking with External Networks.	**Internetworking with External Networks** This will provide amendments to the IEEE 802.11 PHY/MAC layers, which will enable InterWorking with other networks, granting limited access, based on a relationship with an external network. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for InterWorking.	This standard is in the proposal evaluation stages and a scheduled completion date has not been set.
802.11v	This standard will create amendments to provide Wireless Network Management enhancements to the IEEE 802.11 MAC, and PHY, to allow configuration of client devices connected to the network.	**Wireless Network Management** This will provide amendments to the IEEE 802.11 PHY/MAC layers that enable management of attached stations in a centralized or in a distributed fashion (e.g. monitoring, configuring, and updating) through a layer 2 mechanism. While the IEEE 802.11k Task Group is defining messages to retrieve information from the station, the ability to configure the station is not in its scope. The proposed Task Group will also create an Access Port Management Information Base (AP MIB).	This standard is in the early proposal stages and a scheduled completion date has not been set.
802.11w	This standard will enhance IEEE 802.11 MAC layer security for selected management frames by providing data integrity, data origin authenticity, replay protection, data confidentiality, and other security features.	**Management Frame Protection** This will extend the use of IEEE 802.11i to selected management frames to increase the overall security of IEEE 802.11-based networks. The increased level of security is intended to mitigate malicious network-based attacks, such as DoS attacks. Additionally, this amendment will provide security for sensitive network information that will be included in transmissions outlined in several new amendments, including IEEE 802.11r, IEEE 802.11k, and IEEE 802.11y.	The standard is currently under development and is expected to be completed and ratified in 2008.

Appendix E—References

The list below provides references for the publication.

Anderson, Gustave et al, "A Secure Wireless Agent-based Testbed", *Proceedings of the Second IEEE International Information Assurance Workshop*, 2004.

Baghaei, Nilufar and Hunt, Ray, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", *Proceedings of the 12th IEEE International Conference on Networks*, 2004.

Bargh, Mortaza et al, "Fast Authentication Methods for Handovers Between IEEE 802.11 Wireless LANs", *Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, 2004.

Becker, Bernd, Eisinger, Jochen, and Winterer, Peter, "Securing Wireless Networks in a University Environment", *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 2005.

Carli, Marco, Neri, A., and Rossetti, A., "Integrated Security Architecture for WLAN", *Proceedings of the IEEE 10th International Conference on Telecommunications*, 2003.

Chen, Jyh-Cheng, Jiang, Ming-Chia, and Liu, Yi-Wen, "Wireless LAN Security and IEEE 802.11i", *IEEE Wireless Communications*, February 2005.

Chen, Jyh-Cheng, Liu, Yi-Wen, and Wang, Yu-Ping, "Design and Implementation of WIRE1x", *Proceedings of Taiwan Area Network Conference*, 2003.

Edney, Jon and Arbaugh, William A., *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley, 2004.

Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi, "Weaknesses in the Key Schedule Algorithm of RC4", *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, 2001.

Gast, Matthew S., *802.11® Wireless Networks: The Definitive Guide (2nd Edtion)*, O'Reilly Media, 2005.

He, Changhua, and Mitchell, John, "Analysis of the 802.11i 4-Way Handshake", *Proceedings of the 2004 ACM Workshop on Wireless Security*, 2004.

IEEE Standard 802.11, 1999 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11-1999.pdf.

IEEE Standard 802.11i, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

IEEE Standard 802.1X, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.1X-2004.pdf.

Matsunaga, Yasuhiko et al, "Secure Authentication System for Public WLAN Roaming", *Proceedings of the First ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, 2003.

Mitsuyama, Yukio et al, "Embedded Architecture of IEEE 802.11i Cipher Algorithms", *Proceedings of the IEEE International Symposium on Consumer Electronics*, 2004.

O'Hara, Bob and Petrick, Al, *IEEE 802.11 Handbook: A Designer's Companion*, IEEE Press, 2001.

Schmoyer, Tim, Lim, Yu-Xi, and Owen, Henry, "Wireless Intrusion Detection and Response: A Case Study Using the Classic Man-in-the-middle Attack", *Proceedings of IEEE Wireless Communication and Networking Conference 2004*, 2004.

Smyth, Neil, McLoone, Máire, and McCanny, John, "Reconfigurable Hardware Acceleration of WLAN Security", *IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation*, 2004.

Šorman, Matija, Kovač, Tomislav, and Maurović, Damir, "Implementing Improved WLAN Security", *46th International Symposium Electronics in Marine*, 2004.

Wool, Avishai, "A Note on the Fragility of the 'Michael' Message Integrity Code", *IEEE Transactions on Wireless Communications*, Vol. 3 No. 5, September 2004.

You, Liyu and Jamshaid, Kamran, "Novel Applications for 802.11x Enabled Wireless Networked Home", *2004 IEEE Consumer Communications and Networking Conference*, 2004.

Appendix F—Online Resources

The lists below provide examples of online resources related to wireless network security that may be helpful to readers.

Documents

Name	URL
Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise	http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/
The DoD Public Key Infrastructure and Public Key-Enabling Frequently Asked Questions	http://iase.disa.mil/pki/faq-pki-pke-may-2004.doc
EAP Registry	http://www.iana.org/assignments/eap-numbers
FIPS 140-2, *Security Requirements for Cryptographic Modules*	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 180-2, *Secure Hash Standard (SHS)*	http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
FIPS 197, *Advanced Encryption Standard*	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
GAO-05-383, *Information Security: Federal Agencies Need to Improve Controls over Wireless* Networks	http://www.gao.gov/new.items/d05383.pdf
GRS 24, *Information Technology Operations and Management Records*	http://www.archives.gov/records-mgmt/ardor/grs24.html
Michael: An Improved MIC for 802.11 WEP	http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-020.zip
NIST Personal Identity Verification (PIV) Project	http://csrc.nist.gov/piv-program/
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-31, *Intrusion Detection Systems*	http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
NIST SP 800-40 version 2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*	http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf
NIST SP 800-63, *Electronic Authentication Guideline*	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

Name	URL
NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*	http://checklists.nist.gov/docs/SP_800-70_20050526.pdf
NIST SP 800-77, *Guide to IPsec VPNs*	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*	http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf
NIST SP 800-100, *Information Security Handbook: A Guide for Managers*	http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
NIST SP 800-113 (DRAFT), *Guide to SSL VPNs*	http://csrc.nist.gov/publications/drafts.html
Wi-Fi Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1	http://www.wi-fi.org/OpenSection/protected_access.asp (obtained from a link on this site for a fee)

Resource Sites

Name	URL
Bluetooth Special Interest Group	http://www.bluetooth.com/bluetooth/
Cellular Telecommunications and Internet Association (CTIA)	http://www.ctia.org/
Federal Communications Commission	http://www.fcc.gov/
FIPS-validated Cryptographic Modules	http://csrc.nist.gov/cryptval/
IEEE 802.11 Working Group on Wireless Local Area Networks	http://www.ieee802.org/11/
IEEE 802.15 Working Group for Wireless Personal Area Networks	http://www.ieee802.org/15/
IEEE 802.16 Working Group on Broadband Wireless Access Standards	http://www.ieee802.org/16/
International Engineering Consortium	http://www.iec.org/online/tutorials/eap_methods/
NIST National Vulnerability Database (NVD)	http://nvd.nist.gov/
NIST's Security Configuration Checklists Program for IT Products	http://checklists.nist.gov/
SNMP	http://www.snmp.com/snmpv3/
Wi-Fi Alliance	http://www.wi-fi.org/
Wi-Fi Alliance Certified WLAN Systems	http://www.wi-fi.org/OpenSection/certification_programs.asp?TID=2
Wireless Vulnerabilities & Exploits Homepage	http://www.wirelessve.org/