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

Special Publication 800-48

DRAFT

Wireless Network Security

802.11, Bluetooth™ and Handheld Devices

Tom Karygiannis
Les Owens

1
2 *NIST Special Publication 800-48*

Wireless Network Security

Recommendations of the National
Institute of Standards and Technology

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

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Note to Readers

This document is a publication of the National Institute of Standards and Technology (NIST) and is not subject to U.S. copyright. Certain commercial products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

For questions or comments on this document, contact Tom Karygiannis at sp800-48@nist.gov.

Acknowledgements

The authors wish to express their thanks to the numerous individuals who reviewed drafts of this document. In particular, several staff members at NIST provided valuable contributions to the technical content of this publication. In addition, the authors wish to express special thanks to _____, _____, _____, _____, _____ and _____ who contributed valuable comments and suggestions. [Specific individuals who assisted with this document will be identified by name at the conclusion of the 30-day public comment period.]

Table of Contents

List of Figures

List of Tables

Executive Summary

Wireless communications offer organizations and users many benefits such as portability and 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 office environment without the need for wires and without losing network connectivity. Less wiring means greater flexibility and efficiency and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and applications sharing between devices. Bluetooth can also eliminate cables for printer and other peripheral device connections. Handheld devices, such as Personal Digital Assistants (PDA and cell phones, allow remote users to synchronize personal databases, and they provide access to network services such as wireless e-mail, web browsing, and Internet access. Moreover these technologies offer dramatic cost savings and added capabilities to diverse applications ranging from the retail setting to the manufacturing shop floor to first responders.

Risks are inherent, however, 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 difference from wired networks and the main source of these risks is that with wireless networks the organization's underlying communications medium, the airwave, is openly exposed to intruders, making it the logical equivalent of placing 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. Malicious users may gain access to organizational systems and information and compromise the confidentiality of the organization, its users, and its network. These same users may corrupt the organization's data by spreading viruses, or they may simply launch attacks that prevent users from accessing the network.

Several public web sites provide maps of insecure wireless access points throughout the nation. Using this information, an intruder can gain access to network services, without being an authorized user of the access point or a member of the organization that owns it. Even if data confidentiality or integrity is not compromised, unauthorized users may steal bandwidth and cause a decrease in network performance, or may use a vulnerable wireless network as a platform for launching a network attack on a third party.

Specific threats and vulnerabilities to wireless networks and handheld devices 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 not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.

- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and 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 activity.
- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

This document provides an overview of wireless networking technologies and wireless handheld devices most commonly used in an office environment and by a mobile workforce today. This document seeks to assist organizations in reducing the risks associated with 802.11 wireless LANs and Bluetooth wireless networks and for ensuring security when using handheld devices.

NIST recommends the following actions:

Agencies should understand that maintaining a secure wireless network is an ongoing process that requires greater effort than for other networks and systems. Moreover, it is important that agencies more frequently assess risks and test and evaluate system security controls when wireless technologies are deployed.

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 the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

Agencies should not undertake wireless deployment for essential operations until they understand and can acceptably manage and mitigate the risks to their information, system operations, and risk to continuity of essential operations.

As described in this document, the risks provided by wireless technologies are considerable. Many current communications protocols and commercial products provide inadequate protection and thus present unacceptable risks to agency operations. Agencies must proactively address such risks to protect their ability to support essential operations, before deployment. Furthermore, many organizations poorly

administer their wireless technologies. Some examples include deploying equipment with "factory default" settings, failing to control or inventory their access points, not implementing the security capabilities provided, and not developing or employing a security architecture suitable to the wireless environment (e.g., firewalls between wired and wireless systems, blocking unneeded services/ports, using strong cryptography, etc.). To a large extent, most of the risks can be mitigated. However, mitigating these risks requires considerable tradeoffs between technical solutions and costs. Today, the vendor and standards community is aggressively working towards more robust, open, and secure solutions in the near future. For these reasons, it may be prudent for some agencies to simply wait for these more mature solutions.

Agencies should understand the technical and security implications of wireless and handheld device technologies.

While these technologies offer significant benefits, they also provide unique security challenges over their wired counterparts. The relative immaturity of the technology coupled with poor security standards, flawed implementations, limited user awareness, and lax security and administrative practices is 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. Simply stated, data may be captured when it is broadcast. Because of differences in building construction, wireless frequencies and attenuation, and the capabilities of high gain antennas, the distance necessary for positive control for some wireless technologies to prevent eavesdropping can vary considerably. It can vary up to kilometers, even when the nominal or claimed operating range of the wireless device is less than a hundred meters.

Agencies should carefully plan the deployment of 802.11, Bluetooth or any other wireless technology.

As 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.

Agencies should understand 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 (with some illustrative examples) should be implemented:

- Organizational-wide information system security policy that addresses the use of 802.11, Bluetooth and other wireless technologies.
- Configuration/change control and management to ensure that equipment (such as access points) has the latest, as appropriate, software release to include security feature enhancements and patches to discovered vulnerabilities.

- Standardized configurations to reflect the security policy, to ensure change of default values, and to ensure consistency of operation.
- Security awareness and training to promulgate a raised consciousness about the threats and vulnerabilities inherent in use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" channel and that simple theft of equipment is a major concern).

Agencies should understand that physical controls are especially important in a wireless environment.

Organizations should make sure that adequate physical security is in place. Physical security – barriers, access control systems, and guards– is 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, if sufficient distance is controlled, the risk of unauthorized access, especially to wireless access points can be minimized though not eliminated.

Agencies must enable, use, and routinely test the inherent security features (authentication and encryption) that exist in wireless technologies. In addition, firewalls and other protection mechanisms, as appropriate, 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 is needed. Since the security features provided in some wireless products may be weak and to attain the highest levels of integrity, authentication and confidentiality, organizations should carefully consider the deployment of robust, proven, well-developed and implemented cryptography.

NIST strongly recommends that the built-in security features of Bluetooth or 802.11 (data link level encryption and authentication protocols) be used as part of an overall defense-in-depth strategy. While 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, NIST notes, for agencies who have determined that certain information be protected via cryptographic means, that Federal Information Processing Standard (FIPS) 140-2 *Security Requirements for Cryptographic Modules* is mandatory and binding for federal agencies. As currently defined, neither the security of 802.11 or Bluetooth meets the FIPS 140-2 standard.

In the above-mentioned instances, it will be necessary to employ higher level cryptographic protocols and applications such as SSH, Transport-Level Security (TLS) or 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.

NIST expects that future 802.11 (and possibly other wireless technologies) products will offer AES-based data link level cryptographic services that are validated under FIPS 140-2. These will mitigate most concerns about wireless eavesdropping or active wireless attacks and their use is strongly recommended when they become available. However, it must be recognized, that a data link level wireless protocol protects only the wireless sub network, and, where traffic traverses other network segments, including wired segments or the agency or Internet backbone, higher level FIPS-validated, end-to-end cryptographic protection may also be required.

Finally, even when federally approved cryptography is used, additional countermeasures are typically necessary such as strategically locating access points, ensuring firewall filtering and blocking and

installation of antivirus software. Agencies must fully understand the residual risk following the application of cryptography and all security countermeasures in the wireless deployment.

1. Introduction

Wireless technologies have become increasingly popular in our everyday business and personal lives. Cell phones offer users a freedom of movement unimaginable just over 10 years ago. Personal Digital Assistants (PDA allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years.

An increasing number of government agencies, businesses, and home users are using, or considering using, wireless technologies in their environments. However, these groups need to be aware of the security risks associated with wireless technologies. They need to develop strategies that help mitigate those risks as they integrate these technologies in their computing environments. This document discusses wireless technologies, outlines the associated risks, and offers guidance for mitigating those risks.

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996 (specifically 15 United States Code [U.S.C.] 278 g-3 (a)(5)). This is not a guideline within the meaning of 15 U.S.C. 278 g-3 (a)(3).

Guidelines in this document are for federal organizations that process sensitive information. They are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130 Appendix III.

This document may be used by nongovernmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon 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, the Director of the OMB, or any other federal official.

1.2 Document Purpose and Scope

The purpose of this document is to provide organizations with guidance for establishing secure wireless networks.[1] Organizations are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements. However, NIST recommendations are not intended to supersede an organization's existing security policy.

The document addresses two wireless technologies that government organizations are most likely to employ: wireless local area networks (WLAN and ad hoc or, more specifically, Bluetooth networks. The document also addresses the use of wireless handheld devices. The document does not address technologies such as wireless radio and other WLAN standards that are not designed to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. These technologies are considered out of the scope of this document.

[1] See also NIST Special Publication 800-46, "Security for Telecommuting and Broadband Communications."

Wireless technologies are changing rapidly. New products and features are being introduced continuously. Many of these products now offer security features designed to resolve long-standing weaknesses or address newly discovered ones. Yet with each new capability, a new threat or vulnerability is likely to arise. Wireless technologies are evolving swiftly, and so it is essential to remain abreast of the current and emerging trends in the technologies and in the security or insecurities of these technologies. This guideline does NOT cover security of other types of wireless or emerging wireless technologies such as "Third-Generation" wireless telephony.

1.3 Audience and Assumptions

The intended audience is varied. 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. In fact, several sections are tutorial in nature.

Hence, the following list highlights how people with differing backgrounds might use this document:

- Government managers who are planning to employ wireless networked computing devices in their organizations (chief information officers, senior managers, etc.)
- Systems engineers and architects when designing and implementing networks
- System administrators when administering, patching, securing, or upgrading wireless networks
- Security consultants when performing security assessments to determine security postures of wireless environments
- Researchers and analysts who are trying to understand the underlying wireless technologies

This document assumes the readers have some minimal 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 document is divided into five sections followed by four appendices. This subsection is a roadmap describing the document structure.

- Section 1 (this section) provides an authority, purpose and scope, audience and assumptions, and document structure.
- Section 2 provides an overview of wireless technology.
- Section 3 examines 802.11 wireless local area network technology including the benefits and security risks of 802.11 and provides guidelines for mitigating those risks.
- Section 4 examines 802.11 Bluetooth ad hoc network technology including its benefits and security risks and provides guidelines for mitigating those risks
- Section 5 discusses the benefits and security risks of handheld wireless devices 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 used in this document.
- Appendix D contains the references used in the development of the document.

This document is written both as a working document and as a reference document. Checklists are provided in back of Sections 3, 4, and 5 – the critical sections of the document – to be used by wireless security practitioners performing a security assessment. Those practitioners may also want to refer back to the document to understand, for instance, the authentication method of Bluetooth or to find a useful website for additional wireless information.

2. Overview of Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections – without requiring network cabling. Wireless technologies use radio transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as WLANs and cell phones, to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. Wireless technology aims to provide users access to information anywhere – it allows mobility. Historically, the number one application for wireless has been mobile voice communication with cellular technology, that has been around since the early 1980s. Today, however, databased applications are beginning to burgeon. In this section, a brief overview of critical elements of wireless is presented: wireless networks, wireless devices, wireless standards, and wireless security issues.

2.1 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: WWAN, WLAN, and WPAN. WWAN, representing wireless wide area networks, includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, Hyperlan, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and Infrared. All of these technologies are "tetherless" –they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band.[2] The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. (See Appendix A for a list of common wireless frequencies.) Because wireless network and technology are so diverse, we primarily focus on the WLAN and WPAN technologies.

2.1.1 Wireless LANs

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users even to "roam" within a building or between buildings.

2.1.2 Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs.[3] These networks are termed ad hoc because of their shifting network

[2] Appendix A provides an overview of wireless frequencies and their use.
[3] Specifically, a "Bluetooth" network. See Section 2.3.2.

topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. In a Bluetooth network, mobile routers control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocol Bluetooth employs allows the routers to establish and maintain these shifting networks.

The mobile router is commonly integrated in a device such as a PDA (Figure 2-1). This mobile router, when configured, ensures that a remote, mobile device, such as a mobile phone, stays connected to the network. The router maintains the connection and controls the flow of communication. (Figure 2-1 also illustrates how with emerging technologies the mobile phone will be capable of connecting to the network, synchronizing the PDA address book, and downloading e-mail on an IEEE 802.11 WLAN all at the same time.)

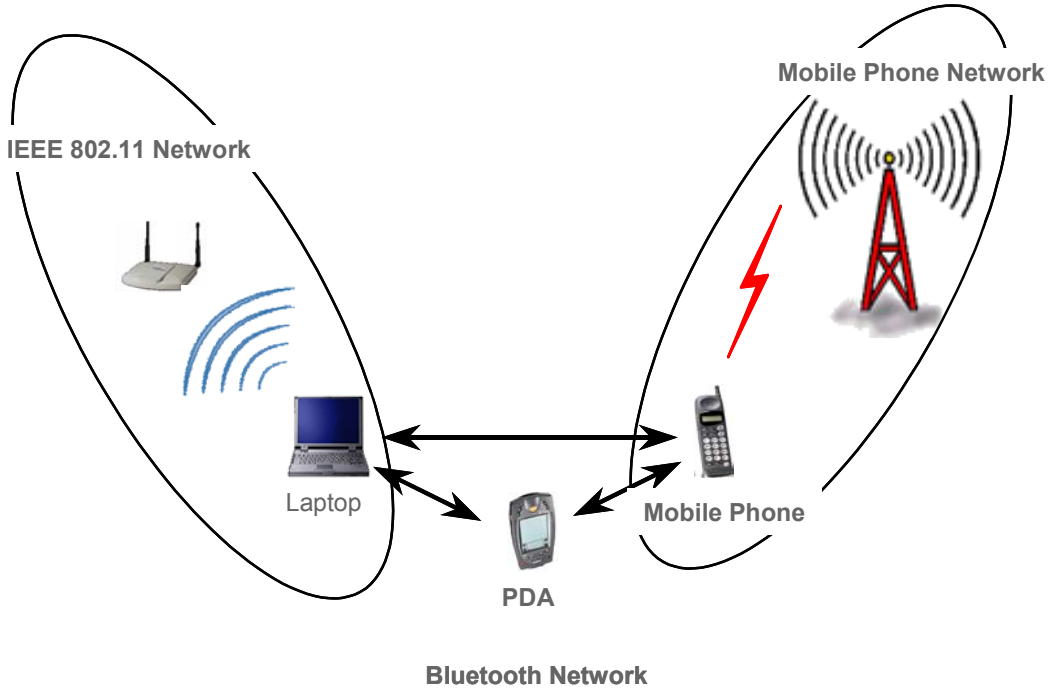

Figure 2-1. Notional Ad Hoc Network

2.2 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as text-messaging devices, PDAs, and Smart Phones.[4] Other devices include wireless e-mail devices with push technology, whereby e-mail gets delivered to the device without the user actually polling a Server (e.g., RIM's Blackberry device).

[4] It should be noted, however, that the lines between these categories are rapidly blurring as manufacturers incorporate and integrate increased capabilities and features.

2.2.1 Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Internet.

2.2.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a cell. As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next. Today's cell phone is rapidly evolving to include integration with PDAs, thus providing users with increased wireless e-mail and Internet access. Mobile phones with information processing and data networking capabilities are called Smart Phones. This document addresses the risks introduced by the information processing and networking capabilities of Smart Phones.

2.2.3 Text-Messaging Devices

Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network. Text-messaging technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld via the Internet and wireless network.

2.3 Wireless Standards

Wireless, at its current relatively immature state, encompasses a variety of standards. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to communicate. The Advanced Mobile Phone Systems (AMPS) standard, which governed first generation mobile telephone devices, allowed devices from various manufacturers to work on wireless network infrastructure developed by other manufacturers. The AMPS standard uses Frequency Division Multiple Access (FDMA) and requires a great deal of bandwidth while operating in the 824–829MHz range (similar to FM radios). Other telephony standards include IS-136, a Time Division Multiple Access (TDMA) standard, IS-95, a Code Division Multiple Access (CDMA) standard, and Global System for Mobile (GSM) – yet another TDMA standard. Many handheld devices (e.g., PDAs and cell phones) have followed the Wireless Application Protocol (WAP) standard, which provides for secure access to e-mail and the Internet. As briefly demonstrated, there are a plethora of wireless standards. All of these standards are different and offer varying levels of security features. For this document, the wireless standards discussion is limited to the IEEE 802.11 and the Bluetooth standard.

WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth. Introductions to these are provided below.

2.3.1 IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and

to address mobile and portable stations. Mobile stations access the LAN while in motion, while portable stations are moved from location to location, but are only used while in a fixed physical location.[5]

802.11 is the original WLAN standard, designed for 1Mbps to 2Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5GHz band and supported 54Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 – 2.48GHz band and supports 11Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed.[6] These weaknesses will be discussed in Section 3.4.3.1.1. Another standard, 802.11g, still in draft, operates in the 2.4GHz waveband, where current WLAN products based on the 802.11b standard operate.[7]

Two other important and related standards for WLANs are 802.1x and 802.11i. The 802.1x, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1x. The 802.11i standard is discussed further in Section 3.5.

2.3.2 Bluetooth

Bluetooth has emerged as the primary ad hoc network standard. The Bluetooth standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers using short-range wireless connections. Bluetooth network applications include wireless synchronization, e-mail/Internet/intranet access using local personal computer connections, hidden computing through automated applications and networking, and applications that can be used for such devices as hands-free headsets and car kits. The Bluetooth standard specifies wireless operation in the 2.45 Gigahertz (GHz) radio band and supports data rates up to 720kbps.[8] It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1

2.4 Wireless Security Threats and Risk Mitigation

The NIST handbook *An Introduction to Computer Security* classifies security threats into one of nine categories:[9]

- Errors and omissions
- Fraud and theft committed by authorized or unauthorized users of the system
- Employee sabotage
- Loss of physical and infrastructure support
- Malicious hackers
- Industrial espionage

[5] ANSI/IEE, 1999

[6] Rysavy, P., Network Computing, Mobile and Wireless Technology Feature, "Break Free With Wireless LANs," October 29, 2001.

[7] See http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm.

[8] Next generation of Bluetooth will have a theoretical throughput of up to 2Mbp.

[9] The NIST Handbook, Special Publication 800-12, *An Introduction to Computer Security*

- Malicious code
- Foreign government espionage
- Threats to personal privacy.

All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are fraud and theft, malicious hackers, malicious code, and industrial and foreign espionage. Theft is likely to occur with wireless devices due to their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, the former are more likely to carry out such acts. Since users of a system may know what resources a system has and the system security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an organization (although users within an organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Industrial and foreign espionage involve gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease in which eavesdropping can occur on radio transmissions.

These threats, if successful, place an organization's systems—and, more importantly, its data—at risk. Ensuring confidentiality, integrity, and network availability are (or should be) prime objectives of all government security policies and practices. These are the areas of most concern for the ever-increasing use of wireless networks within government. Confidentiality is "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."[10] The impact of unauthorized disclosure of confidential information can range from revealing private information about an individual to jeopardizing national security.[11] Information that government organizations should keep confidential includes, for example, both sensitive but unclassified and classified information, proprietary information from companies and vendors, and any information about citizens that may be covered under the Privacy Act of 1974.

Integrity is "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."[12] NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems* explains that information must be protected from unauthorized, unanticipated, or unintentional modification. This protection includes but is not limited to—

- **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.
- **Non-repudiation**—The origin or the receipt of a specific message must be verifiable by a third party.
- **Accountability**—The actions of an entity must be traceable uniquely to that entity.[13]

Network availability is "the property of being accessible and usable upon demand by an authorized entity."

---

10 ISO/International Electrotechnical Commission (IEC) 7498-2.

11 Stoneburner, G., Goguen, A., and A. Feringa, *Risk Management for Information Technology Systems*, NIST Special Publication 800-30, October 2001.

12 RFC 2828.

13 Swanson, M., *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, August 2001.

The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.[14]

Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, organizations need to adopt security measures and practices that help bring their risks to a manageable level. They need, for example, to perform security assessments prior to implementation to determine the specific threats and vulnerabilities wireless networks will introduce in their environments. In performing the assessment, they 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 it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization will need to reassess periodically the policies and measures it puts in place because computer technologies and malicious threats are continually changing. (For more detailed information on the risk mitigation and safeguard selection process, refer to NIST SPs 800-12, *An Introduction to Computer Security* and 800-30*, Risk Management Guide for IT Systems*.) To date, the list below represents some of the more salient threats and vulnerabilities of wireless systems:

- 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 not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and 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 activity.
- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

[14] ISO/IEC 7498-2.

2.5 Emerging Wireless Technologies

Originally, handheld devices had limited functionality because of size and power requirements. However, the technology is improving and handheld devices are becoming more feature-rich and portable. More significantly, the various wireless devices and their respective technologies are coalescing. The mobile phone, for instance, has increased functionality that now allows it to serve as a PDA as well as a phone. Smart phones are merging mobile phone and PDA technologies to provide normal voice service and e-mail, text messaging, paging, web access, and voice recognition. Next-generation mobile phones, already on the market, are quickly incorporating PDA, IR, wireless Internet, e-mail, and GPS capabilities.

Manufacturers are combining standards as well, with the goal to provide a device capable of delivering multiple services. Other developments that will soon be on the market include GSM-based technologies such as General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). These technologies will provide high data transmission rates and greater networking capabilities. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected.

3. Wireless LANs

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

3.1 Wireless LAN Overview

WLAN technology and the WLAN industry date back to the mid-1980s when the Federal Communications Commission (FCC) first made available the radio frequency spectrum. During the 1980s and early 1990s, growth was relatively slow. Today, however, WLAN technology is experiencing tremendous growth. There are several reasons for the growth, but the key reason is because of the increased bandwidth of the IEEE 802.11b standard of WLAN technology. As an introduction to the 802.11 and WLAN technology, Table 3-1 provides some key characteristics at a glance.

Table 3-1. Key Characteristics of 802.11 Wireless LANs

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

3.1.1 Brief History

Motorola developed one of the first commercial WLAN systems with its Altair product. However, early WLAN technologies had several problems that prohibited its pervasive use. These LANs were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF (radio frequency) technologies. The Institute of Electrical and Electronics Engineers (IEEE) initiated the 802.11 project in 1990 with a scope "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 802.11 international interoperability standard. Then, in 1999, the IEEE ratified the 802.11a and the 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, similar to what was done with the 802.3 Ethernet standard. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This soon-to-be introduced

technology will use the 5GHz frequency spectrum and can process data at up to 54Mbps. The direct descendent of 802.11a, IEEE's 802.11b, is the focus of this document.

Although this document focuses on the IEEE 802.11b WLAN standard, it is important to note that several other WLAN technologies and standards are available from which consumers may choose, including HiperLAN and HomeRF. For information on the European Telecommunications Standards Institute (ETSI) developed HiperLAN, visit the HiperLAN Alliance site (http:///www.hiperlan.com). For more information on HomeRF, visit the HomeRF Working Group site (http://www.homeRF.org). This document does not address those technologies.

3.1.2 Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The popular IEEE 802.11b standard is the latest completed member of 802.11 WLAN family. The 802.11b standard operates in the unlicensed 2.4GHz–2.5GHz ISM (Industrial, Scientific, and Medical) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b standard focuses on the MAC and PHY protocols for connectivity. The 802.11b WLAN technology permits transmission speeds of up to 11Mbits per second. This makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2Mbps) and slightly faster than standard Ethernet.

3.1.3 Architecture

The IEEE 802.11b standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network. The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a basic service set (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campus areas. By deploying multiple APs with overlapping coverage areas, broad network coverage can be achieved. WLAN technology can be used to replace wired LANs totally as well as to extend LAN infrastructure.

A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generally equipped with a wireless network interface card (NIC) that consists of the radio modem and the logic to interact with the client machine and software. An AP comprises essentially a radio modem on one side and a bridge to the wired backbone on the other. The AP, a stationary device that is part of the wired infrastructure, is analogous to a cell-site (base station) in cellular communications. All communications between the client stations and between clients and the wired network go through the AP. The basic topology of a WLAN is depicted in Figure 3-1.

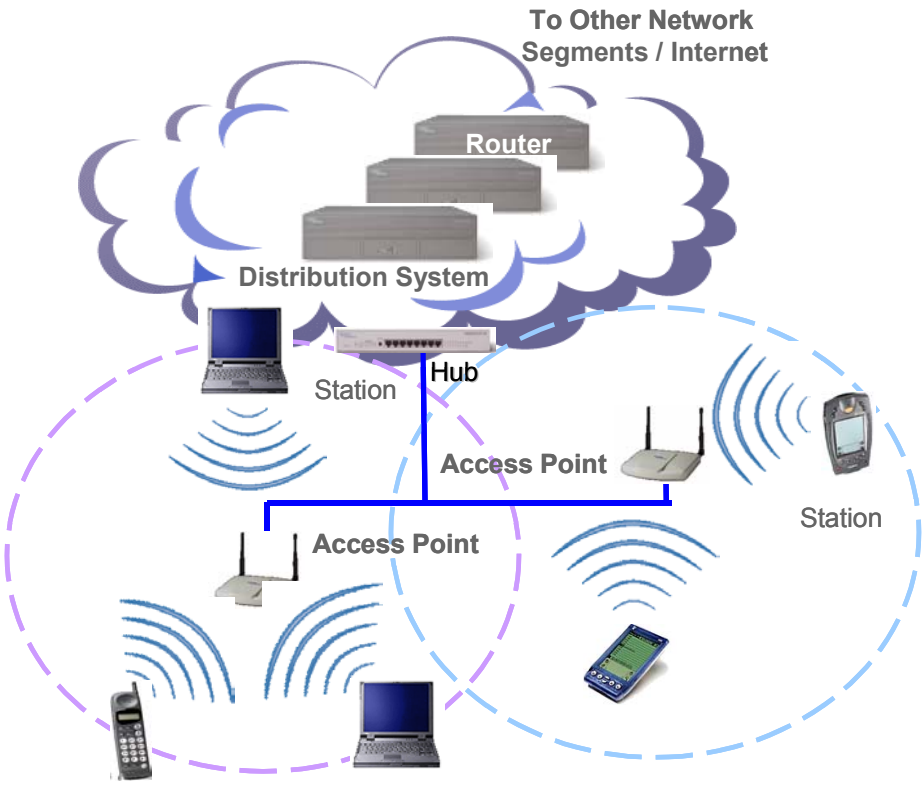

Figure 3-1. Fundamental 802.11b Wireless LAN Topology

Although most WLANs operate in the "infrastructure" mode and architecture described above, another topology is also possible. This second topology, the ad hoc network, is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be internetworked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an IBSS (independent basic service set). The ad hoc topology is depicted in Figure 3-2 below.

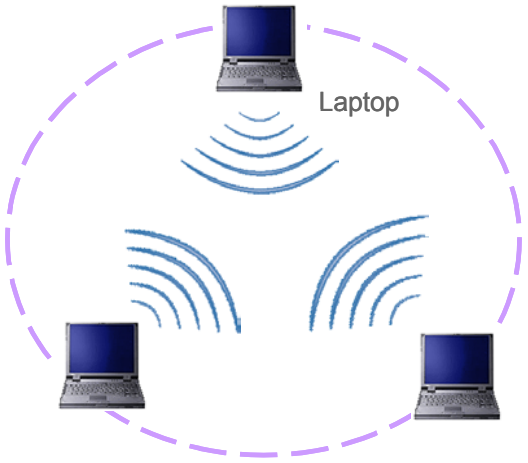

Figure 3-2. 802.11b Wireless LAN Ad hoc Topology

The ad hoc configuration is similar to a peer-to-peer office network in which no node is required to function as a server. As an ad hoc WLAN, laptops, desktops and other 802.11 devices can share files without the use of an AP.

3.1.4 Wireless LAN Components

A WLAN comprises two types of equipment: a wireless station and an access point. A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless network interface card (NIC).[15] A WLAN client may also be a desktop or handheld device (e.g., PDA, or custom device such as a barcode scanner), or equipment within a kiosk, on a manufacturing floor, or other publicly accessed area. Wireless laptops and notebooks—"wireless enabled"—are identical to laptops and notebooks except that they use wireless NICs to connect to access points in the network. The wireless NIC is commonly inserted in the client's Personal Computer Memory Card International Association (PCMCIA) slot or Universal Serial Bus (USB) port. The NICs use radio frequencies or infrared beams to establish connections to the WLAN. The AP, which acts as a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface such as 802.3, and bridging software. The AP functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network.

3.1.5 Range

The reliable coverage range for 802.11b WLANs depends on several factors including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11Mbps) in a closed office area to 485 meters (for 1Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11b equipment is approximately 50 meters (about 163 ft.) indoors. With an omni-directional antenna outdoors, the connectivity can be increased to 400 meters. A range of 400 meters, nearly ¼ mile, makes WLAN ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.

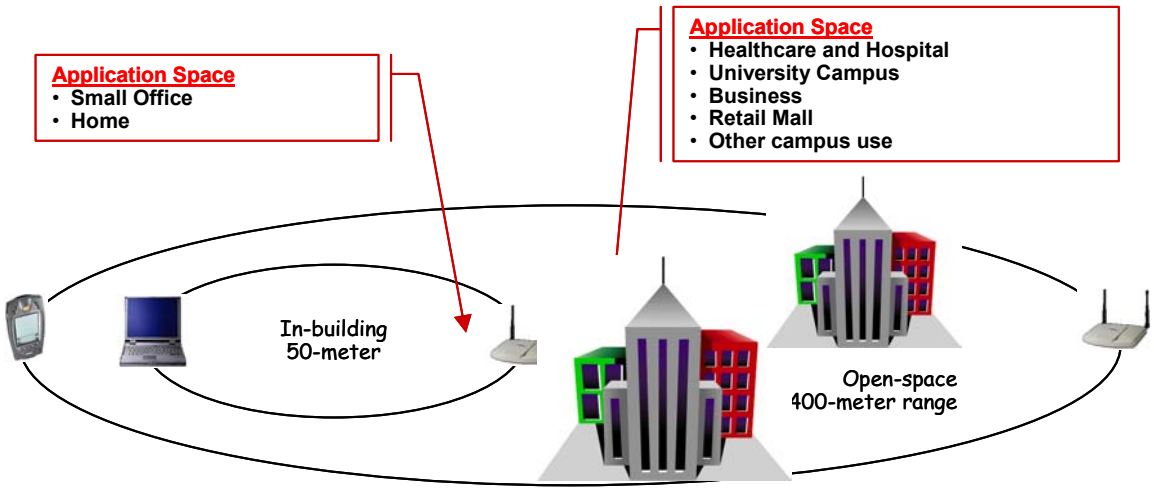

Figure 3-3. Typical Range of 802.11 WLAN

[15] Notebook computers are basically the same as laptop computers, except that they are generally lighter in weight and thinner in size.

APs may also provide a "bridging" function. Bridging connects two or more networks together and allows them to communicate—to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via the LANs' respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, if a computer on Subnet A needed to connect to computers on Subnets B, C, and D, Subnet A's AP would connect to B, C, and D's respective APs.

Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used.[16] Figure 3-4 illustrates point-to-point bridging between two LANs. In the example, wireless data is being transmitted from Laptop A to Laptop B, from one building to the next, using each building's appropriately positioned AP. Laptop A connects to the closest AP within the building A. The receiving AP in building A then transmits the data (over the wired LAN) to the AP bridge located on the building's roof. That AP bridge then transmits the data to the bridge on nearby building B. The building's AP bridge then sends the data over its wired LAN to Laptop B.

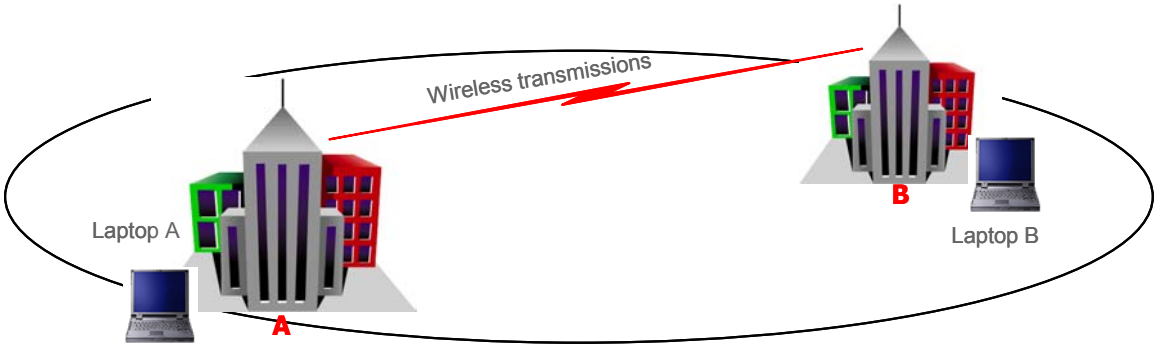

Figure 3-4. Access Point Bridging

3.2 Benefits

WLANs' "untethered" method of communication, making them very attractive today, can result both in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for home and enterprise users.

WLANs offer four primary benefits to users:

- **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.
- **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.

[16] See Bridging at ftp://download.intel.com/support/network/Wireless/pro201lb/accesspoint/bridging.pdf for more information on access point bridging.

- **Flexibility**—Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.

- **Scalability**—WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small P2P 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. According to IDC, the number of mobile subscribers will surpass 500 million worldwide by 2002. IDC also posits that sales of WLAN technology will reach $3.2 billion by 2005. WLANs are now becoming a viable alternative to traditional wired solutions. In fact, hospitals, universities, airports, hotels, and specialty shops are now offering WLAN access to the Internet.

3.3 Security of 802.11 Wireless LANS

This section helps the reader understand the built-in security features of 802.11b. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11b specification identified several services to provide a secure operating environment. The security services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and access points. That is, WEP does not provide end-to-end security but only for the wireless portion of the connection. Security for the radiopath is depicted in Figure 3-5.

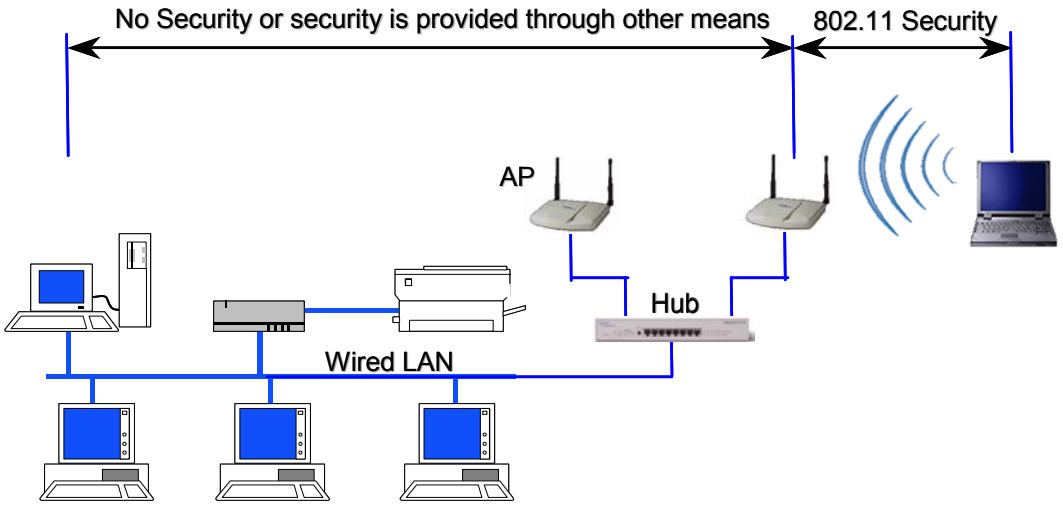

Figure 3-5. Wireless Security of 802.11b in Typical Network

3.3.1 Security Features of 802.11 Wireless LANS per the Standard

The three basic security services defined by IEEE for the WLAN environment are as follows:

- **Authentication**—A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This is to provide access control to the network through denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorized persons allowed to gain access to my network?”

- **Confidentiality—**Confidentiality, or privacy, was a second goal of WEP. It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, "Are only authorized persons allowed to view my data?"
- **Integrity**—Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. This service addresses the question, "Is the data coming into or exiting the network trustworthy – has it been tampered with?"

It is important to note that the standard did not address other security services such as audit, authorization, and non-repudiation. These three security services offered by 802.11 are described in greater detail below.

3.3.1.1 Authentication

The IEEE 802.11b specification defines two means to validate wireless users attempting to gain access to the wired network, as depicted previously. One means is based on cryptography and the other is not. For the non-cryptographic approach, there are essentially two different ways to identify a wireless client attempting to join a network. However, both of these approaches are identity-based verification mechanisms. The wireless stations requesting access simply respond with the Service Set Identifier (SSID) of the wireless network—there is no true "authentication." The two ways are referred to as Open System authentication and Closed System authentication. A taxonomy of the techniques for 802.11b is depicted in Figure 3-6.

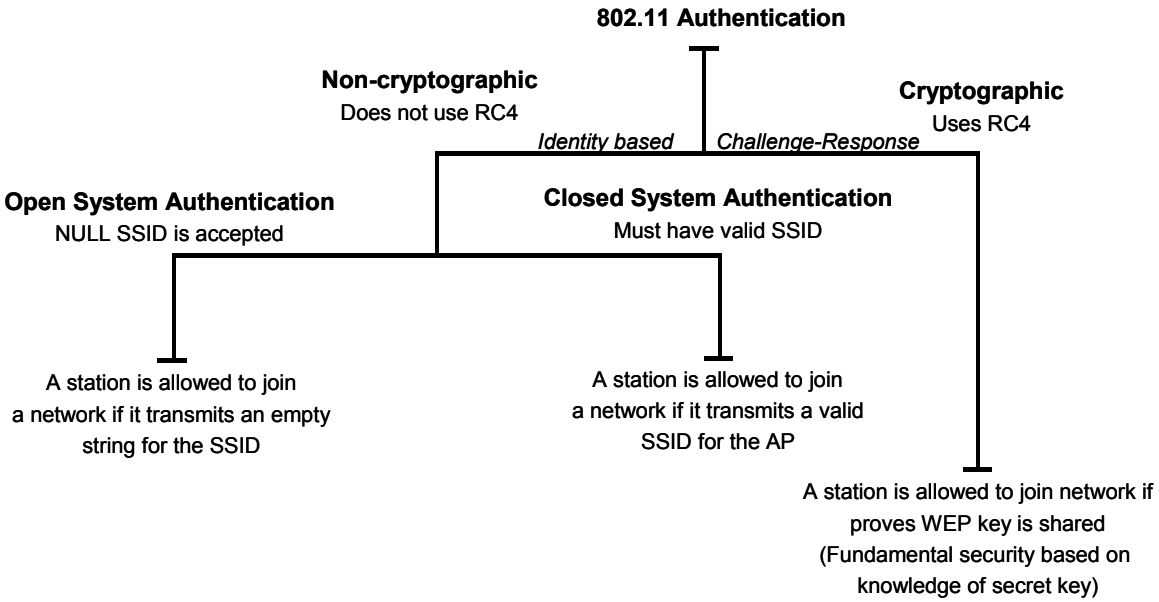

Figure 3-6: Taxonomy of 802.11b Authentication Techniques

With Open System, a client is authenticated if it simply responds with an empty string for the SSID (Service Set Identifier)—hence, the name "NULL authentication." With the second method, Closed Authentication, wireless clients must respond with the actual SSID of the wireless network. That is, a client is allowed access if it responds with the correct 0-byte to 32-byte string identifying the BSS of the wireless network. Again, this primitive type of authentication is only an identification scheme. Practically

speaking, neither of these two schemes offers robust security against unauthorized access. To reiterate, both Open and Closed Authentication schemes are highly vulnerable to attacks—against even the most novice adversaries—and without enhancements, they practically invite security incidents.

Shared key authentication is a cryptographic technique for authentication. It is a simple "challenge-response" scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted in Figure 3-7, a random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key (WEP key) that is shared with the AP, encrypts the challenge (or "nonce," as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP and therefore there is no assurance that a client is communicating with a legitimate AP, and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer from numerous attacks including the infamous "man-in-the-middle" attack.

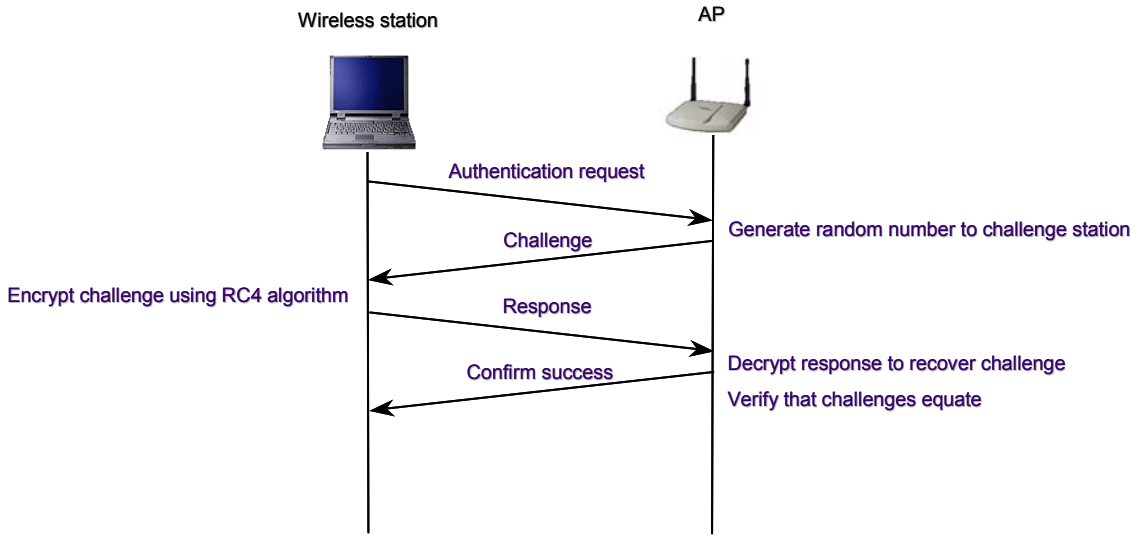

Figure 3-7. Shared-key Authentication Message Flow

3.3.1.2 Privacy

The 802.11b standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric-key, stream cipher algorithm to generate a pseudo random data sequence. This "keystream" is simply added modulo 2 (exclusive-ORed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11b WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).

The WEP supports cryptographic keys sizes from 40-bits to 104-bits. The 104-bit WEP key, for instance, with a 24-bit IV becomes a 128-bit RC4 key. In general, increasing the key size increases the security of a cryptographic technique. Research has shown that key sizes of greater than 80-bits make brute-force cryptanalysis (codebreaking) an impossible task. For 80-bit keys, the number of possible keys—a

keyspace of more than 10^{24}—exceeds contemporary computing power. However, in practice, most WLAN deployments rely on 40-bit keys. Moreover, recent attacks have shown that the WEP approach for privacy is, unfortunately, vulnerable to certain attacks regardless of keysize.

The WEP privacy is illustrated conceptually in Figure 3-8.

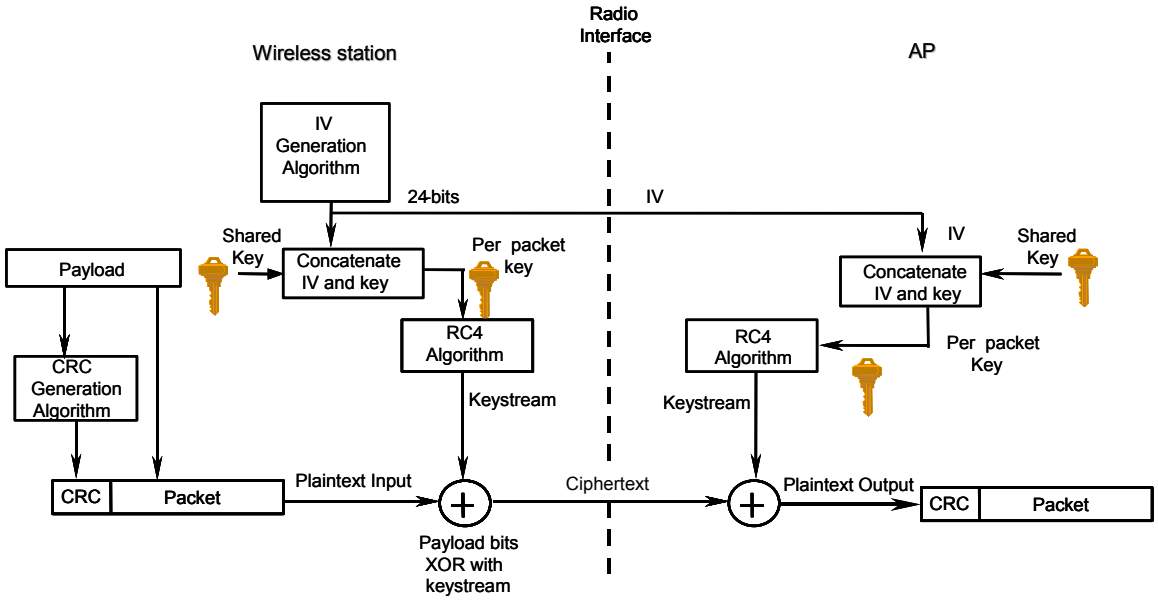

Figure 3-8. WEP Privacy Using RC4 Algorithm

3.3.1.3 Integrity

The IEEE 802.11b specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary "in the middle." This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the ciphertext message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, "received in error," this would indicate an integrity violation (an active message spoofer), and the packet would be discarded. As with the privacy service, unfortunately, the 802.11b integrity is vulnerable to certain attacks regardless of key size.

The IEEE 802.11b specification does not, unfortunately, 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 those deploying WLANs. Again, key management (probably the most critical aspect of a cryptographic system) for 802.11b is left largely as an exercise for the users of the 802.11b network (perhaps, individuals not totally cognizant of its importance). As a result, many vulnerabilities can 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 is poor for 802.11b, WEP-secured WLANs suffer from the inability to scale. In other words, even if an enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000

APs. Generating, distributing, loading, and managing keys for an environment of this size is a most significant challenge.

3.3.2 Problems with the IEEE 802.11b Standard Security

This section discusses some known vulnerabilities in the standardized security of the 802.11b WLAN standard. As mentioned above, the WEP protocol is used in 802.11-based WLANs. WEP in turn uses a RC4 cryptographic algorithm with a variable length key to protect traffic. Again, the 802.11 standard supports WEP cryptographic keys of 40-bits. However, some vendors have implemented products with keys to 104-bits, plus the addition of a 24-bit IV. It is worthy to note that keys are often based on passwords that are chosen by users; this typically reduces the effective key size.

Several groups of computer security specialists have discovered security problems that let malicious users compromise the security of WLANs. These include passive attacks to decrypt traffic based on statistical analysis, active attacks to inject new traffic from unauthorized mobile stations (i.e., based on known plaintext), active attacks to decrypt traffic (i.e., based on tricking the access point), and dictionary-building attacks. The dictionary building attack is possible after analyzing a full day's traffic.[17] Because significant attention is now on the security of 802.11, more attacks are likely to be discovered.

There are several problems with WEP, including the following:

1. The use of static WEP keys—many users in a wireless network potentially sharing the identical key for long periods of time, is a well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key. Moreover, since every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks, such as 2 and 3 below.

2. The initialization vector (IV) in WEP, as shown in Figure 3-8, is a 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for the protection of data, and the short IV guarantees that they will repeat after a relatively short time in a busy network. Moreover, the 802.11 standard does not specify how the IVs are set or changed, and individual wireless NICs from the same vendor may all generate the same IV sequences, or some wireless NICs may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the ciphertext.

3. The IV is a part of the RC4 encryption key. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a deadly analytic attack, that recovers the key, after intercepting and analyzing only a relatively small amount of traffic. This attack has been reduced to script.

4. WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a noncryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledges packets with the correct checksum. The combination of noncryptographic checksums with stream ciphers is dangerous and often leads to unintended "side channel" attacks, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP, and noting whether the packet

[17] Borisov, N., Goldberg, I., and D. Wagner, http://www.isaac.cs.berkley.edu/isaac/wep-faq.html.

is acknowledged. These kinds of attacks are often subtle, and it is now generally believed that it is 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 cipher text.

Note that only one of the four problems listed above depends on a weakness in the cryptographic algorithm. Therefore, the other three problems would not be improved by substituting a stronger stream cipher. The third problem listed above is in part a consequence of a weakness in the RC4 stream cipher, but is only exposed by a poorly designed protocol.

Some of the problems associated with WEP and 802.11b WLAN security are summarized in Table 3-2.

Table 3-2. Key Problems with Existing 802.11 Wireless LAN Security

Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	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. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. 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 brute-force 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 keystream 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 noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system.
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.

3.4 Security Requirements and Threats

As discussed above, the 802.11b WLAN industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11b WLAN technology. Many organizations—including retail stores, hospitals, airports, and business enterprises—plan to capitalize on the benefits of "going wireless." However, although there has been tremendous growth and success, everything relative to 802.11b WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless and exposing risks to any organization deploying the technology. This subsection will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability.

Figure 3-9 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

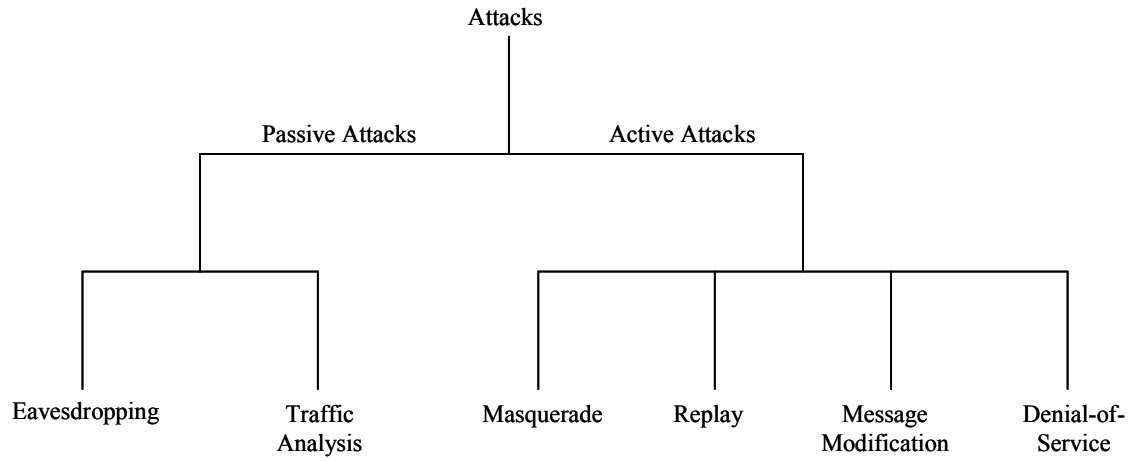

Figure 3-9. Taxonomy of Security Attacks

As Figure 3-9 shows, network security attacks are typically divided into *passive* and *active* attacks. These two broad classes are then subdivided into other types of attacks. All are defined below.

- **Passive Attack**—An attack in which an unauthorized party simply gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either simple eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.
  - **Eavesdropping**—The attacker simply monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
  - **Traffic analysis**—The attacker, in a more subtle way, 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.
- **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 combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

- **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

All risks against 802.11 are the result of one or more of these attacks. The consequences of these attacks include loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

3.4.1 Loss of Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. This is, in general, a fundamental security requirement for most organizations. Due to the broadcast and radio nature of wireless, confidentiality is typically a more difficult security requirement to meet. Adversaries do not have to tap into a network cable to access network resources. Moreover, it may not be possible to control the distance over which the transmission occurs. This makes traditional physical security countermeasures less effective.

Passive eavesdropping of native 802.11b wireless communications may cause significant risk to an organization. An adversary may be able to listen in and obtain sensitive information including proprietary information, network IDs and passwords, and configuration data. This risk is present because the 802.11b signals may travel outside the building perimeter or because there may be an "insider." Because of the extended range of 802.11 broadcasts, adversaries can potentially detect transmission from a parking lot or nearby roads. This kind of attack, performed through the use of a wireless network analyzer tool or *sniffer*, is particularly easy for two reasons: 1) frequently confidentiality features of WLAN technology are not even enabled, and 2) because of the numerous vulnerabilities in the 802.11b technology security, as discussed above, determined adversaries can compromise the system.

Wireless packet analyzers, such as AirSnort and WEPcrack, are tools that are readily available on the Internet today.[18] AirSnort is one of the first tools created to automate the process of analyzing networks. Unfortunately, it is also commonly used for breaking into wireless networks. AirSnort can take advantage of flaws in the key-scheduling algorithm of RC4, which forms part of the WEP standard. To accomplish this, AirSnort requires only a computer running the Linux operating system and a wireless network card. The software passively monitors the WLAN data transmissions and computes the encryption keys after at least 100MB of network packets have been *sniffed*.[19] On a highly saturated network, collecting this amount of data may only take three or four hours; if traffic volume is low, a few days. After the network packets have been received, the fundamental keys may be guessed in less than one second.[20] Once the malicious user knows the root key, that person can read any packet traveling over the WLAN. Such sniffing tools' wide availability, ease of use, and ability to compute keys makes it essential for security administrators to implement secure wireless solutions.

[18] WEPcrack was released on the Internet around the same time as AirSnort, but WEPcrack is still considered an alpha release.
[19] See "Tools Dumb Down Wireless Hacking," *The Register*, August 2001 (www.theregister.co.uk).
[20] For more information from AirSnort, visit their web page at www.airsnort.sourceforge.net.

Another risk to loss of confidentiality through simple eavesdropping is broadcast monitoring. An adversary can monitor traffic, using a laptop in promiscuous mode, when an access point is connected to a hub instead of a switch. Hubs generally broadcast all network traffic to all connected devices, which leaves the traffic vulnerable to unauthorized monitoring. For example, if a wireless access point was connected to an Ethernet hub, a device that is monitoring broadcast traffic could pick up data intended for wireless clients. Consequently, organizations should consider using switches instead of hubs for connections to wireless access points.[21]

WLANs risk loss of confidentiality following an active attack as well. Sniffing software as described above can obtain user names and passwords (as well as any other data traversing the network) as they are sent over a wireless connection. An adversary may be able to masquerade as a legitimate user and gain access to the wired network from an AP. Once "on the network," the intruder can scan the network using software available off the Internet. The malicious eavesdropper then uses the user name, password, and IP address information to gain access to network resources and sensitive corporate data.

Lastly, rogue APs pose a security risk. A malicious 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 and use it to gain access to the network. As long as its location is in close proximity to the users of the WLAN, the rogue AP can intercept the wireless traffic between an authorized AP and wireless clients. It need only be configured with a stronger signal than the existing AP to intercept the client traffic. A malicious user can also gain access to the wireless network through APs that are configured to allow access without authorization.[22]

3.4.2 Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Since organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. A hacker, for example, can compromise data integrity by deleting or modifying the data in an e-mail from an account on the wireless system. Depending on the importance of the e-mail and how widespread its distribution among e-mail recipients, the impact could be detrimental to an organization.

Because the existing security features of 802.11 do not provide for strong message integrity, other kinds of active attacks are possible that compromise system integrity. As discussed before, the WEP-based integrity mechanism is simply a linear CRC. Message modification attacks are possible without the use of cryptographic checking mechanisms such as message authentication codes and hashes.

3.4.3 Loss of Network Availability

A denial in network availability involves some form of DoS attack, such as jamming. Jamming occurs when a malicious user deliberately emanates a signal from a wireless device in order to overwhelm legitimate wireless signals. Jamming results in a breakdown in communications since legitimate wireless signals are unable to communicate on the network. Non-malicious users can also cause a DoS. A user, for instance, may unintentionally monopolize a wireless signal by downloading large files, effectively denying other users access to the network. As a result, organizational policies should limit the types and amounts of data that users are able to download on wireless networks.

[21] See Internet Security Systems, "Wireless LAN Security: 802.11b and Corporate Networks."
[22] See http://iss.net.

3.4.4 Other Security Risks

With the prevalence of wireless devices, more users are seeking ways to connect remotely to their own organizations' networks. One such method is the use of untrusted, third party networks.[23] Conference centers, for example, commonly provide wireless networks for users to connect to the Internet and subsequently to their own organizations while at the conference. Airports and even some coffee franchises are beginning to do the same. Starbucks and Boingo, for instance, are planning to deploy 802.11-based publicly accessible wireless networks for their customers, even offering virtual private network (VPN) capabilities for added security.[24]

These untrusted public networks introduce three primary risks: 1) because they are public, they are accessible by anyone, even malicious users; 2) they serve as a bridge to a user's own network, thus potentially allowing anyone on the public network to attack or gain access to the bridged network; and 3) they use high RF transmission power levels for a strong signal strength, thus allowing malicious users to eavesdrop more readily on their signals.

In connecting to their own networks via an untrusted network, users may create vulnerabilities for their company networks and systems unless their organizations take steps to protect their users and themselves. Users typically need to access resources that their organizations deem as either public or private. Organizations should protect their public resources using an application layer security protocol such as Transport Layer Security (TLS), the Internet Engineering Task Force standardized version of Secure Sockets Layer (SSL). For private resources, organizations should use a VPN solution to secure their connections, since this will help prevent eavesdropping and unauthorized access to private resources.

Lastly, as with any network, social engineering and dumpster diving are also concerns. An enterprise should consider all aspects of network security when planning to deploy the wireless network.

3.5 Risk Mitigation

Government organizations can mitigate risks to their 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 associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. This section describes risk-mitigating steps for an organization, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no "one size fits all" when it comes to security. Some organizations may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in dollars spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some organizations may be willing to accept risk because applying various countermeasures may exceed financial or other constraints.

3.5.1 Management Countermeasures

Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance therewith, is the foundation on which other countermeasures—the operational and technical—are rationalized and implemented. A WLAN security policy should be able to do the following:

---

[23] The following provides a list of publicly accessible Wireless networks around the world: http://www.toaster.net/Wireless/community.html.

[24] See "Starbucks Takes Wireless Leap," http://www.computerworld.com/cwi/story, and www.boingo.com.

- Identify who may use WLAN technology in an organization
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for access points
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed
- Define standard security settings for access points
- Describe limitations on how the wireless device may be used, such as location
- Describe the hardware and software configuration of any access device
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines on the use of encryption and other security software
- Define the frequency and scope of security assessments

Another management countermeasure is to ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasures are trained and aware users.

3.5.2 Operational Countermeasures

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. For example, photo identification, card badge readers, or biometric devices can be used to minimize the risk of improper penetration of facilities. Some possible access mechanisms are proximity methods such as keypads or cipher locks. Biometric systems for physical access control include palm scans, hand geometry, iris scans, retina scans, fingerprint, voice pattern, signature dynamics, or facial recognition. 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.

It is important to consider the range of the AP when deciding where to place an AP in a WLAN environment. If the range extends beyond the physical boundaries of the office building walls, the extension creates a security vulnerability. An individual outside of the building, perhaps "wardriving," could eavesdrop on network communications by using a wireless device that picks up the RF emanations. A similar consideration applies to the implementation of building-to-building bridges. Ideally, the APs 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 (see next paragraph) 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 available to measure and secure AP coverage. The tools, which some vendors include with their products, measure the received signal strength from the APs. These measurements can be used to map out the coverage area. However, security administrators should use caution when interpreting the results since each vendor interprets the received signal strength differently. Some AP vendors also have special features that allow control of power levels and therefore the range of the AP. Such control is useful if the required coverage range is not broad because, for example, to the building or room in which access to the wireless network is needed happens to be small. Controlling the coverage range for this smaller building or room may help prevent the wireless signals from extending beyond the intended coverage area. Organizations could additionally use directional antennas to control emanations. However, directional antennas do not protect network links; they merely help control coverage range.

Although mapping the coverage area may yield some advantage relative to security, it should not be seen as an absolute solution. There is always the possibility that an individual might use a high-gain antenna to eavesdrop on the wireless network traffic. It should be recognized that only through the use of strong cryptographic means can a user gain any assurance against true eavesdropping adversaries. The following paragraphs discuss how cryptography (Internet Protocol Security [IPsec] and VPNs) can be used to thwart many attacks.

3.5.3 Technical Countermeasures

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment.[25] Software countermeasures include proper AP configurations (i.e., the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems (IDS), and encryption. Hardware solutions include smart cards, VPNs, public key infrastructure (PKI), and biometrics.[26]

3.5.3.1 Software Solutions

Technical countermeasures involving software include properly configuring access points, regularly updating software, implementing authentication and IDS solutions, performing security audits, and adopting effective encryption. These are described in the paragraphs below.

3.5.3.1.1 Access Point Configuration

Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet Medium Access Control (MAC) Access Control Lists (ACL), shared keys, and Simple Network Management Protocol (SNMP) agents will help eliminate many of the vulnerabilities inherent in a vendor's software default configuration.

Updating default passwords. Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example. On some APs, the factory default configuration does not require a password (i.e., the password field is blank). 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

[25] The classification of a countermeasure as falling into one of the two categories is, in some instances, arbitrary, since the two may actually overlap.

[26] It should be noted that the distinction between the software and hardware countermeasures identified in this document is blurring, and many could arguably fit into either category.

consider using an automated password generator.[27] 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.

Establishing proper encryption settings. Encryption settings should be set for the strongest encryption available in the product, depending on the security requirements of the organization. Typically, APs have only a few encryption settings available: none, 40-bit shared key, and 128-bit shared key (with 128-bit being the strongest). Encryption as used in WEP, simple stream cipher generation, and exclusive-OR processing does not pose an additional burden on the computer processors performing the function. Consequently, organizations do not need to worry about computer processor power when planning to use encryption with the longer keys. However, it should be noted that some attacks against WEP yield deleterious results regardless of the key size.

Controlling the reset function. The reset function poses a particular problem because it allows an individual to negate any security settings administrators have configured in the AP. It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. 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.

Using MAC ACL functionality. A MAC address is a hardware address that uniquely identifies each computer (or attached device) on a network. Networks use the MAC address to help regulate communications between different computer NICs on the same network subnet. Many 802.11 product vendors provide capabilities for restricting access to the WLAN based on MAC ACLs that are stored and distributed across many APs.[28] The MAC ACL grants or denies access to a computer using a list of permissions designated by MAC address. However, the Ethernet MAC ACL does not represent a strong defense mechanism by itself. Because MAC addresses are transmitted in the clear from a wireless NIC to an AP, the MAC can be easily captured. Malicious users can spoof a MAC address by changing the actual MAC address on their 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.

---

[28] Dave Molta, "WLAN Security On the Rise," www.networkcomputing.com.

Changing the SSID. The SSID of the AP must be changed from the factory default. 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.

Changing default cryptographic keys. The manufacturer may provide one or more keys to enable shared key authentication between the device trying to gain access to the network and the AP. Using a default shared key setting is a security vulnerability because many vendors use identical shared keys in their factory settings. A malicious user may know the default shared key and use it to gain access to the network. Changing the default shared key setting to another key will mitigate the risk. For example, the shared key could be changed to "954617" instead of using a factory default shared key of "111111." No matter what their security level, organizations should change the shared key from the default setting because it is easily exploited. In general, organizations should opt for strong encryption (e.g.,128-bit), regardless of their security levels, whenever it is available. If it is not available or feasible, organizations should, assuming they have already performed a risk analysis, use 40-bit encryption. Finally, a generally accepted principle for proper key management is to change cryptographic keys often.

Changing default SNMP Parameter. Some wireless APs use *SNMP* agents, which allow network management software tools to monitor the status of wireless APs and clients. 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. If SNMP is not required on the network, the organization should disable SNMP altogether.

Changing default channel. One other consideration that is not directly exploitable is the default channel. Vendors commonly use default channels in their APs. 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. Organizations that incur radio interference need to determine if a nearby AP(s) is using the same channel or a channel within five channels of their own, and then choose a channel that is in a different range.[29]

Using DHCP. Automatic network connections involve the use of a Dynamic Host Control Protocol (DHCP) server. The DHCP server automatically assigns IP addresses to devices that associate with an AP when traversing a subnet. 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 through the use of 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 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 would also negate some of the key advantages of wireless networks, such as roaming or establishing ad hoc networks. Another possible solution is to implement a DHCP server inside of the wired network's firewall that grants access to a wireless network located outside of the wired network's firewall. Still another solution is to use APs with integrated firewalls. This

[29] See Tyson Macaulay, "Hardening IEEE 802.11 Wireless Networks."

last solution will add an additional layer of protection to the entire network. All users should evaluate the need for DHCP taking into consideration the size of their network.

3.5.3.1.2 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 and upgrades. Network administrators need to regularly check with the vendor to see whether security patches and upgrades are available and apply them as needed. Also, administrators can check with the NIST ICAT[30] vulnerability database (http://icat.nist.gov) 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: *Applying Security Patches* (currently in draft).

An example of a software or firmware patch is the one related to the RSA Security WEP security enhancement. In November 2001, RSA Security, Inc., developed a technique for the security holes found in WEP. This enhancement, referred to as "fast packet keying," generates a unique key to encrypt each network packet on the WLAN. The IEEE has approved the fast packet keying technology as one fix to the 802.11 protocol.[31] Vendors have started applying the fix to new wireless products and have developed software patches for many existing products. Organizations should check with their individual vendors to see if patches are available for the products they have already purchased.

3.5.3.1.3 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, biometrics, PKI; or a combination of solutions (e.g., smart cards with PKI).[32] 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 have their own individual requirements and will be addressed in greater detail later in the document. All organizations should implement a strong password policy, regardless of the security level. Strong passwords are simply a fundamental measure in any environment. Organizations further should consider other types of authentication mechanisms (e.g., smart cards with PKI) if their 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. This does not in and of itself solve all problems. For example, a strong password scheme used for accessing parameters on a NIC card does nothing to address the problems with WEP cryptography.

3.5.3.1.4 Personal Firewalls

Resources on public wireless networks have a higher risk of attack since they generally do not have the same degree of protection as internal resources. Personal firewalls offer some protection against certain attacks.[33] Personal firewalls are software-based solutions that reside on a client's machine and are either client-managed or centrally managed. Client-managed versions are best suited to low-end users because individual users are able to configure the firewall themselves and may not follow any specific security

---

30 See http://icat.nist.gov/icat.cfm.

31 Ewalt, D., 2001.

32 See Federal Information Processing Standards Publication 196: "Entity Authentication Using Public Key Cryptography," http://csrc.nist.gov/publications/fips/index.html

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

guidelines.[34] Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage them.[35] 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 forms of attack. Depending on the security requirement, organizations may still need additional layers of protection.

3.5.3.1.5 Intrusion Detection System

An IDS is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network. IDS for WLANs can either be host-based or network-based. A host-based IDS adds a targeted layer of security to particularly vulnerable or essential systems. A host-based agent is installed on an individual system (for example, a database server) and monitors audit trails and system logs for suspicious behavior, such as repeated failed login attempts or changes to file permissions. The agent may also employ a checksum at regular intervals to look for changes to system files. In some cases, an agent can halt an attack on a system, although a host agent's primary function is to log and analyze events and send alerts. A network-based IDS monitors the LAN (or a LAN segment) network traffic, packet by packet, in real time (or as near to real time as possible) to determine whether traffic conforms to predetermined attack signatures (activities that match known attack patterns). For example, the TearDrop DoS attack sends packets that are fragmented in such a way as to crash the target system. The network monitor will recognize packets that conform to this pattern and take action such as killing the network session, sending an e-mail alert to the administrator, or other action specified. Host-based systems have an advantage over network-based IDS when encrypted connections, e.g., SSL web sessions or on VPN connections, are involved. Because the agent resides on the component itself, the host-based system is able to examine the data after it has been decrypted. In contrast, a network-based IDS is not able to decrypt data; therefore, encrypted network traffic is passed through without investigation. (For more information about IDS, see NIST Special Publication 800-21, *Intrusion Detection Systems*.)

Users requiring high levels of security should implement an IDS because it provides an added layer of security. Low-end users should consider an IDS as well but only if it is financially feasible. In addition to the cost of the system itself, an IDS requires staff to monitor and react to IDS events and to provide general administration to the IDS database and components.

3.5.3.1.6 Encryption

As mentioned earlier, APs generally have only three encryption settings available: none, 40-bit shared key, and 104-bit. "None" represents the most serious risk since unencrypted data traversing the network can easily be intercepted, read, and altered. A 40-bit shared key will encrypt the network communications data, but there is still a risk of compromise.[36] The 40-bit encryption has been broken by brute force cryptanalysis using a high-end graphics computer and even low-end computers; consequently, it is of questionable value.[37] In general, 104-bit encryption is more secure than 40-bit encryption because of the significant difference in the size of the cryptographic keyspace. Although this is not true for 802.11 WEP because of poor cryptographic design using IVs as discussed previously, it is recommended nonetheless

---

[34] See http://www.iss.net/products_services/hsoffice_protection/blkice_protect_pc.php for an example of a client-managed product.

[35] See http://www.iss.net/products_services/enterprise_protection/rsdesktop/index.php for an example of a centrally managed solution.

[36] This is also a threat for 128-bit encryption but just harder to break.

[37] See Basgall, M., "Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security," (January, 1999, http://www.dukenews.duke.edu/research/encrypt.html.

as a "good practice." Again, users of 802.11b APs and wireless client should be vigilant about checking with the vendor regarding upgrades to firmware and software as they may overcome some of the WEP problems.

3.5.3.1.7 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 it remains secure. It is important for organizations to perform regular audits using wireless network analyzers and other tools. An analyzer, again, 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, such as Netstumbler (see http://www.netstumbler.com/), to determine if wireless products are transmitting correctly and on the correct channels.[38] Administrators should periodically check within the office building space (and campus) for rogue APs and against other unauthorized access. Organizations may also consider using an independent third party to conduct the security audits. Such organizations are, generally, many times more up-to-date on security vulnerabilities, better trained on security solutions, and 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 its WLAN is compliant with established security procedures and policies, and that the system is up-to-date with the latest software patches and upgrades.[39] For more information on network security, see NIST Draft Special Publication 800-42, *Guideline on Network Security Testing*.[40] 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 as well.

3.5.3.2 Hardware Solutions

Hardware countermeasures for mitigating WLAN risks include implementing smart cards, VPNs, PKI, biometrics, and other hardware solutions.

3.5.3.2.1 Smart Cards

Smart cards may add another level of protection, although they also add another layer of complexity. Organizations can use smart cards in conjunction with username or password or by themselves. They can use smart cards in two-factor authentication (see above). Organizations can also combine smart cards with biometrics.

In wireless networks, smart cards provide the added feature of authentication. Smart cards are beneficial in environments requiring authentication beyond simple username and password. User certificate and other information are stored on the cards themselves and generally require the user only to remember a PIN number. Smart cards are also portable; consequently users can securely access their networks from various locations. As with an authentication software solution, these tamper-resistant devices may be integrated into a WLAN solution to enhance the security of the system. Again, users should be careful to fully understand the security provided by the smart card solution. These alone will not solve all the problems of 802.11 security.

---

[38] Internet Security Systems (ISS) (http://iss.net) recently announced "the industry's first Wireless security assess ment tool" called Wireless Scanner™. The Wireless Scanner software provides detection of unauthorized APs and clients, security assessment of AP vulnerability to attack, reporting to display information on Wireless LAN devices, configuration and vulnerabilities, and mobility of scanning for either offsite or onsite access point signals.

[39] 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 www.itsecurity.com.

[40] See http://csrc.nist.gov.

3.5.3.2.2 Virtual Private Networks

VPN technology is a rapidly growing technology to provide secure data transmission across public network infrastructures. VPNs have in recent years allowed corporations to harness the power of the Internet for remote access. Today, VPNs are typically used in three different scenarios: for remote user access, for LAN-to-LAN (site-to-site) connectivity, and for extranets. VPNs employ cryptographic techniques to protect IP information as it passes from one network to the next or from one location to the next. Data that is inside the VPN "tunnel"—the encapsulation of one protocol packet inside another—is encrypted and isolated from other network traffic. A VPN for site-to-site connectivity is illustrated in Figure 3-10. In this scenario, traffic communicated from Site A to Site B is protected as it moves across the Internet. Confidentiality, integrity, and other security services are provided as discussed below.

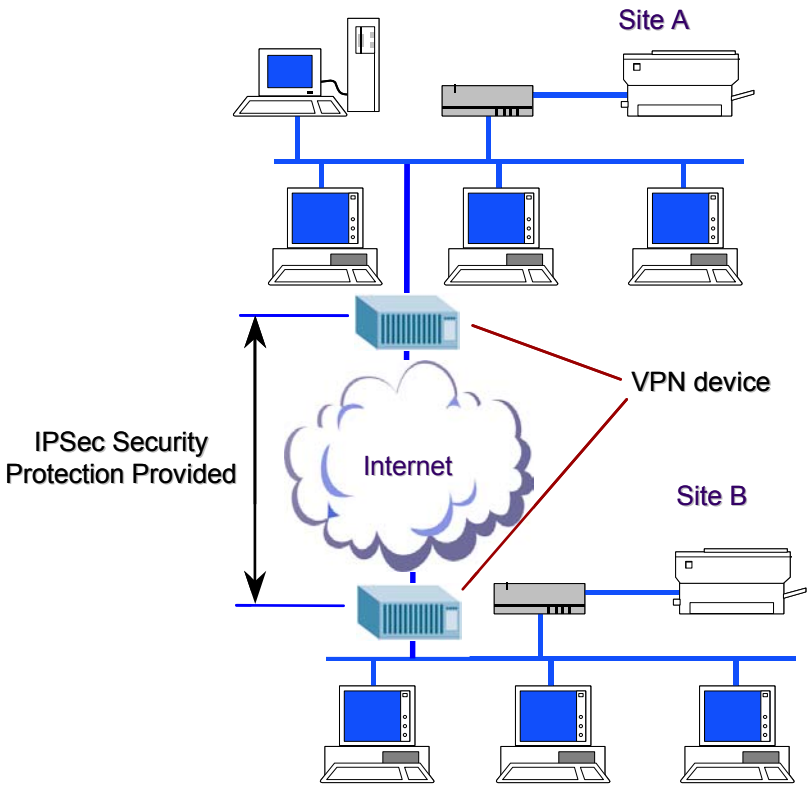

Figure 3-10. Typical Use of VPN for Secure Internet Communications from Site-to-Site

Most VPNs in use today make use of the IPsec protocol suite. IPsec, developed by the Internet Engineering Task Force (IETF), is a framework of open standards for ensuring private communications over IP networks. It provides the following types of robust protection:

- Confidentiality
- Connectionless integrity
- Data origin authentication
- Replay protection
- Traffic analysis protection.

Connectionless integrity guarantees that a received message has not changed from the original message. Data origin authentication guarantees that the received message was sent by the originator and not by a person masquerading as the originator. Replay protection provides assurance that the same message is not delivered multiple times, and that messages are not out of order when delivered. Confidentiality ensures that others cannot read the information in the message. Traffic analysis protection provides assurance that an eavesdropper cannot determine who is communicating or the frequency or volume of communications. IPsec accomplishes the task of routing the messages via an encrypted tunnel by two special IPsec headers inserted immediately after the IP header in each message. The Encapsulating Security Protocol (ESP) header provides privacy and protects against malicious modification, and the Authentication header (AH) protects against modification without providing privacy. The Internet Key Exchange (IKE) Protocol is a mechanism that allows for secret keys and other protection-related parameters to be exchanged prior to a communication without the intervention of a user.[41]

The use of IPsec with WLANs is depicted in Figure 3-11. As shown, the IPsec tunnel is provided from the wireless client through the AP to the VPN device on the enterprise network edge. With IPsec, security services are provided at the network layer of the protocol stack. This means all applications and protocols operating above that layer (i.e., above layer 3) are IPsec protected. The IPsec security services are independent of the security that is occurring at layer 2, the WEP security. As a defense-in-depth strategy, if a VPN is in place, an organization can consider having both IPsec and WEP applied. With a configuration as in Figure 3-11, the VPN encrypts (and otherwise protects) the transmitted data to and from the wired network.[42]

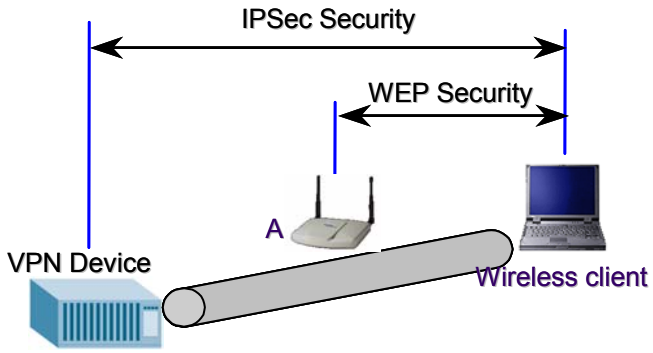

Figure 3-11. VPN Security In addition to WEP

Figure 3-12 illustrates another example of a wireless network with the "VPN overlay." As shown, with wireless devices with VPNs, clients can connect securely to the enterprise network through a VPN gateway on the enterprise edge. Wireless clients establish IPsec connections to the wireless VPN gateway—in addition to or in substitute for WEP. Note that the wireless client does not need special hardware; it just needs to be provided with IPsec/VPN client software. The VPN gateway can use preshared cryptographic keys or digital certificates (public-key based) for wireless client device authentication. Additionally, user authentication to the VPN gateway can occur using Remote Authentication Dial-In User Service (RADIUS) or one-time-passwords (OTP) generated with SecureID, for example. The VPN gateway may or may not have an integral firewall to restrict traffic to certain

[41] For more information on IPsec protocol security, including discussion of the IPsec authentication header, Encapsulating Security Payload (ESP) header, and Internet Key Exchange (IKE), refer to the NIST ITL Bulletin, "An Introduction to IPsec (Internet Protocol Security)," March 2001.

[42] See "Identifying the Weakest Link," *Wireless Internet Magazine*, November/December 2001 (www.Wirelessinternetmag.com).

locations within the enterprise network. Additionally, the VPN gateway may or may not have the ability to create an audit journal of all activities. An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities. A security manager may be able to use an audit trail on the VPN gateway to monitor compliance with security policy and to gain an understanding of whether only authorized persons have gained access to the wireless network.

It should be noted that although the VPN approach enhances the air-interface security significantly, this approach does not completely address security on the enterprise network. For example, authentication and authorization to a particular enterprise application are not addressed with this security solution. Organizations may want to seek assistance in developing a comprehensive enterprise security strategy.

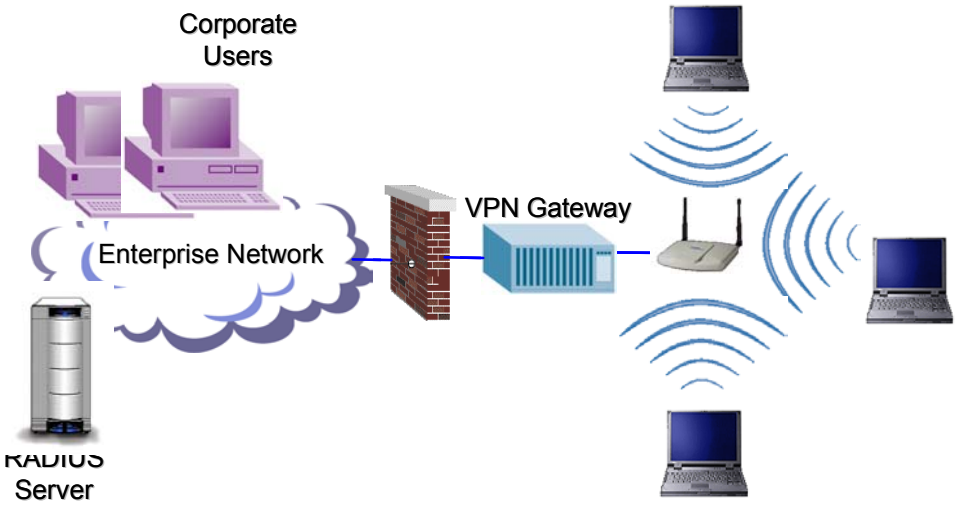

Figure 3-12. Simplified Diagram of VPN WLAN

3.5.3.2.3 Public Key Infrastructure

PKI provides the framework and services for the generation, production, distribution, control, and accounting of public key certificates. It provides applications with secure encryption and authentication of network transactions as well as data integrity and non-repudiation, using public key certificates to do so. WLANs can integrate PKI for authentication and secure network transactions. Third-party manufacturers, for instance, provide wireless PKI, handsets, and smart cards that integrate with WLANs.

Users requiring high levels of security should strongly consider PKI. It provides strong authentication through user certificates and users can use those same certificates with application-level security, such as signing and encrypting (i.e., using encryption certificates) messages. Smart cards provide even greater utility (e.g., portability, mobility) since the certificates are integrated in the card. Users requiring lower levels of security, on the other hand, need to consider carefully the complexity and cost of implementing and administering a PKI before adopting this solution.

3.5.3.2.4 Biometrics

Biometric devices include fingerprint/palm-print scanners, optical scanners (including retina and iris scanners), facial recognition scanners, and voice recognition scanners. Biometrics provides an added layer of protection when used either alone or along with another security solution. For example, for

organizations needing higher levels of security, biometrics can be integrated with wireless smart cards or wireless laptops or other wireless devices and used in lieu of username and password to access the wireless network. Additionally, biometrics can combine with VPN solutions to provide authentication and data confidentiality.

3.5.3.2.5 Other Hardware Solutions

The security industry has responded to the reports of vulnerabilities in WEP and 802.11b WLAN security. Numerous products are currently available to address the vulnerabilities. Several vendors offer combined security solutions in a single product. Two such vendors, described here as examples, are Bluesocket and Vernier Networks. Bluesocket's Wireless Gateway 1000 (WG-1000) effectively creates a firewall between the wireless APs and the rest of the corporate network. The WG-1000 requires authentication via an internal database or a central corporate server. For centralized authentication, the WG-1000 supports RADIUS, Lightweight Directory Access Protocol (LDAP), NT 4 Domain and Windows 2000 Active Directory. In addition, Extensible Authentication Protocol (EAP) for token-based authentication is also supported. The use of roles is available to support assigning different encryption to different users depending on the level of security needed. Role assignment also supports a maximum bandwidth for each user category such as "employees" and "visitors." WG-1000 also supports strong encryption to overcome the weaknesses in WEP that are described in the encryption section above.

Vernier Networks has created the Vernier Networks System that consists of two hardware devices that authenticate, control, redirect, and log network traffic generated by each user's wireless network, cell phone, or other device without installing client software. The devices are the CS 5000 Control Server and the AM 5004 Access Manager. The Control Server centrally manages authentication for all wireless users, coordinates layer 3 roaming, and enforces policies. The Access Manager resides at the edge of the network and connects to APs, enforces user rights for authenticated users, and enables roaming and other security functions such as IPsec, Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP).

These two products illustrate the numerous products that are available to secure the WLAN environment. Organizations that decide to investigate any potential solution should carefully consider the security features offered by various products and make sure that the residual risk, after the countermeasures are applied, is acceptable.

3.6 Emerging Security Standards and Technologies

Like the security industry, standards organizations too have responded to the flurry over insecurities in 802.11b WLANs. Activity is occurring in the Internet Engineering Task Force (IETF) as well as the IEEE. The IEEE is currently working on three separate initiatives for improving WLAN security. The first involves the IEEE 802.11 Task Group i (TGi) which has proposed significant modifications to the existing IEEE 802.11 standard as a long-term solution for security. The TGi is defining a second version of WEP—based on the newly-released Advanced Encryption Standard (AES). The AES-based solution will provide a highly-robust solution for the future but will require new hardware and protocol changes. TGi currently has design requirements to address all the known problems with WEP including the prevention of forgeries and detection of replay attacks.

The second initiative for improving WLAN security is the TGi's short-term solution to address the problems of WEP. The group is defining the Temporal Key Integrity Protocol (TKIP) to address the problems without requiring hardware changes – that is, changes to firmware and software drivers only will be required. Again the primary goal of TKIP is, in the near-term, to remove all known vulnerabilities and allow operation on existing wireless-fidelity (Wi-Fi)-certified hardware. Wi-Fi certification is

awarded by WECA, and this certification ensures that 802.11 devices with the certification are interoperable with other Wi-Fi certified 802.11 devices. The group seeks to produce the solution before the IEEE 802.11i standard is complete.

The third initiative from IEEE is the introduction of a new standard, IEEE 802.1x. The IEEE 802.1x standard defines a generic framework for port-based access control and key distribution. By using the existing Extensible Authentication Protocol (EAP), an AP authenticates a NIC by consulting an authentication server. The 802.1x standard supports authentication servers such as RADIUS or Kerberos. RADIUS is an authentication and accounting server for terminal servers that communicate in the RADIUS protocol. The 802.1x standard can be implemented with different EAP types, including EAP-MD5 for Ethernet LANs and EAP-Transport-level Security (TLS) for 802.11b WLANs. Currently numerous EAP-based protocols are being developed within the IETF, to work with 802.1x, in addressing the WEP WLAN problems.

The 802.1x standard also addresses another serious omission in the WEP standard by providing for secure delivery of session keys. For example, session keys might be created as needed by the AP or supplied by a RADIUS server. If a malicious user recovered keys from WEP session traffic, the keys would be of no value for other sessions. This is an improvement from the original session key delivery method, which allowed session keys to be intercepted. If secure delivery of session keys was not in place, an attack could occur by intercepting the session keys. It is the intent of the IEEE that with the introduction of 802.1x, in concert with EAP techniques from the IETF, some of the security vulnerabilities that have been exposed in the 802.11b standard can be eliminated.

3.7 Case Study: Implementing a Wireless LAN in the Work Environment

Organization A is considering implementing a WLAN so that employees may use their laptop computers anywhere within the boundaries of their office building. Before deciding, however, Organization A has its computer security department perform a risk assessment in accordance with NIST Special Publication 800-30.[43] The security department first identifies WLAN vulnerabilities and threats. The department, assuming that threat-sources will try to exploit WLAN vulnerabilities, determines the overall risk of operating a WLAN and the impact a successful attack would have on Organization A. The manager reads the risk assessment and decides that the residual risk exceeds the benefit the WLAN provides. The manager directs the computer security department to identify additional countermeasures to mitigate residual risk before the system can be implemented.

Using the risk assessment as its basis, the computer security department concentrates on four areas for risk mitigation: physical security, AP location, AP configuration, and security policy. Analysis of physical security reveals that nonemployees are able to gain access to the building after checking in at the main desk. To ensure that only authorized employees and guests may access the building, the security department recommends that Organization A adopt the use of photo identification, card badges, or biometric devices. The security team will physically secure the APs by installing them within the secured building facility, which requires users to have proper identification to enter.

The computer security department wants to minimize the possibility that unauthorized users will access the WLAN from outside the building. The security department evaluates each AP to determine the network vulnerabilities such as eavesdropping. Network engineers conduct a site survey to determine the best physical location for the APs, to reduce the threat of eavesdropping. This involves physically mapping where users have wireless access to the network. The security department realizes that with a high-gain antenna, attackers will still be able to eavesdrop on wireless network traffic. To offset this risk,

[43] See NIST SP 800-30, Risk Management Guide for Information Technology Systems, at http:csrc.nist.gov.

the department proposes placing the WLAN outside the firewall and passing traffic through a VPN that supports high-level encryption. This configuration will greatly reduce the risks associated with eavesdropping.

Next, the computer security department focuses on vulnerabilities related to AP configuration. Because many APs retain the original default factory password setting, the computer security department chooses a robust password to ensure a higher level of assurance. In conjunction with management and network administrators, the security department develops a security policy that requires passwords to be regularly updated and have a minimum length of eight alphanumeric characters. The policy includes the provision to change the encryption setting from "no encryption" to 128-bit encryption. The policy further deals with MAC ACL usage. To provide an additional level of access security, the department allows the use of MAC ACLs whenever possible. The policy also addresses the use of SNMP. The computer security department decides to disable remote SNMP because of the related threat and only allows it from internal hosts. Finally, since many vendors use default shared authentication keys, unauthorized devices can gain access to the network if they know the default key. Consequently, the security department stipulates the use of username and password as supplemental authentication to APs.

The security department adds additional policies to address software upgrades and use of the network. The policy requires system administrators to test and update security patches and upgrades, as soon as the vendor makes them available. Frequent patches and upgrades will help reduce the possibility of attack on the older, faulty version of the software. Check the NIST ICAT Vulnerability Database (http://icat.nist.gov) or an equivalent of source for a comprehensive list of known vulnerabilities in major software packages and hardware products. The policy also strongly discourages users from processing proprietary or employee personal data when connected from their laptops to the WLAN, thus helping to reduce the risk of personnel data exploitation. Additionally, the policy states that if a laptop is lost or stolen, the employee to whom the laptop belongs will promptly notify the security department. This will ensure that the security department can quickly identify the IP address assigned to the laptop and prevent that IP address from accessing the network.

As an additional security measure, the security department recommends that Organization A incorporate the use of an IDS. The IDS will help determine whether unauthorized users are attempting to access, have already accessed, or have compromised the network. The department views an IDS as a useful tool in protecting Organization A's network and, more importantly, the data that traverses it.

The security department presents the manager with the risk assessment, which includes the countermeasures described above (and listed below) and a diagram (Figure 3-13) of the proposed WLAN. The risk assessment also includes an update of the residual risk with the proposed measures in place. Realizing that the benefits of system operation now outweigh the residual risks, the manager agrees to implement the WLAN. However, the security department warns that although the risk assessment is thorough, WLAN technology is continually changing along with the security vulnerabilities that malicious users expose. They offer encryption algorithms as an example. As encryption-breaking programs become more sophisticated, malicious users may expose more software flaws in vendor programs or weaknesses in encryption algorithms. They also point out that users always represent the weakest link in a security chain. The organization must continue to educate the user community about the risks that wireless technologies pose, reiterating, for example, how important it is not to give others their usernames and passwords and not to execute programs that come from unknown sources. In conclusion, the security department conveys that the strategy is one of defense-in-depth. They cite, for example, that WEP encryption will be enabled with random keys, MAC ACLs will be used, and a IPsec-based VPN overlay will be deployed. They also note that they will monitor the appropriate standards organizations and the availability of products such that the optimal security solution—most secure and cost-effective—for the enterprise can be determined.

Organization A's Proposed Countermeasures are as follows:

- Adopt personal identification system for physical access control
- Secure AP configuration
  - Choose robust password to ensure a higher level of security
  - Use 128-bit encryption
  - Create MAC ACLs and enable checking in APs
  - Change SSID from default setting and suppress its broadcast
  - Change WEP keys from default settings
  - Disable remote SNMP
- Conduct site survey and strategically place wireless APs
- Deploy VPN overlay (gateway and client) with integral firewall
- Establish comprehensive security policies regarding use of wireless devices
- Deploy personal firewalls and antivirus software on the wireless clients
- Investigate 802.11b products with best long-term wireless security strategy and longevity in marketplace
- Seek third-party assistance in conducting a security assessment after deployment

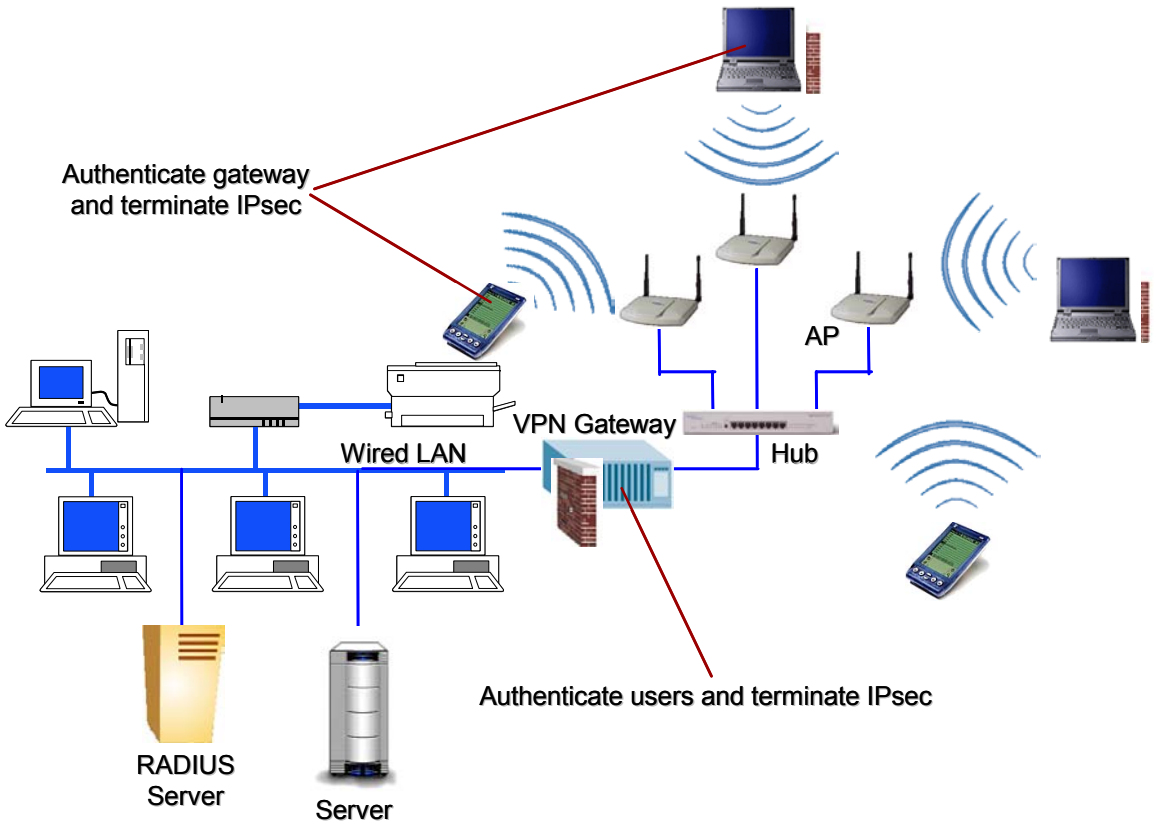

Figure 3-13. Organization A WLAN Architecture

3.8 Wireless LAN Security Checklist

Table 3-3 provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network. For each recommendation or guideline, three columns are provided. The first column, the *Best Practice* column, if checked, means this is something recommended of all organizations. The second column, the *May Consider* column, if checked, means the recommendation is something that an organization may want to 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 *May Consider* column is checked, organizations need to carefully consider the option and weigh the costs versus the benefits. The last column, the *Done?* column, is intentionally left blank and allows an organization to use this table as a true checklist. For instance, an individual performing a wireless security audit in an 802.11 environment can quickly check off each recommendation for the organization – asking, "Have I done this?"

Table 3-3. Wireless LAN Security Checklist

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Develop an organizational security policy that addresses the use of wireless technology, including 802.11.	✓		
Ensure users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
Perform a risk assessment to understand the value of the assets in the organization that need protection.	✓		
Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they come available (prior to purchase).	✓		
Perform comprehensive security assessments at regular intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
Ensure external boundary protection is in place around the perimeter of the building or buildings of the organization.	✓		
Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
Complete a site survey to measure and establish the AP coverage for the organization.	✓		
Take a complete inventory of all APs and 802.11 wireless devices.	✓		
Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	✓		
Ensure AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
Locate APs on the interior of buildings versus near exterior walls and windows.	✓		
Place APs in secured areas to prevent unauthorized physical access and user manipulation.	✓		
Make sure that APs are turned off during all hours during they are not used.	✓		
Make sure the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	✓		
Restore the APs to the latest security settings when the reset functions are used.	✓		
Change the default SSID in the APs.	✓		
Disable the “broadcast SSID” feature so that the client SSID must match that of the AP.	✓		
Validate that the SSID character string does not reflect the organization’s name (division, department, street, etc.) or products.	✓		
Disable the broadcast beacon of the APs.		✓	
Understand and make sure all default parameters are changed.	✓		
Disable all insecure and nonessential management protocols on the APs.	✓		
Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.	✓		
Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	✓		

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Install antivirus software on all wireless clients.		✓	
Install personal firewall software on all wireless clients.		✓	
Deploy MAC access control lists.		✓	
Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.		✓	
Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.		✓	
Ensure encryption being used is as strong as possible given the sensitivity of the data on the network and the processor speeds of the computers.		✓	
Fully test and deploy software patches and upgrades on a regular basis.	✓		
Ensure all APs have strong administrative passwords.	✓		
Ensure all passwords are being changed regularly.	✓		
Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.		✓	
Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable.	✓		
Use static IP addressing on the network.		✓	
Disable DHCP.		✓	
Enable user authentication mechanisms for the management interfaces of the AP.	✓		
Ensure management traffic destined for APs is on a dedicated wired subnet.		✓	
Make sure adequately robust community strings are used for SNMP management traffic on the APs.	✓		
Configure SNMP settings on APs for least privilege (i.e., *read only*). Disable SNMP if it is not used.	✓		
Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.		✓	
Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.		✓	
Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.		✓	
Deploy intrusion detection sensors on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.		✓	
Wait until future releases of 802.11 WLAN technology that incorporates fixes to the security features or enhanced security features.		✓	

3.9 Wireless LAN Risk and Security Summary

Table 3-4 summarizes the wireless applications of LANs, security threats and vulnerabilities associated with those applications, and the risk mitigation for securing the WLAN solutions from these threats and vulnerabilities.

5

Table 3-4: Summary of Wireless LAN Security

Wireless Application	Security Threat/Vulnerability	Risk Mitigation Solution
Physical security: AP cells	Eavesdropping on wireless network communications could come either from inside the network or outside the network if AP range extends beyond building boundaries (e.g., eavesdropping could occur from such areas as parking lots outside of buildings).	Implement: encryption to limit eavesdropping on network communications. Consider placement of AP and AP range (does it extend beyond building boundaries?).
Physical security: AP building-to-building wireless bridging	Eavesdropping of wireless network communications could occur from areas in AP range if no or low encryption is configured.	Implement encryption to limit eavesdropping on network communications.
Physical security: AP channels	When implementing a new AP, it is possible that a different wireless network AP that is using a channel within five channels of the new AP could cause DoS attacks from radio interference.	Check AP channels to determine that AP channel is configured for at least five channels difference from all other nearby APs on different networks.
AP configuration: AP administrative password	Login to AP by unauthorized user is possible if no password is required or default password is not changed.	Implement strong AP password.
AP configuration: Encryption settings	Default setting of APs may be “no encryption”.	Change the AP encryption setting from 40-bit to 128-bit encryption.
AP configuration: Reset functions	If reset option is initiated, default encryption setting could return to “no encryption”.	Return AP setting to appropriate values.
AP configuration: shared key authentication	Shared key authentication is a risk because many vendors use default shared keys, which could be used by unauthorized devices to gain access to the network.	When using shared key authentication, make sure that the keys are unique. Carefully choose WLAN products that support better key management.
AP configuration: AP administrative password	Login to AP by unauthorized user is possible if no password is required. Restrict Remote administration from specific host located on the protected network segment.	Always protect APs with password. Implement a strong password with both alphanumeric and special characters. Require minimum password length of eight characters Implement password expiration of 30 days.
AP configuration: Ethernet MAC ACLs	MAC addresses could be spoofed, since MAC addresses are passed in the clear (with no encryption) when using MAC access control lists. This is a vulnerability because it could allow unauthorized access to the LAN.	If using MAC access control lists for authentication to the LAN, make sure to understand their limitations.

Wireless Application	Security Threat/Vulnerability	Risk Mitigation Solution
AP configuration: Shared Key Authentication	Shared key authentication is a risk because many vendors use default shared keys, which could be used by unauthorized devices to gain access to the network.	Do not use shared key authentication. Use other alternatives to authentication, such as user name and password, instead of shared key.
Encryption	Some encryption algorithms use longer keys (e.g., 3DES and AES) than others (e.g., RC4 and DES); algorithms using shorter keys can be more easily cracked.	Use highest level of encryption possible for wireless communications. WEP should be enabled to provide encryption. However, since WEP provides limited protection, a third-party solution or a VPN may be necessary.
Security patches/upgrades	Vulnerabilities exists when security patches and upgrades are not up to date.	Test and update security patches and upgrades in a timely manner to limit the likelihood that older versions of software are being used that may contain security vulnerabilities.

4. Ad Hoc Networks

This section provides a detailed overview of ad hoc networks, in particular, those based on Bluetooth technology. As mentioned earlier, ad hoc networks are a relatively new paradigm of wireless communications in which there is no fixed infrastructure such as base stations or access points. In ad hoc networks, devices maintain random network configurations formed "on-the-fly," relying on a system of mobile routers connected by wireless links to enable devices to communicate with each other. Devices within an ad hoc network control the network configuration and maintain and share resources. Ad hoc networks are similar to P2P networking in that they both use decentralized networking, in which the information is maintained at the end user location rather than in a centralized database. However, ad hoc and P2P networks differ in that P2P relies on a routing mechanism to direct information queries, whereas ad hoc networks rely on the device hardware to request and share the information.

Ad hoc networks allow devices to access wireless applications, such as address book synchronization and file sharing, within a personal area network (PAN). When combined with other technologies, these networks can be expanded to include network and Internet access. Bluetooth devices that typically do not have access to network resources, but that are connected in a Bluetooth network with an 802.11 capable device, can achieve connection within the corporate network as well as reach out to the Internet.

4.1 Bluetooth Overview

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It 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. Bluetooth is considered a PAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

Bluetooth can be used to connect almost any device to any other device. An example is the connection between a PDA and a mobile phone. The goal of Bluetooth is to connect disparate devices (PDAs, cell phones, printers, faxes, etc.) together wirelessly in a small environment such as an office or home. According to the leading proponents of the technology (Ericsson, Intel, IBM, and Nokia), Bluetooth is a standard that will ultimately—

- Eliminate wires and cables between both stationary and mobile devices
- Facilitate both data and voice communications
- Offer the possibility of ad hoc networks and deliver synchronicity between personal devices.

Bluetooth is designed to operate in the unlicensed ISM (industrial, scientific, medical applications) band that is available in most parts of the world, with variation in some locations. The characteristics of Bluetooth are summarized in Table 4-1. Bluetooth-enabled devices will automatically (termed, "unconsciously") locate each other and form networks.

As with all ad hoc networks, Bluetooth network topologies are established on a temporary and random basis. A distinguishing feature of Bluetooth networks is the master-slave relationship maintained between the network devices. Up to eight Bluetooth devices may be networked together in a master-slave relationship, called a piconet. In a piconet, one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network's hopping scheme). Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device may perform 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. This series of piconets, often referred to as scatternets, allows several devices to be internetworked over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward and away from the master device in the network, the topology, and therefore the relationships of the devices in the immediate network, change.

Table 4-1. Key Characteristics of Bluetooth Technology

Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 – 2.45GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level, and service level); two levels of device trust and three levels of service security. Stream encryption algorithm for confidentiality and authentication. PIN-derived keys and limited management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 720 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technologies. Relatively low data rates.

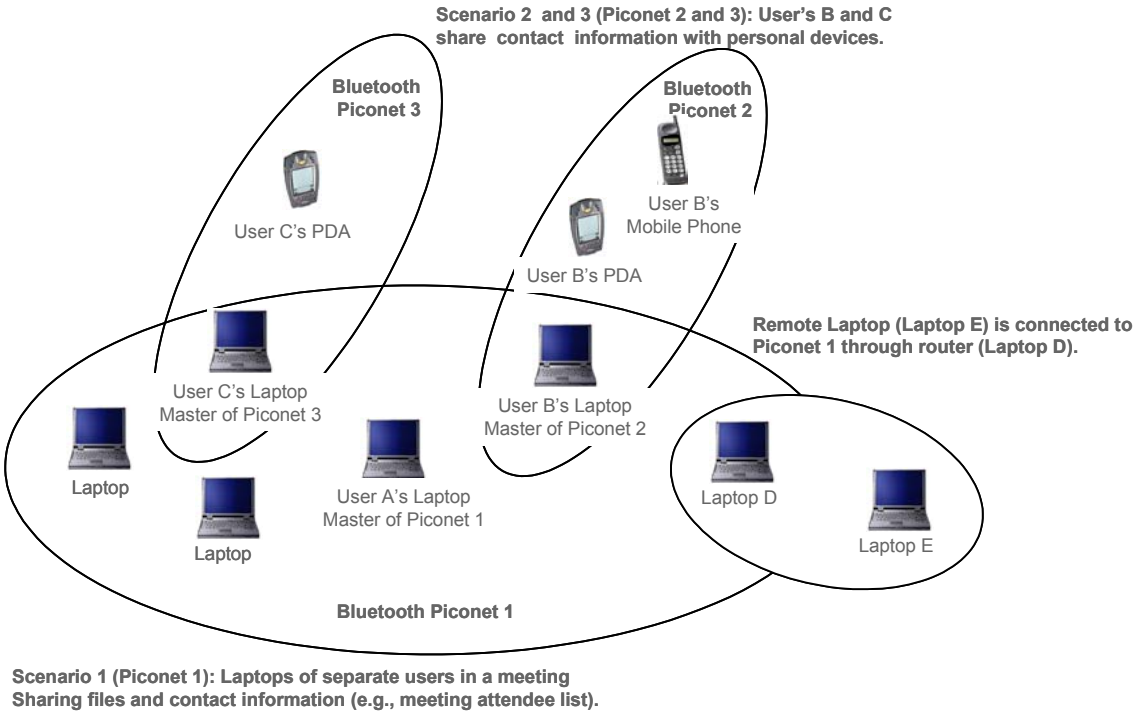

Figure 4-1. Typical Bluetooth Network —A Scatternet

Mobile routers in a Bluetooth network control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting a direct link to each

other. As devices move about in a random fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocols it employs allow Bluetooth to establish and maintain these shifting networks.

Bluetooth transceivers operate in the 2.4GHz, ISM band, which is similar to the band WLAN devices and other IEEE 802.11-compliant devices occupy. Bluetooth transceivers, which use Gaussian Frequency Shift Keying (GFSK) modulation, employ a frequency hopping (FH) spread spectrum system with a hopping pattern of 1,600 times per second over 79 frequencies in a quasi-random fashion. The theoretical maximum bandwidth of a Bluetooth network is 1Mbps. However, in reality the networks cannot support such data rates because of forward error correction (FEC). The second generation of Bluetooth technology is expected to provide up to 2Mbps maximum bandwidth.

Bluetooth networks can support either one asynchronous data channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous data and synchronous speech simultaneously.

Bluetooth uses a combination of packet- and circuit-switching technologies. The advantage of using packet switching in Bluetooth is that it allows devices to route multiple packets of information by the same data path. Since this method does not consume all the resources on a data path, it becomes easier for remote devices to maintain data flow throughout a scatternet.

4.1.1 Brief History

The original architect for Bluetooth, named after the 10th century Danish king Harald Bluetooth, was Ericsson Mobile Communication. In 1998, IBM, Intel, Nokia, and Toshiba formed the Bluetooth SIG, which serves as the governing body of the specification. The SIG began as a means to monitor the development of the radio technology and the creation of a global and open standard. Today more than 2,000 organizations are part of the Bluetooth SIG, comprising leaders in the telecommunications and computing industries that are driving development and promotion of Bluetooth technology. Bluetooth was originally designed, primarily, as a cable replacement protocol for wireless communications. However, SIG members plan to develop a broad range of Bluetooth-enabled consumer devices to enhance wireless connectivity. Among the array of devices that are anticipated are cellular phones, PDAs, notebook computers, modems, cordless phones, pagers, laptop computers, cameras, PC cards, fax machines, and printers. Bluetooth is now standardized within the IEEE 802.15 Personal Area Network (PAN) Working Group that formed in early 1999. The Bluetooth SIG website is www.bluetooth.com ,from which numerous other links are available.

4.1.2 Frequency and Data Rates

The designers of Bluetooth like those of the 802.11b WLAN standard designed Bluetooth to operate in the unlicensed 2.4GHz–2.5GHz ISM frequency band. Because numerous other technologies also operate in this band, Bluetooth uses a frequency-hopping spread-spectrum (FHSS) technology to solve interference problems. The FHSS scheme uses 79 different radio channels by changing frequency about 1,600 times per second. One channel is used in 625 microseconds followed by a hop in a pseudo-random order to another channel for another 625microsecond transmission; this process is repeated continuously. As stated previously, the ISM band has become popular for wireless communications because it is available worldwide and is unlicensed.

In the ISM band, Bluetooth technology permits transmission speeds of up to 1Mbps and achieves a throughput of approximately 720kbps. Although the data rates are low compared to 802.11b wireless LANs, it is still three to eight times the average speed of parallel and serial ports, respectively. This rate is

adequately fast for many of the applications for which Bluetooth was conceived. Moreover, it is anticipated that even faster data rates will be available in future.

4.1.3 Bluetooth Architecture and Components

As with the IEEE 802.11b standard, Bluetooth permits devices to establish either P2P networks or networks based on fixed access points with which mobile nodes can communicate. For the purposes of this document, however, we will discuss the ad hoc network topology only. This topology is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be internetworked without access to the wired LAN (infrastructure network). The basic Bluetooth topology is depicted in Figure 4-2. As shown in this piconet, one of the devices would be a master and the other two devices would be slaves.

Figure 4-2. Bluetooth Ad Hoc Topology

Unlike a WLAN that comprises both a wireless station and an access point, with Bluetooth, there are only wireless stations or clients. Again, a Bluetooth client may be a laptop, a handheld device (e.g., PDA or custom device such as a barcode scanner), desktop, or any other kind of Bluetooth-enabled device. A Bluetooth client is simply a device with a Bluetooth radio and Bluetooth software module incorporating the Bluetooth protocol stack and interfaces.

4.1.4 Range

As shown in Table 4-2, Bluetooth provides one of three classes of power management. Class 3 devices operate at 1 milliwatt (mW) and have an operating range of 0.1 meter to 10 meters (m). Class 2 devices operate at 10mW and have an operating range of 10m. Class 1 devices operate at 100mW and have an operating range of up to 100m.

Table 4-2. Device Classes of Power Management

Type	Power Level	Operating Range
Class 3 Devices	100mW	Up to 100 meters
Class 2 Devices	10mW	Up to 10 meters
Class 1 Devices	1mW	0.1-10 meters

The three ranges for Bluetooth are depicted in Figure 4-3. As shown, the shortest range may be good for applications such as cable replacement (e.g., mouse or keyboard), file synchronization, or business card exchange. The high-powered range can reach distances of 100m, or about 300ft. At this relatively long range, Bluetooth can compete with other WLAN technologies and applications. Additionally, as with the data rates, it is anticipated that even greater distances will be achieved in the future.

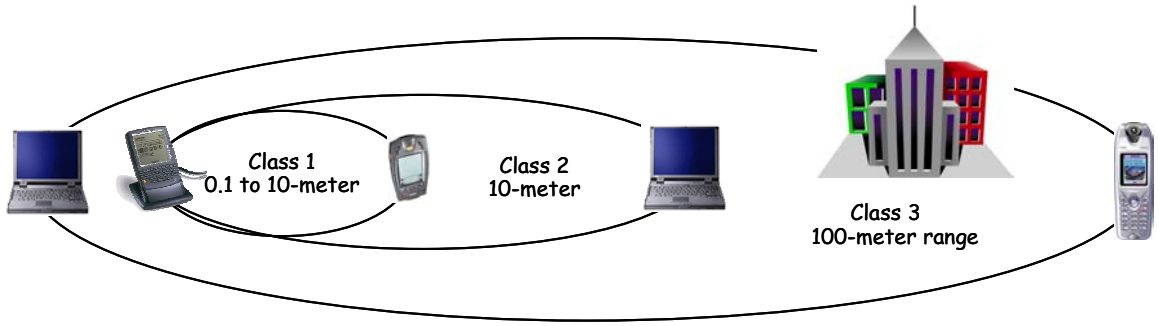

Figure 4-3. Bluetooth Operating Range

4.2 Benefits

Bluetooth offers five primary benefits to users. This ad hoc method of untethered communication makes Bluetooth very attractive today and can result in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for the home user and the enterprise business user.

Benefits of Bluetooth include—

- **Cable replacement—**Bluetooth technology replaces cables for a variety of interconnections. These include peripheral devices (i.e., mouse and keyboard computer connections), USB – at 12Mbps (USB 1.1) up to 480Mbps (USB 2.0); printers and modems, usually at 4Mbps; and wireless headsets and microphones that interface with PCs or mobile phones.

- **Ease of file sharing**—Bluetooth enables file sharing between Bluetooth-enabled devices. For example, participants of a meeting with Bluetooth-compatible laptops can share files with each other. In another example, a Bluetooth-compatible mobile phone acts as a wireless modem for laptops. Using Bluetooth, the laptop interfaces with the cell phone, which in turn connects to a network, thus giving the laptop a full range of networking capabilities without the need of an electrical interface for the laptop-to-mobile phone connection.[44]

- **Wireless synchronization**—Bluetooth provides automatic wireless synchronization with other Bluetooth-enabled devices. For example, personal information contained in address books and date books can be synchronized between PDAs, laptops, mobile phones, and other devices. The synchronization occurs automatically, without the need of input from the device owner. It automatically occurs whenever the devices come within range of one another's device transmission, without the device user's knowledge.

- **Automated wireless applications—**Bluetooth supports automatic wireless application functions. Unlike synchronization, which typically occurs locally, automatic wireless applications interface with the LAN and Internet. For example, an individual working offline on e-mails might be outside of their regular service area—on a flight, for instance. To e-mail the files queued in the

[44] See "An Overview of Bluetooth Security," February 22, 2001, at http://www.sans.org.

inbox of the laptop, the individual, once back in a service area (i.e., having landed), would activate a mobile phone or any another device capable of connecting to a network. The laptop would then automatically initiate a network join by using the phone as a modem and automatically send the e-mails after the individual logs on.

- **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 together to use each other's 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 that connection.

With all of these benefits, Bluetooth is expected to be built into office appliances (e.g., PCs, faxes, printers, laptops), communication appliances (e.g., cell phones, handsets, pagers, headsets), and home appliances (DVD players, cameras, refrigerators, microwave ovens). Applications for Bluetooth also include vending machines, banking, and other electronic payment systems; wireless office and conference rooms; smart home; and in-vehicle communications and parking.

4.3 Security of Bluetooth

This section helps the reader to understand the built-in security features of Bluetooth. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. Security for the Bluetooth radio path is depicted in Figure 4-4.

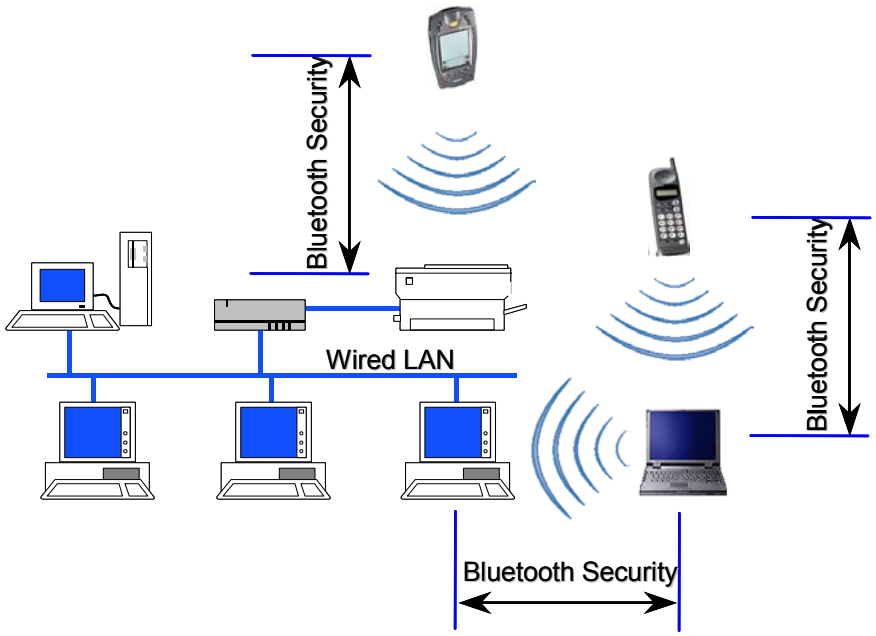

Figure 4-4. Bluetooth Air-Interface Security

As shown in the illustration, security for Bluetooth is provided on the various wireless links – on the radio paths only. In other words, link encryption and authentication may be provided but true end-to-end security is not possible. In the example provided, security services are provided between the PDA and the printer, between the cell phone and laptop, and between the laptop and the desktop.

Briefly, the three basic security services defined by the Bluetooth specifications are the following:

- **Confidentiality**—Confidentiality, or privacy, is one security goal of Bluetooth. The intent is to prevent information compromise from eavesdropping (passive attack). This service, in general, addresses, "Are only authorized persons allowed to view my data?"
- **Authentication**—A second goal of Bluetooth is the identity verification of communicating devices. This security service addresses, "Do I know to whom I'm communicating?" This service provides an abort mechanism if a device cannot authenticate properly.
- **Authorization**—A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses, "Has this device been authorized to use this service?"

It is important to note that, like the 802.11 standard, Bluetooth did not address other security services such as audit and non-repudiation. If these other security services are desired or required, they must be provided through other means. The three security services offered by Bluetooth and details about the modes of security are described in greater detail below.

Also worthwhile to note, Bluetooth provides a frequency-hopping scheme with 1,600 hops/second combined with radio link power control (to limit transmit range). These characteristics 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 for an adversary to locate the Bluetooth transmission. Using the power control feature appropriately forces any potential adversary to be in relatively close proximity to pose a threat to the Bluetooth network.

4.3.1 Security Features of Bluetooth per the Specifications

Bluetooth has three different modes of security. Each Bluetooth device can operate in one mode only at a particular time. The three modes are the following:

- **Security Mode 1**—Nonsecure mode
- **Security Mode 2**—Service-level enforced security mode
- **Security Mode 3**—Link-level enforced security mode.

In Security Mode 1, a device will not initiate any security procedures. In this nonsecure mode, the security functionality (authentication and encryption) is completely bypassed. In effect, the Bluetooth device in Mode 1 is in a "promiscuous" mode that allows other Bluetooth devices to connect to it. This mode is provided for applications for which security is not required, such as exchanging business cards.

In Security Mode 2, the service-level 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 services and to devices. The centralized security manager maintains polices for access control and interfaces with other protocols and device users. Varying security polices 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. Obviously, in this mode, the notion of authorization is introduced – the process of deciding if device A is allowed to have access to service X.

In Security Mode 3, the link-level security mode, a Bluetooth device initiates security procedures before the channel is established. This is a built-in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication (unidirectional or mutual) and

encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two devices communicate for the first time.

The Bluetooth modes are depicted in Figure 4-5.

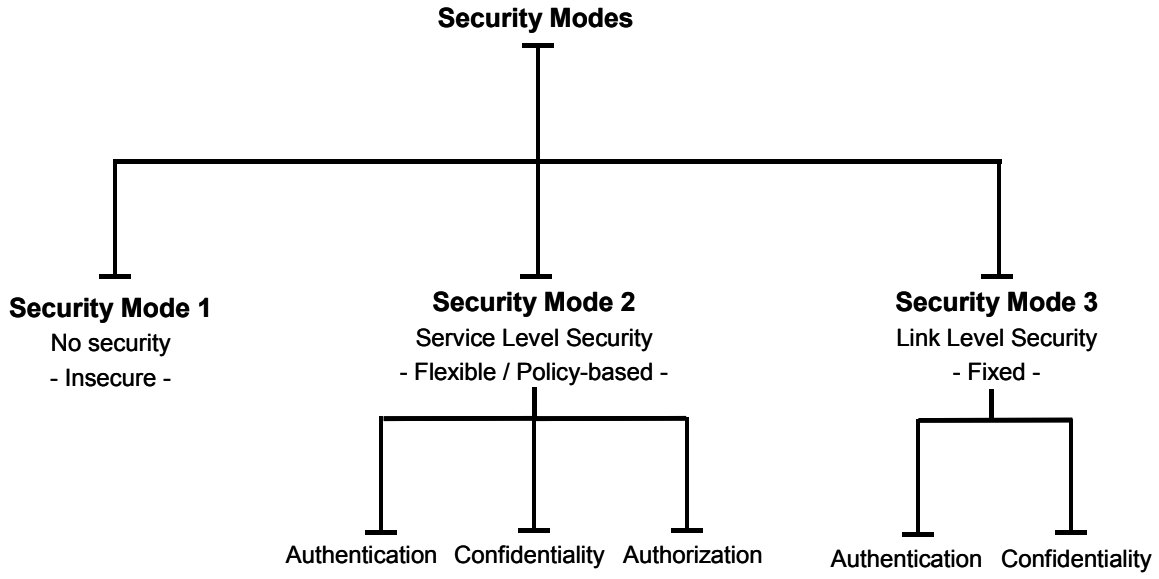

Figure 4-5. Taxonomy of Bluetooth Security Modes

4.3.1.1 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 verifier is the Bluetooth device validating the identity of another device. The claimant is the device attempting to prove its identity. 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 4-6. As shown, one of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier).

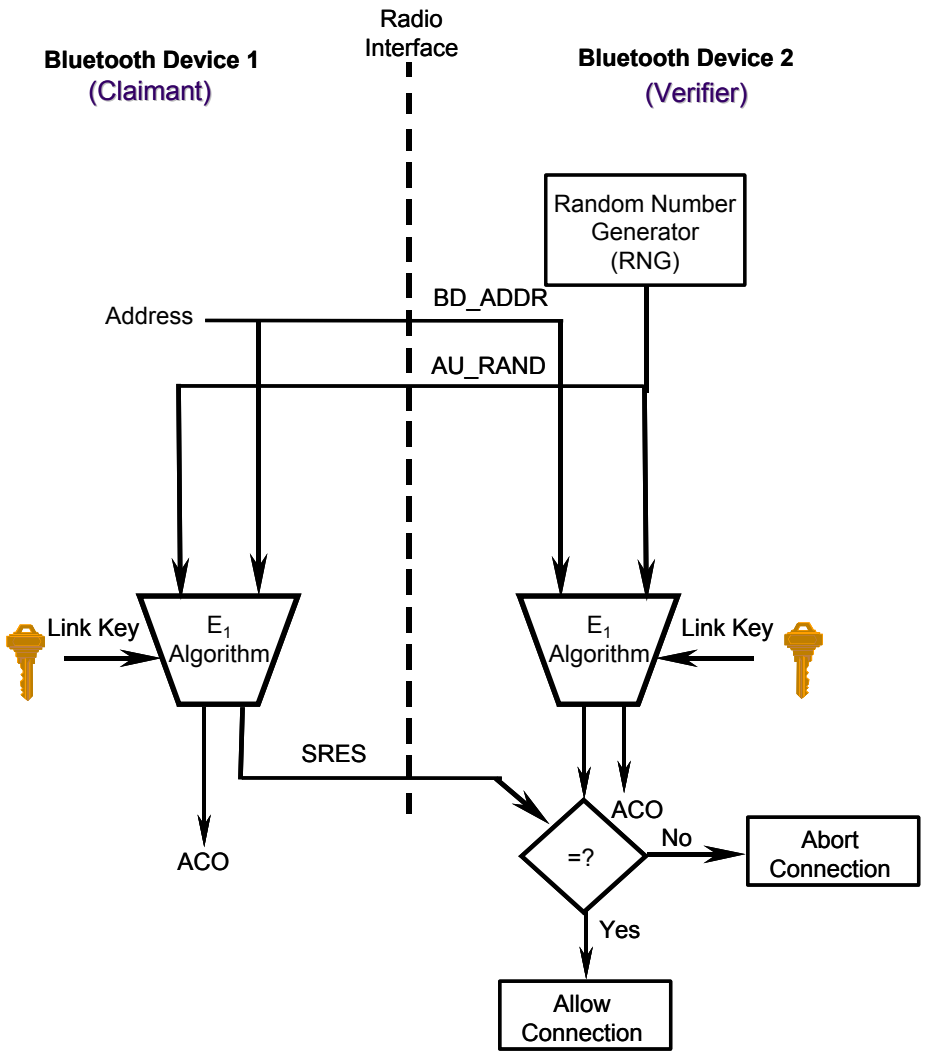

Figure 4-6. Bluetooth Authentication

The steps in the authentication process are the following:

Step 1. The claimant transmits its 48-bit address (BD_ADDR) to the verifier.

Step 2. The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.

Step 3. The verifier uses the E_1 algorithm to compute an authentication response using the address, link key, and random challenge as inputs. The claimant performs the same computation.

Step 4. The claimant returns the computed response, SRES, to the verifier.

Step 5. The verifier compares the SRES from the claimant with the SRES that it computes.

Step 6. If the two 32-bit SRES values are equal, the verifier will continue connection establishment.

If authentication fails, a Bluetooth device will wait an interval of time before a new attempt can be made. This time interval will increase exponentially to prevent an adversary from repeated attempts 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.

Again, the Bluetooth standard allows both uni-directional and mutual-authentication to be performed. The authentication algorithm used for the validation is based on the SAFER+ algorithm.[45]

The Bluetooth address is a public parameter that is unique to each device. This address can be obtained through a device inquiry process. The private key, or link key, is a secret entity. The link key is derived during initialization, is never disclosed outside the Bluetooth device, and is never transmitted over the air-interface. The random challenge, obviously a public parameter, 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. With knowledge of the challenge and response parameters, it should be impossible to predict the next challenge or derive the link key.

The parameters used in the authentication procedure are summarized in Table 4-3.

Table 4-3. Summary of Authentication Parameters

Parameter	Length	Secrecy Characteristic
Device address	48 bits	Public
Random challenge	128 bits	Public, unpredictable
Authentication (SRES) response	32 bits	Public
Link key	128 bits	Secret

4.3.1.2 Confidentiality

In addition to the authentication scheme, Bluetooth provides for a confidentiality security service to thwart eavesdropping attempts on the air-interface. Bluetooth encryption is provided to protect the payloads of the packets exchanged between two Bluetooth devices. The encryption scheme for this service is depicted conceptually in Figure 4-7.

As shown Figure 4-7, the Bluetooth encryption procedure is based on a stream cipher, E_0. A keystream output is exclusive-ORed with the payload bits and sent to the receiving device. This keystream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR).[46] The encrypt function takes as inputs, the master identity (BD_ADDR), the random number (EN_RAND), a slot number, and an encryption key, which initialize the LFSRs before the transmission of each packet, if encryption is enabled. Since the slot number used in the stream cipher changes with each packet, the ciphering engine is also reinitialized with each packet even though the other variables remain static.

[45] 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.

[46] 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. The security of this type of KSG is dependent on a number of factors; many KSGs are insecure.

As shown in Figure 4-7, 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, random number (EN_RAND again), and the ACO value. The ACO parameter, a 96-bit authenticated cipher offset, is another output produced during the authentication procedure shown in Figure 4-6. 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

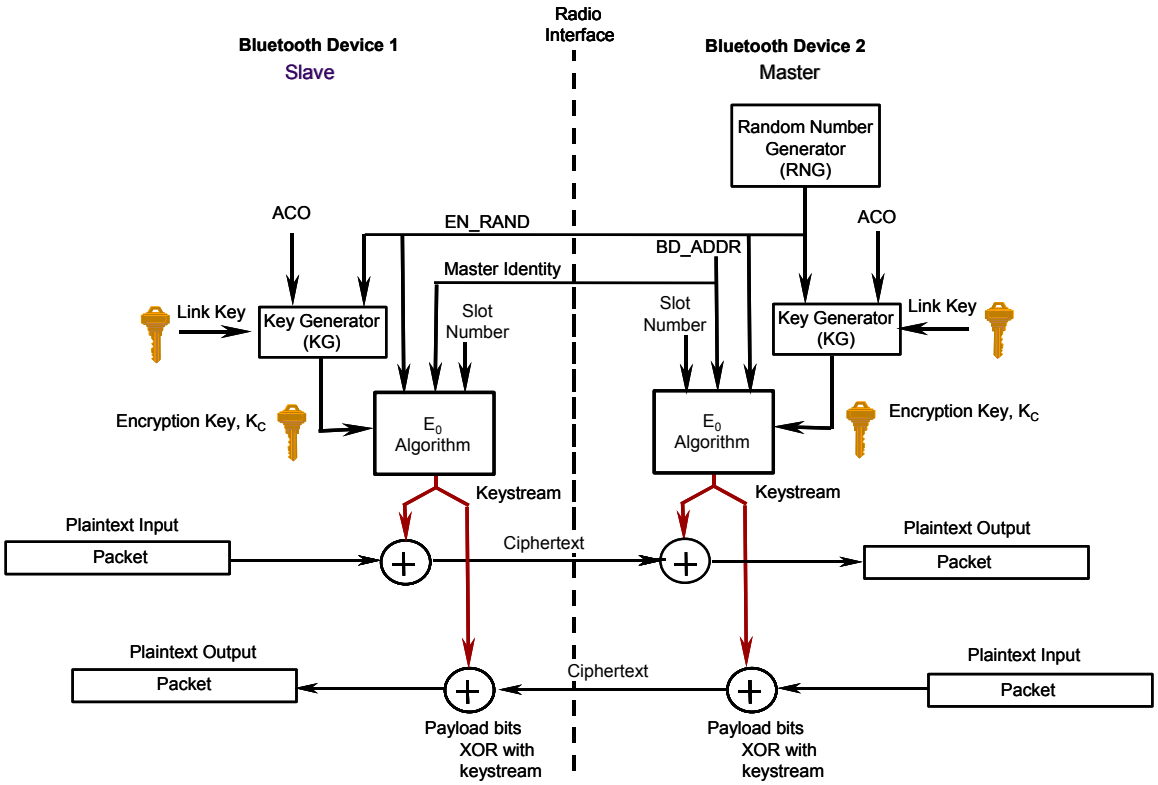

Figure 4-7. Bluetooth Encryption Procedure

The encryption key (K_C) is generated from the current link key. The key size may vary from 8 bits to 128 bits and is negotiated. The negotiation process occurs between master and slave devices. During negotiation, a master device makes a key size suggestion for the slave. In every application, 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 – rending the link totally insecure.

The Bluetooth specification also allows three different encryption modes to support the confidentiality service:

- **Encryption Mode 1**—No encryption is performed on any traffic.
- **Encryption Mode 2**—Broadcast traffic goes unprotected (not encrypted), but individually addressed traffic is encrypted with the master key.
- **Encryption Mode 3**—All traffic is encrypted with the master key.

The link key is generated during an initialization phase, during which time two Bluetooth devices that are communicating are "associated" or "bonded." Per the Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. The PIN entry, device association, and key derivation are depicted conceptually in Figure 4-8. After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4-digit PIN may be sufficient for some applications; however, longer codes may be necessary.

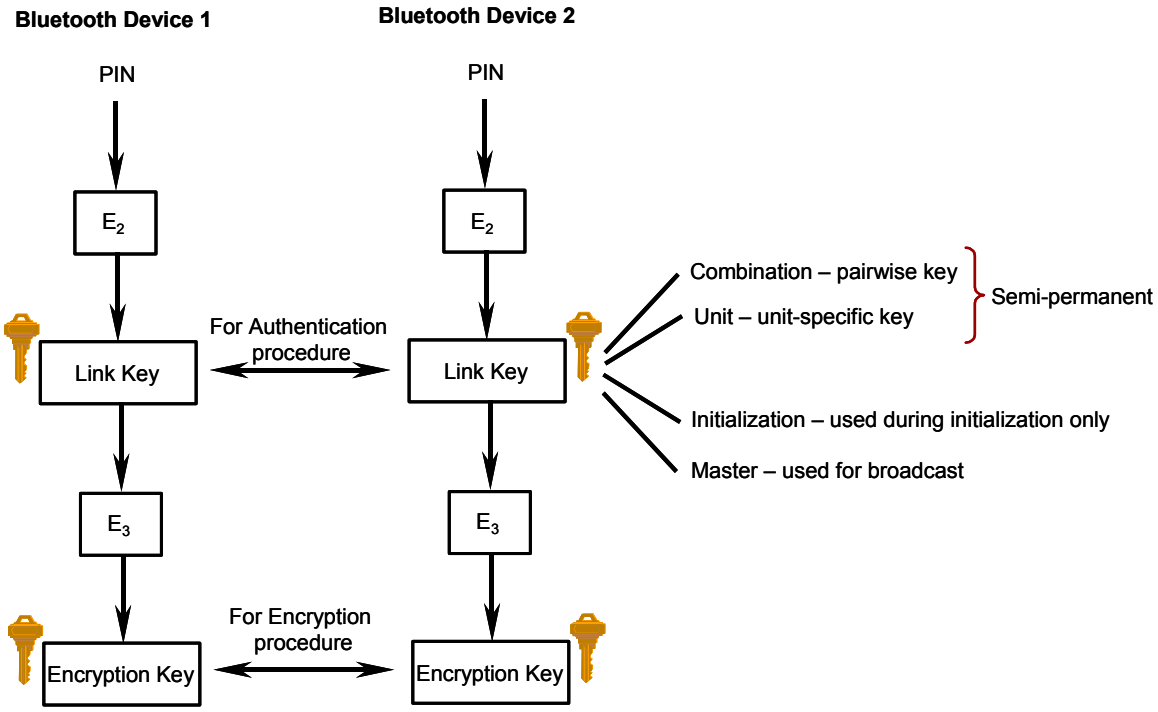

Figure 4-8. Bluetooth Key Generation from PIN

4.3.1.3 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 levels of trust are "trusted" and "untrusted." Trusted devices are ones that have a fixed relationship and therefore have full access to all services. Untrusted devices do not maintain a permanent relationship; this results in a restricted service access. For services, three levels of security have been defined. These levels are provided so that the requirements for authorization, authentication, and encryption can be set independently.

The security levels can be described as follows:

- **Service Level 1**—Those that require **authorization and authentication**. Automatic access is granted only to trusted devices. Untrusted devices need manual authorization.
- **Service Level 2**—Those that require **authentication only.** Access to an application is allowed only after an authentication procedure. Authorization is not necessary.
- **Service Level 3**—Those that are **open to all devices**. Authentication is not required and 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 and not to others. It is important to understand that Bluetooth core protocols can authenticate only devices and not users. This is not to say that user-based access control is not possible. The Bluetooth security architecture (through the security manager) allows applications to enforce their own 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.

4.3.2 Problems with the Bluetooth Standard Security

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

Table 4-4. Key Problems with Existing (native) Bluetooth Security

Security Issue / Vulnerability	Remarks
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.
PINs are only 4 digits.	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.
An elegant way to generate and distribute PINs does not exist.	Establishing PINs in large Bluetooth networks with many users may be difficult. Scalability problems frequently yield security problems. PINs suffer all the typical problems of passwords: get written down, do not change, get forgotten, get shared, etc.
Initialization key may be too weak.	The Bluetooth SIG needs to develop a more robust initialization key generation procedure.
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.
The master key is shared.	The Bluetooth SIG needs to develop a better broadcast keying scheme.
No user authentication.	Device authentication only is provided. Application-level security and user authentication can be employed.
Repeating attempts for authentication.	The Bluetooth SIG needs to develop a limit feature to prevent unlimited requests.
E_0 stream cipher algorithm is weak.	The Bluetooth SIG needs to develop a more robust encryption procedure.
Negotiable key length.	A global agreement must be established on minimum key length.
Eavesdropping resulting from unit key sharing.	A corrupt user may be able to compromise the security (gain unauthorized access to) between two other users if that corrupt user has communicated with either of the other two users. This is because the link key (unit key), derived from shared information, gets disclosed.
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.

Security Issue / Vulnerability	Remarks
Device authentication is simple shared-key challenge-response.	One-way-only 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.
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.
Security services are limited.	Audit, non-repudiation, and other services do not exist. If needed, these can be developed at particular points in a Bluetooth network.

4.4 Security Requirements and Threats

Bluetooth offers several benefits and advantages. However, organizations must not only address the security threats associated with Bluetooth before they implement the technologies; they must also assess the vulnerabilities of the devices they allow to participate in the Bluetooth networks. Specifically, organizations need to address security concerns for confidentiality, data integrity, and network availability.

There have been some reports and papers describing practical or possible attacks on Bluetooth wireless and exposing risks to any organization deploying the technology. This subsection will briefly cover some of the risks to security, i.e., attacks on confidentiality, integrity, and network availability.

The reader is directed to Figure 3.9 in the 802.11 wireless section for a general taxonomy of security attacks to help organizations and users understand some of the attacks against Bluetooth. This figure and relevant discussion will not be repeated here.

4.4.1 Loss of Confidentiality

Threats to confidentiality involve, first of all, compromised Bluetooth devices. When a Bluetooth device that is part of a piconet becomes compromised (e.g., is in the possession of an unauthorized user), it may still receive information that the malicious user should not access. Moreover, the compromised device may still have network or information privileges, resulting in a compromise of the wider network as well. In the latter case, the compromised device may not only receive normal proprietary traffic but may also request that information as part of a targeted network attack. A trait of Bluetooth that makes this compromise unique is that the Bluetooth network requires device—and not user—authentication to access resources. Once the device is authenticated, it is automatically connected to resources without the need for subsequent authentication.[47]

Bluetooth devices themselves have inherent security vulnerabilities. For example, malicious users can use wireless microphones as bugging devices. Although such attacks have not been documented because Bluetooth is not yet commercially prevalent, there have been recorded incidents of successful attacks on PCs using programs such as Back Orifice and Netbus. If a malicious user has a program such as Back Orifice installed on a device in the Bluetooth network, that user could access other Bluetooth devices and networks that have limited or no security. These same programs could be used against Bluetooth devices and networks. Bluetooth devices are further vulnerable because the system authenticates the devices, not

[47] Devices are authenticated through the Bluetooth chip at the link level. The Bluetooth authentication scheme is essentially a challenge-response strategy, where a two-move protocol is used to check whether the other party knows a shared identical secret key (a symmetric key). Basically the protocol checks that both devices have the same key, and if they do authentication is successful. This process is sometimes invisible to the device user, since the devices can automatically authenticate once they are within the transmission range. (See www.palowireless.com/blueartricles/cc1_security1.asp for more information.)

the users. As a result, a compromised device can gain access to the network and compromise both the network and devices on the network.

Authorized remote users pose a threat to Bluetooth networks. Remote users are not always subject to the same security requirements as users onsite. They frequently use nonsecure links, whether at home or on travel. In the process of connecting, they transmit user IDs and passwords, which a malicious user can capture using a network sniffer. Without the secure perimeter typically provided in an office environment, the need to be in close proximity to the user to intercept traffic becomes less. Once the device or link is compromised, all devices in that Bluetooth network are vulnerable to attacks. For example, a compromised link allows a malicious user to monitor data traffic, while a compromised device allows the malicious user to request and receive sensitive data. In addition, remote users often delegate authority (rights) to a host machine (e.g., a shared server) to execute programs. If the remote device is compromised and the authorized user had granted rights to the machine, the malicious user could then use those rights to compromise the network.

An example of this is a PDA automatically requesting a laptop to send and download e-mails. If the user had enabled (i.e., had delegated authority to) the PDA to download e-mail from the laptop, a malicious user could use the compromised PDA to obtain the e-mail.

The man-in-the-middle attack poses an additional threat to Bluetooth devices that rely on unit keys – typically, the more simple "dumb" devices. In this attack, the man-in-the-middle (Device C) obtains the security encryption key a network device (Device A) uses to monitor traffic between itself and another network device (Device B). All the attack requires is that Device A separately share its unit key (a static key unique to each device) with Device C and Device B. The reason for the connections between Device A and B and A and C may be completely unrelated, and the level of confidentiality may even be different. However, once C knows the unit key, it can use a fake device address to calculate the encryption key and monitor traffic between A and B without their knowledge. The man-in-the-middle attack does not require costly or special equipment to carry out the attack. A knowledgeable malicious user who has access to the unit key and who can mimic a Bluetooth address to generate the encryption key can conduct the attack. Attacks such as these use a priori knowledge of the targeted Bluetooth devices. Although this does not necessarily preclude malicious users from randomly attacking Bluetooth devices as they enter the transmission range, there are no documented instances of such attacks.

Figure 4-9 illustrates the attack. A trusted PDA (Device A) shares proprietary information with a trusted laptop (Device B). During the connection with B, Device A connects to an untrusted PDA (Device C) to share personal contacts in A's PDA address book. Once C makes the connection to A, C now becomes the man-in-the-middle and can monitor the traffic between the A and B by using device A's unit key and a fake address. The biggest danger in such monitoring is that the owners of device A or B may never realize that the information is being compromised.

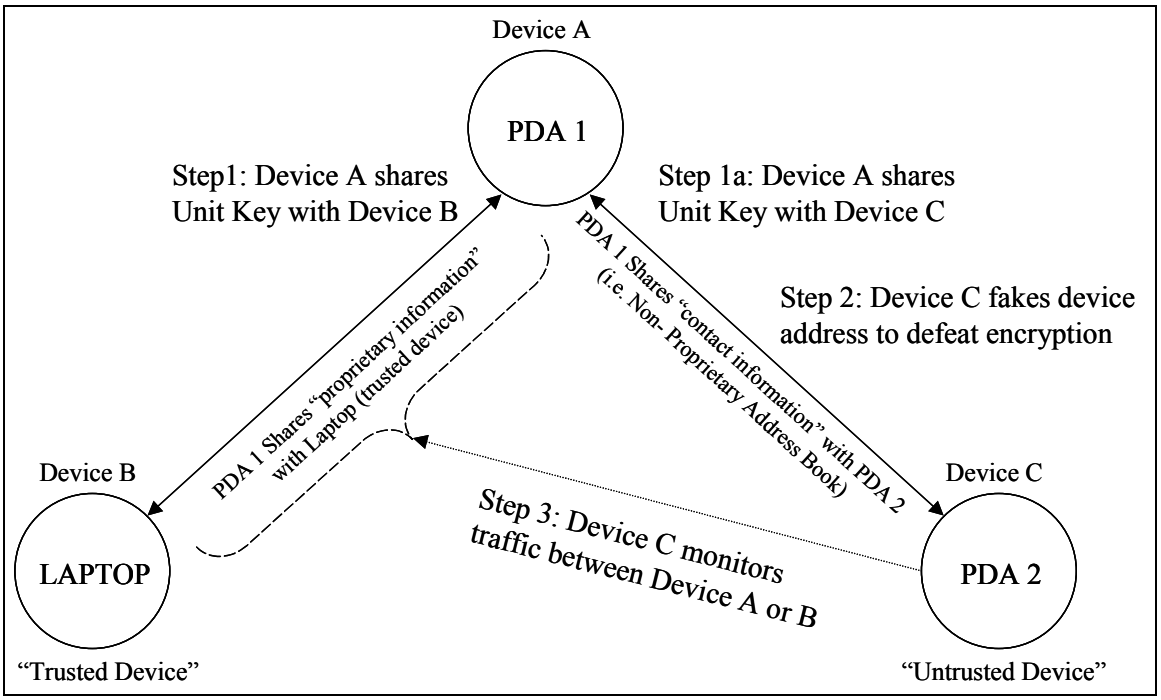

Figure 4-9. Man-in-the-Middle Attack Scenarios

To date, there is no available software for monitoring such intrusions, and Bluetooth devices are invisible to network administrators.[48] It is important to remember that although different participants from different organizations may enforce different security policies, in an ad hoc network this has little bearing. Every device participating in the ad hoc network is susceptible to the security risks of every other device. As the saying goes, a chain is only as strong as its weakest link.

Although not directly a security threat, organizations need to consider the potential for privacy violations when implementing Bluetooth technologies. Each Bluetooth device is equipped with its own unique address (BD_ADDR), and this address is used to log each device's participation in the network. Although logging ensures non-repudiation (i.e., an individual cannot deny that he/she participated in the network since the address is logged), it also allows organizations to monitor and track what an individual does on the network.[49]

4.4.2 Loss of Integrity

Violations to integrity result from the corruption of an organization or user's data. The immediate effect is similar to that of a confidentiality, or disclosure, threat: a compromised network. However, integrity threats extend beyond this, involving the alteration, addition, or deletion of information, which is then passed through the network without the user or network administrator's knowledge. Information subject to such corruption includes files on the network and data on user devices. For example, a malicious user might employ an untrusted device, such as a PDA, to access the address book of another PDA or laptop. However, instead of just monitoring the information, as would be the case with a disclosure threat, the malicious user alters the contact information without the owner's knowledge or may even delete the information completely. If undetected, such attacks could result in the organization (or user) losing confidence in its data and system.

[48] See "Security in a Mobile World – Is Bluetooth the Answer?" *Computers and Security*, Vol. 20 (2001).
[49] See "Bluetooth Security: An Oxymoron?" November 28, 2000, at http://www.mcommercetimes.com.

4.4.3 Loss of Availability

DoS and distributed DoS (DDoS) attacks result in the loss of network availability and "usability upon demand" for authorized users and devices. DoS attacks block authorized user access to system resources and network applications. Besides the typical DoS attacks (e.g., flooding techniques) directed against LANs and Internet services, Bluetooth devices are also susceptible to signal jamming. Bluetooth devices share bandwidth with microwave ovens, cordless phones, and other wireless networks and thus are vulnerable to interference. Malicious users can interfere with the flow of information (i.e., disrupt the routing protocol by feeding the network inaccurate information) by using devices that transmit in the 2.4GHz ISM band. Disrupting the routing protocol prevents ad hoc network devices from negotiating the network's dynamic topologies. Remote users may encounter jamming more frequently than onsite users. Not only must remote users contend with the same interference users experience in the office, but since the remote environment is uncontrolled, remote devices are more likely to be in close proximity to devices (e.g., other Bluetooth and ISM band devices) that are intentionally or unintentionally jamming their signals.

Another threat associated with ad hoc devices is a battery exhaustion attack. This attack attempts to disable a device by draining its battery. A malicious user continually sends requests to the device asking for data transfers (assuming the user is part of the network topology) or asking the device to create a network.[50] Although this type of attack does not compromise network security, it ultimately prevents the user from gaining access to the network, because the device cannot function.

4.5 Risk Mitigation

Bluetooth is a relatively new standard and has yet to become prevalent in the marketplace. However, countermeasures are available to help secure Bluetooth networks. These measures include management countermeasures, operational countermeasures, and technical countermeasures.

4.5.1 Management Countermeasures

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 the user's responsibilities. The policy document should include a list of approved uses for Bluetooth networks, the type of information that may be transferred in the network, and any disciplinary actions that may result from misuse. The security policy should also specify a proper password usage scheme.

4.5.2 Operational Countermeasures

Since Bluetooth devices do not register when they join a network, they are invisible to network administrators. Consequently, it is difficult for administrators to apply traditional physical security measures. However, there are some security approaches that can be applied, including establishing spatial distance and securing the gateway Bluetooth devices that connect remote Bluetooth networks or devices.

Establishing spatial distance requires setting the power requirements low enough to prevent a device operating on the organization's premises from having sufficient power to be detected 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 30 feet (using a class 3 device). Organizations that require both high levels and low levels of security should maintain a secure perimeter

[50] See "Bluetooth Security," May 2000, at http://www.niksula.cs.hut.fi/~jiitv/bluesec.html.

so that onsite network users can maintain secure connections in their office spaces. Organizations with requirements for high levels of security should also restrict unauthorized personnel from using PDAs, laptops, and other electronic devices within the secure perimeter.

4.5.3 Technical Countermeasures

As with WLANs, Bluetooth technical countermeasures fall into one of two categories: software and hardware security solutions. Bluetooth software solutions focus on PIN and private authentications, while hardware solutions involve the use of the Bluetooth device address and link keys that reside at the link level.

4.5.3.1 Software Solutions

Software solutions inherent in Bluetooth technology include the PIN and private authentication. Bluetooth enforces PIN codes at the link level. PINs may be 1 to 16 octets (8-bits to 128-bits) in length, depending on the degree of security selected by the device user. Bluetooth devices use the PIN codes, effectively, for device authentication: the PIN acts as a variable in the initialization key generation process. For authentication between two devices, Bluetooth has the option of storing and retrieving the codes automatically and directly from memory or having a user enter the PIN into the device when the device is initializing. To generate keys between two devices, the devices can use the PIN code from a single device or use the PIN codes of both devices. Because the PIN codes are necessary for authentication and link security, administrators should ensure that Bluetooth devices use PIN codes other than the default, or lowest, setting (e.g., 0000).[51]

Since Bluetooth devices can store and automatically access link-level PIN codes from memory, a Bluetooth device should employ device authentication as an extra layer of security. Incorporating application-level software that requires password authentication to secure the device will add an extra layer of security. Organizations with both high- and low-end users should incorporate application-level software that requires password authentication in Bluetooth devices. Again, passwords are fundamental measures, adding an extra layer of security.

Additionally, some of the software solutions identified for 802.11b WLANs may be appropriate for Bluetooth devices as well. The reader is encouraged to review and consider the software solutions outlined in Section 3. Because Bluetooth is a relatively new wireless communications technology, supplemental software solutions (e.g., application security toolkits, robust IPsec VPN overlay) have not appeared in the marketplace. Moreover, if Bluetooth is intended for less critical and short-range applications, such as simple keyboard or mouse cable replacements, the addition of enhanced security may be ponderous, expensive, and unnecessary.

4.5.3.2 Hardware Solutions

Hardware security solutions for Bluetooth devices are inherent in the design of the standard itself. As mentioned above, the link layer provides its own form of security. Bluetooth uses a device address that is unique to each device. The device address, a 48-bit identifier (note: this is a 6-byte public parameter), serves several purposes, among which is generating 128-bit link keys and encryption keys. For example, a key-generating algorithm (defined by the Bluetooth standards) in combination with a random-generated number and the Bluetooth device address creates the unit and combination keys.

[51] See "Bluetooth Security," May 2000, at http://www.niksula.cs.hut.fi/~jiitv/bluesec.html.

Link keys, the 128-bit random numbers that form the basis of Bluetooth security, are in the form of a unit key, a temporary master key, a combination key and an initialization key. A device in the network generates the unit key (a key that rarely changes) when the new device first comes into operation. This unit key may then become the device's link key for the network. However, since the sharing of unit keys represents a vulnerability (see Section 4.3), organizations should regulate the exchange of unit keys with untrusted devices. Combination keys, pair-wise unique link keys, are derived from information from two communicating devices. The combination key, however, becomes a unique link key for those devices only. This adds a layer of security because it requires a malicious user to possess both unit keys rather than just one. Even if the unit key of one of the devices is compromised, the link is still not compromised. It is important to note that unit key and combination keys are functionally indistinguishable; the difference is merely in the way they are generated. Hence, a Bluetooth device may have either a unit key or a combination key but not both.

Another hardware solution, inherent in the Bluetooth design, is the use of frequency hopping schemes. Frequency hopping schemes allow devices to communicate even in areas where there is a great deal of electromagnetic interference. Frequency hopping schemes also offer protection from burst errors by continually moving signals in and out of the interference band and by making bit error corrections using FEC. Frequency hopping schemes have been thought to protect authorized users from malicious users by transmitting the signal with a pseudo-random sequence that moves the signal arbitrarily around the bandwidth, making it very difficult to track the signal. However, this technique provides only minimal protection in reality and should not be relied upon solely.

A hardware solution for securing devices in the network (and indirectly providing more security for the Bluetooth network) is biometrics, and more specifically, voice authentication. Some devices that have Bluetooth applications, especially mobile phones and PDAs, already employ a form of voice authentication. Voice authentication can help organizations prevent malicious users from compromising remote Bluetooth devices and networks. The hosting devices of Bluetooth devices and networks should be secured in the same manner as PDAs, cell phones, and WLANs and devices. See the appropriate sections in this document for information on securing WLANs and devices, PDAs, and cell phones

It should be noted that Bluetooth is still a relatively new standard. Given that a number of vulnerabilities have been discovered, the standard is likely to continue to evolve such that the built-in hardware security mechanisms become even more robust. Many of the problems cannot be simply fixed by the user. The security problems, or possible security problems (security is not known fully), will exist until the Bluetooth SIG addresses them. Products that are released into the market now may exhibit some vulnerabilities. However by 2007, when Bluetooth is expected to be fully mature and be one of the most ubiquitous wireless technologies, the security will have improved to minimize the risks to its deployment. In addition, the security industry will mature to the point that particular security solutions to address Bluetooth inadequacies will also become more prevalent.

Some of the hardware solutions identified for 802.11b WLANs may be appropriate for Bluetooth devices as well. The reader is encouraged to review and consider the hardware solutions outlined in Section 3.

4.6 Emerging Security Standards and Technologies

Because Bluetooth-enabled devices are not yet widely available, the market has not developed robust security solutions. Trusted third party (TTP) authentication should be considered when it becomes available. TTP centralizes authentication, and as long as the TTP remains secure and trusted, the trustworthiness of the devices is not a concern. Centralized key management authority, which is similar to TTP authentication, is another possibility. Centralized key management, unlike TTP, maintains and distributes keys, so that only trusted devices have access to the secure keys.

Jini is an emerging technology that allows for instant recognition of new devices in a network. It can be viewed as the next step (after the Java programming language) toward making a network look like one large computer. Jini promises to make devices capable of attaching to a network independent of an operating system. Equipped with its own, special-purpose—and possibly microchip-embedded—operating system, the device could connect to a network and immediately be shared by devices with different operating systems (e.g., Windows™, Macintosh™, UNIX™). Mobile devices could easily connect to a network so that others could use the device.

In the Jini architecture, each new device that is added to the network immediately defines itself to the network device registry. Thus, when users plug in devices such as printers, storage devices, and speakers, every other computer, device, and user on the network immediately knows that a new device had been added and is now available. In the future, Jini may serve as a form of TTP, operating on a host device (e.g., a laptop computer or PDA) to authenticate devices on the network. Jini may also monitor device usage by tracking device authentication and network access.

As Bluetooth technology matures over the next few years, the built-in security features will mature and additional add-on solutions will appear in the market.

4.7 Bluetooth Security Checklist

Table 4-5 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, three columns are provided. The first column, the *Best Practice* column, if checked, means this is something recommended of all organizations. The second column, the *May 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 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 *May Consider* column is checked, organizations should carefully consider the option and weigh the costs versus the benefits. The last column, the *Done?* column, is intentionally left blank and allows an organization 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 4-5. Bluetooth Security Checklist

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Develop an organizational security policy that addresses the use of wireless technology including Bluetooth technology.	✓		
Ensure users on the network are fully trained in computer security awareness and the risks associated with wireless technology (i.e., Bluetooth).	✓		
Perform a risk assessment to understand the value of the assets in the organization that need protection.	✓		
Perform comprehensive security assessments at regular intervals to fully understand the wireless network security posture.	✓		

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Make sure the wireless "network" is fully understood. With piconets forming scatternets with possible connections to 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.	✓		
Ensure external boundary protection is in place around the perimeter of the building or buildings of the organization.	✓		
Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
Ensure that handheld / small Bluetooth devices are protected from theft.	✓		
Make sure that Bluetooth devices are turned off during all hours that they are not used.	✓		
Take a complete inventory of all Bluetooth-enabled wireless devices.	✓		
Study and understand all planned Bluetooth-enabled devices to understand any security idiosyncrasies or inadequacies.	✓		
Change the default settings of the Bluetooth device to reflect the organization's security policy.	✓		
Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.	✓		
Make sure the Bluetooth "bonding" environment is secure from eavesdroppers (i.e., the environment has been visually inspected for possible adversaries before the initialization procedures during which key exchanges occur).	✓		
Choose PIN codes that are sufficiently random and avoid all weak PINs.	✓		
Choose PIN codes that are sufficiently long (maximal length if possible).	✓		
Ensure that no Bluetooth device is defaulting to the zero PIN.	✓		
Configure Bluetooth devices to delete PINs after initialization (to ensure that PIN entry is required every time) and is not stored in memory after power removal.	✓		
Use an alternative protocol for the exchange of PIN codes (e.g., the Diffie-Hellman Key Exchange or Certificate-based key exchange methods at the application layer – Use of such processes simplifies the generation and distribution of longer PIN codes).		✓	
Ensure that combination keys are used instead of unit keys.	✓		
Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).	✓		
Make use of Security Mode 2 in controlled and well-understood environments.	✓		
Ensure device mutual authentication for all accesses.	✓		
Enable encryption for all broadcast transmissions (Encryption mode 3).	✓		
Configure encryption key sizes to the maximum allowable.	✓		
Establish a "minimum key size" for any key negotiation processes.	✓		
Ensure that portable devices with Bluetooth interfaces are configured with a password or PIN to prevent unauthorized access if lost or stolen.	✓		
Use application level (on top of the Bluetooth stack) encryption and authentication for highly sensitive data communication. For example, an IPsec-based Virtual Private Network (VPN) technology can be used for highly sensitive transactions.		✓	

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Use smart card technology in the Bluetooth network to provide key management.		✓	
Install antivirus software on intelligent, Bluetooth-enabled hosts.		✓	
Fully test and deploy software Bluetooth patches and upgrades on a regular basis.	✓		
Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.		✓	
Deploy intrusion detection sensors on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
Designate an individual to track the progress of Bluetooth security products and standards (Bluetooth SIG) and the threats and vulnerabilities with the technology.		✓	
Wait until future releases of Bluetooth technology incorporates fixes to the security features or offers enhanced security features.		✓	

4.8 Bluetooth Ad Hoc Network Risk and Security Summary

Table 4.6 lists areas of concern for Bluetooth devices, the security threats and vulnerabilities associated with those areas, and the risk mitigation for securing the device from these threats and vulnerabilities.

5

Table 4-6. Summary of Bluetooth Security

Area of Concern	Security Threat/Vulnerability	Risk Mitigation Solution
Device Physical Security	At risk from malicious users that "sniff" transmissions in an attempt to intercept data At risk from malicious jamming and interference from other devices that operate in the same band	Built-in frequency hopping technique prevents some disclosure. Maintain secure perimeter around devices in network. Require devices to operate at lowest power management level so that transmissions remain within the secure perimeter of the organization
Short PINs are used, PINs are stored in nonvolatile memory, and poor distribution exists.	PINs are guessed or compromised. Automatic connections are established	Use PINs that are as long as possible (e.g., 16 bytes). Ensure that PINs are not stored on Bluetooth devices but are deleted for sensitive applications. Develop a PIN distribution scheme or implement smart card approach.
Device Authentication Methods	Man-in-the-middle attacks Device authentication	Make sure authentication occurs on all transactions. Ensure mutual-authentication is enabled so that both devices in a transaction are verified. Do not share the unit key with untrusted sources. Implement password security software.
Encryption	Eavesdropping occurs on unprotected links The stream cipher may be weak and broken over time. Some encryption algorithms are more robust (e.g., 3DES and AES) than others (e.g., RC4 and DES); weaker algorithms can be easily cracked.	Make sure encryption is enabled on all transactions. Do not use Security Mode 1. Ensure that the Bluetooth device is configured to use broadcast encryption. Ensure that the key size is configured for maximal lengths – ensure that an acceptable "minimal key length" parameter is set. Use highest level of encryption possible for wireless communications. Applications-level encryption using public, well-known, more robust algorithms can be deployed.
Authorization	Bluetooth device connects and gains unauthorized access applications on another device	Implement Bluetooth Security Mode 2 with appropriate access policies established.

Area of Concern	Security Threat/Vulnerability	Risk Mitigation Solution
Security Patches/Upgrades	Vulnerability that may yet be discovered can be fixed through patches.	Monitor the release of Bluetooth security patches. Test and update security patches and upgrades in a timely manner to limit the likelihood that older versions of software are being used that may contain security vulnerabilities. Note: none of these are known to exist at this time.
Device Internet/E-mail Access	Viruses DoS attacks Data is vulnerable to third-party providers.	Incorporate and regularly update virus software. Implement software that monitors management messages that suggest DoS attacks. Use only a trusted third-party provider.
Poor design of built-in Bluetooth security (e.g., bad random number generator)	Adversary exploits a security feature that is not properly designed by the Bluetooth manufacturer. The result is compromised system security (e.g., unauthorized access to a device, unauthorized disclosure of information).	Fully understand the security of Bluetooth products that are deployed. Request manufacturers to provide full disclosure through white papers or provide third-party assessment reports. Do not purchase devices of which the security cannot be determined.
Uncertainties about the built-in security of the algorithms and procedures	Adversaries can defeat some of the mechanisms that are thought to be secure.	Monitor developments surrounding Bluetooth security. Seek guidance from security experts specializing in Bluetooth wireless communications.
Privacy violations	Adversaries can determine the person associated with a Bluetooth device and monitor activities.	Be vigilant about where a Bluetooth device is used. Note: Because of the public parameter address disclosure, not much can be done in this regard.

5. Wireless Handheld Devices

The scope of Section 5 is limited to text-messaging devices, PDAs, and smart phone-PDA products because these are the devices most commonly used by the mobile workforce in a business environment. This section describes the security threats and vulnerabilities associated with these devices and also recommends countermeasures that help mitigate the risks they introduce. Network administrators can, however, apply many of the security measures and recommendations discussed below to wireless handheld devices that are not covered in this section.

5.1 Wireless Handheld Device Overview

Wireless handheld devices range from simple one- and two-way text messaging devices to Internet-enabled PDAs, tablets, and smart phones. These devices are no longer viewed as coveted gadgets for early technology adopters but instead have become indispensable tools and competitive business advantages for the mobile workforce. The use of these devices introduces new security risks to an organization's existing network. Moreover, as these devices begin having their own IP address, the devices themselves can become the target of an attack. Handheld devices have different capabilities and different uses from desktop and laptop computers. The differences between handheld devices and desktop and laptop computers that affect the organization's security are summarized below.

- Their small size, relatively low cost, and constant mobility make them more likely to be stolen, misplaced, or lost.
- Physical security controls that protect desktop computers do not offer the same protection for handheld devices. Security guards are more likely to check the contents of a laptop carrying case or check the laptop itself for proper identification than they are likely to physically search people for handheld devices. A thief can more easily conceal a handheld device than a laptop or desktop computer.
- The devices themselves have limited computing power, memory, and peripherals that make existing desktop security countermeasures impractical for handheld devices. Limited processing power, for example, may render encryption with long key lengths too time-consuming.
- Synchronization software allows PCs to back up and mirror data stored on a handheld device and allows the handheld device to mirror data stored on desktop applications. The PC and the handheld device face different threats and require different security mechanisms to mitigate risk, but both must provide the same level of security to protect sensitive information.
- Members of an organization often purchase and use handheld devices without consulting with or notifying the organization's network administrator. Wireless handheld devices are often used for both personal and business data. Users that purchase these devices on their own often do not consider the security implications of their use in their work environment.
- Handheld devices offer multiple APs such as the user interface, expansion modules, wireless modems, Bluetooth, IR ports, and 802.11 connectivity. These access points present new risks that must be addressed separately from an existing wired network.
- Many users have limited security awareness or training with the use of handheld devices and are not familiar with the potential security risks introduced by these devices. Moreover, because new

models with new capabilities are being rapidly introduced to the market, there are few publications offering guidance, and many publications become quickly outdated.[52]

- Handheld device users can download a number of productivity, connectivity, games, and utilities freeware and shareware programs from untrusted sources. The programs can be easily installed without notifying network administrators. These programs may contain Trojan horses or other malware that can affect the user's handheld device, PC, or other network resources.
- There are few, if any, auditing capabilities or security tools available for many of these devices. In some cases, neither the user nor the administrator can audit security-relevant events related to the use of these devices. As networked PDAs become more affordable and more popular, however, vendors are beginning to offer more stand-alone and enterprise security solutions.
- Users often subscribe to third-party Wireless Internet Service Providers (WISPs) and access the Internet through wireless modems. Users can download or upload data to and from other computers without complying with the organization's firewall policy.
- There are several new handheld operating systems and applications that have not been thoroughly tested by the market to expose potential vulnerabilities.
- Handheld devices have a number of communication ports from which they can send and receive data, but limited capabilities in authenticating the devices with which they exchange data.

5.2 Benefits

One- and two-way text messaging systems have become popular for keeping in touch with colleagues and friends while traveling. They are light, inexpensive, easy to use, reliable, and text-messaging services are widely available. The pager was the first, commercially successful one-way text messaging system. Two-way text messaging systems which have become a popular way to send and receive e-mail, excel at providing a reliable and inexpensive way to communicate, but do not support any other office productivity applications. Many users prefer text-messaging to telephone calls because it allows for asynchronous communication, provides an electronic copy of the communication, costs less, requires no dial-up connection, fosters brevity, and allows users to communicate in public places without having their conversations overheard.

PDAs were first introduced to the market in the 1980s as handheld or palm-size computers that served as organizers for personal information and are gradually replacing the traditional leather-bound organizer. PDAs provide users with office productivity tools that allow users to access e-mail, their organization's network resources, and the Internet. These capabilities are quickly becoming a necessity in today's business environment. In addition, data that users have entered into their PDAs can be synchronized with a PC. Synchronization allows users to easily back up the information on their PDA and transfer data from the PC to the PDA. PDAs can also conveniently transfer data to other handheld devices by sending, or "beaming," the information through IR ports. The most common operating systems for PDAs are the Palm OS, PocketPC, Linux, and Symbian EPOC. This section provides general recommendations for network administrators that can be applied to all handheld devices using these or other operating systems. This section does not provide recommendations to device manufacturers on how to improve the security of the operating system of the device itself.

[52] Printed documents can become outdated quickly, especially documents that cover security in emerging technologies. Network administrators should periodically check vendor sites for product announcements and subscribe to security mailing lists for the most up-to-date information.

Although text-messaging devices and PDAs can help improve the efficiency of a mobile workforce, certain situations require a voice conversation between two or more parties to accurately and quickly convey certain information in the right context. As the emerging mobile and networked workforce began carrying laptops and fumbling with PDAs and cell phones at the same time, handheld device manufacturers began responding by introducing devices that combine a PDA and a cell phone on the same device. These devices are referred to as smart phones. Smart phones incorporate the capabilities of a typical PDA and a digital cellular telephone that provides voice service as well as e-mail, text messaging, web access, and voice recognition. Many smart phones are available that can run programming languages such as C or Java and offer telephony Application Programming Interfaces (API) that allow third-party developers to build new productivity tools to help the mobile workforce. Cell phone security has primarily focused on protecting carriers from fraudulent charges and users from eavesdropping. Typical cell phones use simplified operating systems that have no information processing capabilities and, therefore, present few information security risks. Smart phones, however, have more sophisticated operating systems capable of running applications and supporting networking with other computing devices. This section focuses on the security risks introduced by the information processing and networking capabilities of smart phones. This section does not address the underlying security of TDMA, CDMA, GSM, or GPRS protocols.

5.3 Security Requirements and Threats

Although handheld devices have not generally been viewed as posing security threats, their increased computing power and the ease with which they can access networks and exchange data with other handheld devices introduces new security risks to an organization's computing environment. As handheld devices begin supporting more networking capabilities, network administrators must carefully assess the risks they introduce into their existing computing environment. This section describes how the confidentiality, integrity, authenticity, and availability security requirements for handheld device computing environments can be threatened.

5.3.1 Loss of Confidentiality

Information stored on handheld devices and on handheld device storage modules and mirrored on a PC must remain confidential and be protected from unauthorized disclosure. The confidentiality of information can be compromised while on the handheld device, the storage module, the PC, or while being sent over one of the Bluetooth, 802.11, IR, USB, or serial communication ports.

PDAs can beam information from an IR port to another PDA IR port to easily exchange contact information such as telephone numbers and mailing addresses. This capability is a useful feature, but there may be some concerns about the data being transmitted. The data is unencrypted, and any user who is in close proximity to the handheld device and has the device pointed in the right direction can intercept and read the data. This is known as data leakage. Users familiar with PDA beaming should recognize that they often must have the PDA within a few inches of the other device and also make an effort to align the ports properly. The probability of data leakage occurring without the victim's knowledge is relatively low because it requires the intercepting device to be within a few feet and more often within a few inches. Nonetheless, organizations should not overlook the threat since it could result in a compromise of sensitive information. There is no documented attack of a malicious user being able to pull information out of an IR port because the IR beaming protocol can only issue a request to send information that must be approved by the device user before the information is sent. There is no equivalent request to receive information. A Bluetooth device that is not configured properly, however, is susceptible to having a user with a Bluetooth-enabled device pull data from his device. An 802.11-enabled device with an insecure P2P setting may also expose data to another 802.11-enabled device.

The ability of either the handheld device or the PC to initiate synchronization presents additional risks. A rogue compromised handheld device may attempt to synchronize with a PC, or alternatively, a compromised PC may try to synchronize with a PDA. This type of attack is often referred to as hijacking and relies on hijacking software that is available today.[53] A malicious user could obtain personal or organizational data, depending on what is stored on the PDA or PC. For this type of attack to be successful, either the PC or the handheld device has been compromised, or a malicious user has been able to create a rogue handheld device or PC and gain access to the user's network.

PDAs can also remotely synchronize with a networked PC using dial-up connections, dialing either directly to a corporate facility or through a WISP. The modems allow users to dial into an access server at their office or use a third-party WISP. Dial-up capability, however, also introduces risks. Dialing into a corporate facility requires a handheld device synchronization server; otherwise, the remote PDA must derive synchronization service by connecting to a PC that is logged on using the remote client's ID and password. If the PC is not at least configured with a password-protected screensaver, it is left vulnerable to anyone with physical access to the PC. Moreover, since the WISP is an untrusted network, establishing a remote connection requires additional security mechanisms to ensure a secure connection. The PDA would require a VPN client and a supporting corporate system to create a secure tunnel through the WISP to the organization. Modem-enabled PDAs are still relatively new, and an organization may not have the security services in place to support them. Organizations may want to restrict their use until they have either adapted their existing VPN capabilities or put the required services in place.

Another means for synchronizing data is through an Ethernet connection. Users can synchronize data from any networked workspace. The data that crosses the network is as secure as the network itself and maybe be susceptible to network traffic analyzers or sniffers. PDA users can also synchronize through their organization's wireless network. This entails accessing the organizations 802.11-compliant APs to connect to the organization's wired network. Many PDA vendors support or are beginning to support VPN connections using 802.11 APs.

Analog phones using 1G technologies are more susceptible to eavesdropping than are digital cell phones. Individuals or organizations can intercept unencrypted analog cell phone transmission using simple radio scanners. In contrast, digital phones have built-in security through spread spectrum technologies that use pseudo-random code sequences and forms of encryption. However, when digital phones are roaming (i.e., using other service providers), they frequently must connect to analog networks for coverage. When this connection occurs, the digital device becomes as vulnerable as the analog phone.

Smart phones can support wireless location services by using an on-board GPS integrated circuit or by having service providers analyze the cell phone signal received at cellular antenna sites.[54] GPS-enabled phones can identify the phone's location to within a few meters and also relay position information. Thus, in the case of emergency, a user who may be injured or threatened can relay his location to the proper authorities. These devices are subject to security threats associated with networked computing devices but also have a new set of privacy concerns as the user's location can be disclosed to third parties. Advertisers and other service providers would like to access user location information through agreements with the cellular telephone provider. Users should carefully read cellular phone companies' privacy policies and opt out of any unwanted wireless location services.

[53] See "A Whole New World for the 21st Century", March 2001 at www.sans.org.

[54] GPS is a Department of Defense (DoD) system of 24 satellites that provides positioning for a receiving unit through triangulation of three satellites' signals.

5.3.2 Loss of Integrity

The integrity of the information on the handheld device and the integrity of the handheld device hardware, applications, and underlying operating system are also security concerns. Information stored on, and software and hardware used by, the handheld device must be protected from unauthorized, unanticipated, or unintentional modification. Information integrity requires that a third party be able to verify that the content of a message has not been changed in transit and that the origin or the receipt of a specific message be verifiable by a third party. Moreover, users must be accountable and uniquely identifiable. The integrity of the information can be compromised while in transit or while stored on the handheld device or add-on storage modules. The integrity of the handheld hardware must be protected against the insertion or replacement of critical read-only memory (ROM) or other integrated circuits or upgradeable hardware. Handheld application must be ensured to protect against the installation of software from unauthorized sources that may contain malware. The integrity of add-on modules must be ensured to protect the handheld device from rogue hardware add-on modules.

5.3.3 Loss of Availability

The purpose of a DoS attack is to make computational or network resources unavailable or severely limit their availability by consuming their resources with an inordinate amount of service requests. DoS attacks are typically associated with networked devices with fixed IP addresses for attackers to target. Most handheld devices access the Internet intermittently and do not have fixed IP addresses, but as networking technologies become more widespread, "always-on" connectivity will be commonplace within the next few years. As a result, many handheld devices will be able to support the use of personal firewalls to protect themselves against certain DoS attacks.

Handheld devices can also be the targets of DoS attacks through other means. Trojan horses, worms, viruses and other malware can affect the availability of a network and, in many instances, also compromise the network's confidentiality and integrity.[55] A virus that, for example, sends documents from a user's PC to e-mail addresses found in the user's electronic address book can burden the network with a flood of e-mails, send out confidential information, and even alter the information sent, all while giving the appearance that it was intentionally sent from the user's account. Viruses have not been widely considered a security threat in PDAs because of the PDA's limited memory and processing power. Moreover, users typically synchronize their data with their PCs, and they can recover any lost or corrupted data simply by synchronizing with their PCs. Consequently, even a virus such as the Liberty Crack, which wipes out data on a PDA, has not been considered a serious threat.[56] PDA antivirus protection programs have only been on the market for a few years, and most PDAs do not have antivirus protection either because they do not support networking or the software simply has not been installed. A virus on a handheld device, however, could contain a payload designed to compromise a desktop PC, which in turn could directly affect the local network. As PDAs become more powerful, malicious users will develop viruses designed to achieve more harmful results. PDAs that share the same operating system as a PC may be particularly susceptible to a new strain of viruses. Although offering users additional benefits of sharing documents developed using the same applications, the common operating systems may invite new security threats. With both of the devices running the same applications, the methods for the virus to launch its attack and spread to other parts of the network increase.

Smart phones may lose network connectivity not only when they travel outside a cell coverage area but also from the use of cell phone jammers. Many restaurants and movie theaters, for example, now use commercially available jammers to block cell phone communications often without notifying the cell

[55] See SP 800-28, Guidelines on Active Content and Mobile Code, October 2001, for more information on malware.
[56] See "PDA/Wireless Communication Pains," November 17, 2000, at www.sans.org.

phone users. Users expecting important messages are not able to receive those messages because the jammers block them from accessing network resources. Malicious users may also use cell phone jamming devices. Jamming devices can carry out these attacks by broadcasting transmissions on cellular frequencies that null the actual cellular tower transmissions. The jammed cell phone will not be able to communicate unless other means of communications are available on the phone or in that region (e.g., the use of a dual-band cell phone that can operate at different frequencies and also operate on an analog signal).

Cell phones, smart phones, and text pagers are able to send text messages, from 110 to 160 characters in length depending on the carrier, to other cell phones by using Short Message Service (SMS). To send and receive SMS text messages, phone users usually have to pay a monthly fee to their service provider or a small fee for each text message beyond a preset monthly limit. Text messages can also be sent from a cellular service provider's web page or by visiting websites that allow users to send text messages free of charge. Text-messages rely on the service provider's network and are not encrypted, and there are no guarantees on quality of service. Cell phones and text-messaging devices can be spammed with text messages until their mailbox is full, and the user is no longer able to receive new text messages unless previously stored e-mails are deleted.

As 3G development progresses and 3G phones become more prevalent, organizations will need to be aware of the security issues that arise. One potential security issue is that a 3G mobile device, when connected to an IP network, is in the "always-on" mode. This mode alleviates the need for the device to authenticate itself each time a network request is made. However, the continuous connection also makes the device susceptible to attack. Moreover, because the device is always on, the opportunity exists to track users activities, and this may violate their privacy.

5.4 Risk Mitigation

As the use of handheld devices increases and technology improves, attacks can be expected to become more sophisticated. To control and even reduce the security risks identified above, organizations need to implement management, operational, and technical countermeasures to safeguard handheld devices and the organization's networks.

5.4.1 Management Countermeasures

Network administrators should conduct a risk assessment before handheld devices are introduced into the organization's computing environment. Network administrators should educate the organization's users about the proper use of their handheld devices and the security risks introduced by their use by providing short training courses or educational materials to help users use these devices more productively and more securely. Moreover, network administrators should establish and document security policies that address their use and the users' responsibilities.[57] The policy document should include the approved uses, the type of information that they may store, software programs they can install, how to store the devices and associated modules when not in use, proper password selection and use, how to report a lost or stolen PDA, and any disciplinary actions that may result from misuse. Organizations should also perform random audits to track whether devices have been lost or stolen.

5.4.2 Operational Countermeasures

Operational countermeasures require handheld device users to exercise due diligence in protecting the handheld devices and the networks they access from unnecessary risks. Most operational countermeasures

[57] See SP 800-30, Risk Management Guide for Information Technology Systems, January 2002, *URL:* http://csrc.nist.gov/publications/nistpubs/index.html.

are common sense procedures that require voluntary compliance by the users. Operational countermeasures are intended to minimize the risk associated with the use of handheld devices by well-intentioned users. Although a determined malicious user can find ways to intentionally disclose information to unauthorized sources, the handheld security policy and the organization's operational countermeasures should make clear the user's responsibilities.

The back of the PDA device should always be labeled with the owning organization's name, address, and phone number in case it is lost. Handheld device users should be provided with a secure area to store the device when not in use. A desk with drawers that lock or a file cabinet with locks are available in most offices and should provide sufficient physical security against theft from within the office environment. Galvanized steel cables and locks are also available to secure handheld devices to the user's desktop if other physical controls are not available.

Security administrators should have a list of authorized handheld device users, to enable them to perform periodic inventory checks and security audits. Individuals that use their handheld devices for other than business uses should comply with the organization's security policy or be restricted from accessing the organization's network. Handheld devices should be distributed to the users with security settings that comply with the organization's security policy and should not be distributed with "out-of-the-box" default settings. This entails establishing a configuration management policy. Such a policy frees security administrators from having to focus on many different configurations and allows them to concentrate on the configurations that have been adopted for the organization. Handheld devices should have a PIN code or password to access the device. Some handheld devices already use voice authentication for authenticating users to the device or to network resources. Voice authentication should be coupled with password authentication. A number of security tools are currently available to help mitigate the risks related to the use of PDAs, including password auditing, recovery/restoration, and vulnerability tools.[58]

Users should be encouraged to delete sensitive information on the handheld devices when no longer needed. This information can be archived on the PC during synchronization and transferred back to the PDA when needed. Users can disable IR ports during periods of nonuse to deter them from leaking information from their handheld devices. Users with access to sensitive information should have approval from their management and network security administrators before storing sensitive information on their handheld device to ensure they have the appropriate security countermeasures in place.

Some handheld devices allow users to mark certain records as "private" and hide them unless the device password is entered. Thus, if a malicious user gained access to an unattended device without knowledge of the device password, that malicious user would not be able to see the private data. Depending on the underlying operating system, however, some of these private data fields may be read directly from memory.

5.4.3 Technical Countermeasures

This section describes technical countermeasures for securing wireless handheld devices. Technical countermeasures should address the security risks identified during the risk assessment and should ensure that the organization's security policy is being enforced.

5.4.3.1 Authentication

Identification and authentication (I&A) is the process of recognizing and verifying valid users, processes, or devices. Handheld device users must be able to authenticate themselves to the handheld device by

[58] See "Research Tools" at http://www.atstake.com.

providing a password, a token, or both. At the most basic level, organizations should require PDAs to be password protected. Security administrators should educate users on the selection of strong passwords. Password cracking tools for handheld devices are available for network administrators and users to audit their PC's synchronization application password.[59] Password protection is already included with most handheld devices, but is usually not enabled in the default setting. Several websites offer software that prompts a user to enter a password when the user has turned the PDA off and turned it back on again.[60] Users should be prompted for a password when accessing the handheld device or the desktop PC synchronization software.

Biometric user authentication technologies are also available for handheld devices. Fingerprint readers can be attached to the handheld devices through a serial or USB port and can be set to lock the whole device, to lock an individual application, or to connect to a remote database over a network or dial-up connection. Tamper-proof smart cards, which contain unique user identifying information such as a private key, can also be used to authenticate the user to the device. Users insert the smart card into a peripheral slot on the device and provide a password to authenticate themselves. Malicious users must have possession of the smart card and knowledge of the user's password to gain access to the device.

Unique device identifiers, when available, can be used as part of an authorization mechanism to authenticate and provide network access to a handheld device. Handheld devices can take advantage of several methods to identify a unique handheld device, including flash ID, device ID, and Electronic Serial Number (ESN). Unique device identifiers can be used to authenticate the handheld device for network access or allow the handheld device itself to be used as a physical token for two-factor authentication.

Although it might be possible for an unauthorized user to copy the shape of a signature, many handwriting recognition programs measure aspects that are more difficult to copy, such as the rhythm and timing of the signature. The user can select a password to write instead of his signature, which is more widely available on paper documents distributed in the normal course of business. Organizations may also want to consider installing motion detection applications. These applications require users to complete a series of user-defined physical motions before they are given access to the device.

5.4.3.2 Encryption

Some files on the device may require a higher level of security than password protection can offer. For example, user passwords are required to access all sorts of automated services in our everyday lives. During the course of a single day, a user may need to use a password to withdraw money from an automatic teller machine (ATM), to enter a building by typing an access code, to listen to voice mail, to browse favorite websites or purchase goods online, to access online trading accounts, to make a phone call using a calling card, and to access personal and business e-mail accounts. Using the same password to access different services is discouraged because if this single password were compromised, an unauthorized user would be able to access all of the user's accounts. Many PDA users, however, store many of these passwords in a file on the PDA, possibly even naming the file "mypasswords." Identifying other user accounts once a single password has been obtained can be accomplished through a variety of means ranging from dumpster diving to simply reviewing a user's web browser history file. Encryption software can be used to protect the confidentiality of sensitive information stored on handheld devices and mirrored on the desktop PC. The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. This additional level of security can be added to provide an extra layer of defense to further protect sensitive information stored on handheld devices.

---

[59] See http://www.atstake.com/research/tools/index.html for PDA security assessment tools.

[60] The following websites offer PDA software tools: www.pdacentral.com; www.tucows.com; www.download.com. Vendors, for example Palm (www.palm.com/software) and Microsoft (www.microsoft.com/mobile/pocketpc/downloads/default.asp), also offer software tools for their specific products.

Many software programs are freely available to help users encrypt these types of files. Encrypting the file protects the file from brute-force password guessing if the file falls into the wrong hands. Handheld device users may elect to encrypt files and messages before the files and messages are transferred through a wireless port.

Smart phones use digital technologies to deter unencrypted voice traffic from being intercepted. FEC coding and spread-spectrum techniques add more secure and robust encryption to a link. Organizations should upgrade their analog phones to digital smart phones that offer more capabilities at the application level (e.g., web browsing, networking) and the ability to use more security mechanisms with those applications.

5.4.3.3 Antivirus Software

Antivirus software is another important security measure for handheld devices.[61] All organizations, regardless of their security requirements, should incorporate PDA antivirus applications to scan e-mail and data files and to remove malware from files upon transmission to the device. The software should scan all entry ports (i.e., beaming, synchronizing, e-mail, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files. The organization should further require regular updates to the antivirus software and require associated workstations (i.e., the PCs with which users synchronize their PDAs) to have updated, properly working virus-scanning software. Most major PC antivirus software vendors have handheld device antivirus software that can be downloaded directly from their websites.

5.4.3.4 PKI

Many handheld devices are beginning to offer support for PKI technologies. PKI is one of the best available methods for meeting confidentiality, integrity, and authenticity security requirements.[62] A PKI uses an asymmetric encryption method, commonly known as the "public/private key" method, for encrypting and ensuring the integrity of documents and messages. A certificate authority issues digital certificates that authenticate the identity of people and organizations over a public network such as the Internet. The PKI also establishes the encryption algorithms, levels of security, and the key distribution policy for users. PKI support is often integrated into common applications such as web browsers and e-mail programs by validating certificates and signed messages. The PKI can also be implemented by an organization for its own use to authenticate users that handle sensitive information. The use of PKI counters many threats associated with public networks but also introduces management overhead and additional hardware and software costs that should be evaluated while performing the risk assessment and selecting the appropriate countermeasures to meet the organization's security requirements.

5.4.3.5 VPN and Firewalls

Organizations in a wide variety of industries are using handheld devices for remote access to patient records, merchandise inventory, and shipping logistics. Secure remote access for desktop and laptop computers has been successfully enabled by the use of firewalls and VPN over the last few years.[63] Handheld devices are beginning to offer support for personal firewalls and VPN technologies and offer network administrators effective countermeasures against threats to the confidentiality, integrity, and authenticity of the information being transferred. A packet filter firewall, for example, screens Internet

[61] See http://csrc.nist.gov/virus/ for useful links for more information on viruses.

[62] See SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.URL: http://csrc.nist.gov/publications/nistpubs/index.html.

[63] See Special Publication 800-46, Security for Telecommuting and Broadband Communications, URL: http://csrc.nist.gov/publications/nistpubs/index.html.

traffic based on packet header information such as the type of application (e-mail, ftp, web, etc.) and by the service port number. A VPN creates a virtual private network between the handheld device and the organization's network by sharing the public network infrastructure. VPN technology offers the security of a private network through access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks. Network administrators should look for the following features when purchasing VPN technologies: interoperability with existing infrastructure, support for a wireless and dial-up networking, packet-filtering or stateful-inspection firewall, automatic security updates, and a centralized management console.

5.4.3.6 Enterprise Solutions

Enterprise handheld device management software allows network administrators to discover handheld devices, install and remove applications, back up and restore data, collect inventory information, synchronize data with corporate servers and databases, and perform various configuration management functions from a central location.

5.4.3.7 Miscellaneous

Third-party developers have introduced a number of security tools to help protect handheld devices. These security tools are fairly inexpensive and typically offer simple yet practical security countermeasures to protect against malicious users that are more likely to steal the device than to crack an encrypted file or eavesdrop on their wireless communications. Some of these security tools delete applications and their data after a preset number of unsuccessful login attempts. Authorized users simply have to resynchronize the PDA with their PCs to recover the deleted information. This countermeasure is particularly effective and applicable in instances where PDAs are holding sensitive information. Users must be cautioned that all data entered on the PDA since the last synchronization will be lost. A malicious user could purposely enter several incorrect passwords to delete the data on an unattended handheld device, but this risk can be mitigated by frequent synchronization with the user's PC. Another simple security tool is to add an application that auto-locks the PDA after it is idle for a selected period of time. This solution mitigates risks that arise when users leave PDAs unattended. Users simply enter a password to regain access to the PDA. This solution is similar to a screen saver password for a desktop PC.

5.5 Case Study: PDAs in the Workplace

Organization C is considering purchasing PDAs for its sales force of 150 employees. Before making a decision to purchase the PDAs, the computer security department performs a risk assessment. A canvas of user attitudes reveals that most of the organization's users do not appreciate the implications of losing a PDA and the loss of sensitive organizational data. The network administrators test the devices and set up a one-hour training course for the employees that will be using the PDAs. During the training course, the users are given the security policy and documentation explaining the security risks associated with the devices. The security team also recommends instituting security policies that address the appropriate uses of PDAs, the use of random inventory and security audits, and the users' responsibilities and liabilities. The security policy specifies the type of information users can store on the PDA, proper handling of PDAs, password requirements (e.g., frequency of change, minimum character length), procedures for reporting a lost or stolen PDA, and any disciplinary actions that may result from misuse.

The security department completes its risk assessment and cautions that even though it has done a thorough analysis of the PDAs, there are still risks given the fast pace with which PDAs are evolving and the likelihood that malicious users will try to exploit any new or existing vulnerability. Organization C determines that the operational benefits outweigh the residual risks of the PDAs and moves forward with the purchase.

Organization C considers the protection of sales-leads information paramount. Encryption software is used to encrypt database files stored on the PC and the PDA. Users are encouraged to synchronize their handheld devices every other day; consequently, Organization C does not purchase backup storage modules. The security department realizes that IR beaming has important benefits and decides not to prohibit IR beaming completely. However, it does recommend that users keep IR ports closed during periods of nonuse. The sales force also needs to update the corporate sales tracking database, view inventory information, and access corporate e-mail. It is decided that access to corporate resources will be through a VPN.

Before issuing the PDAs to its sales force, the department ensures that the default settings of the Bluetooth cards are changed to comply with the organization's security policy. The security team upgrades its existing antivirus software to allow it to screen data being transferred to the PC during synchronization. The security team also installs software that automatically prompts the users to enter a password to access the device after 15 minutes of inactivity on all the PDAs. The security team labels the devices and issues the devices to users with the proper security settings. The security team performs regular audits and follows vendor sites and security mailing lists for security news about handheld devices and applications.

5.6 PDA and Smart Phone Checklist

Table 5-1 provides a security checklist for PDAs and Smart PhonesThe table presents guidelines and recommendations for creating and maintaining a secure environment that uses these handheld devices. For each recommendation or guideline, three columns are provided. The first column, the *Best Practice* column, if checked, means this is something recommended of all organizations. The second column, the *May 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, because the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational or cost impacts. In summary, if the *May Consider* column is checked, organizations need to carefully consider the option and weigh the costs versus the benefits. The last column, the *Done?* column, is intentionally left blank and allows an organization to use this table as a true checklist. For instance, an individual performing a handheld device security audit can quickly check off each recommendation for the organization wireless environment – asking, "Have I done this?"

Table 5-1. Wireless Handheld Device Security Checklist

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Develop an organizational security policy that addresses the use of all handheld devices.	✓		
Ensure users on the network are fully trained in computer security awareness and the risks associated with handheld devices.	✓		
Perform a risk assessment to understand the value of the assets in the organization that need protection.	✓		
Conduct ongoing, random security audits to monitor and track devices.	✓		
Ensure external boundary protection is in place around the perimeter of the building or buildings of the organization.	✓		
Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		

Security Recommendation	Checklist		
	Best Practice	May Consider	Done ?
Minimize the risk of loss or theft through the use of physical locks and cables.	✓		
Label all handheld devices with the owner and organization's information.	✓		
Ensure that users know where to report a lost or stolen device.	✓		
Ensure that devices are stored securely when left unattended.	✓		
Make sure that add-on modules are adequately protected when not in use.	✓		
Enable a “power-on” password for each handheld device.	✓		
Ensure proper password management (aging, complexity criteria, etc.) for all handheld devices.	✓		
Ensure that desktop application mirroring software is password protected.	✓		
Store data on backup storage modules in encrypted form.		✓	
Review vendor websites frequently for new patches and software releases.	✓		
Install patches on the affected devices and workstations.	✓		
Review security-related mailing lists for the latest security information and alerts.	✓		
Ensure that all devices have timeout mechanisms that automatically prompt the user for a password after a period of inactivity.	✓		
Synchronize devices with its corresponding PC regularly.	✓		
Delete sensitive data from the handheld device and archive it on the PC when no longer needed on the handheld.	✓		
Turn off IR ports during periods of inactivity.	✓		
Install antivirus software on all handheld devices.		✓	
Install personal firewall software on all handheld devices.		✓	
Ensure that PDAs are provided with secure authorization software/firmware.		✓	
Make sure that a user can be securely authenticated when operating locally and remotely.	✓		
Use robust encryption and password protection utilities for the protection of sensitive data files and applications.		✓	
Use enterprise security applications to manage handheld device security.		✓	
Ensure security assessment tools are used on handheld devices.		✓	

5.7 Handheld Device Risk and Security Summary

Table 5.2 lists areas of concern for handheld devices, the security threats and vulnerabilities associated with those areas, and the risk mitigation for securing the device from these threats and vulnerabilities.

5

Table 5-2. Handheld Device Security Summary

Area of Concern	Security Threats/Vulnerabilities	Risk Mitigation Solution
Physical Security	Handheld device may be lost or stolen, giving the opportunity to an unauthorized user to attempt to access the contents of the handheld device and possibly the services the device can access	Label devices with name, telephone number, and postal address. Perform random audits to monitor usage and track devices. Install software that automatically deletes all data after a preset number of failed login attempts. Securely store handheld devices and backup modules. Delete sensitive data on handheld device when no longer needed and archive on PC.
User Authentication	Unauthorized user gains access to the handheld device contents	Use strong passwords, biometrics, or smart cards.
Device Authentication	An unauthorized user may access network resources or services	Use hardware authentication tokens. Employ server-side authentication, PKI and VPN.
Integrity	Viruses Installation of unauthorized software containing malware Rogue modules Installation of ROM modules	Incorporate and regularly update anti-virus software on PC and handheld device. Perform random audits Install software and hardware only from authorized sources. Use handheld device enterprise management software to monitor device use, applications installed, and hardware configurations.
Confidentiality	Open IR ports can lead to data leakage Data transmitted is often unencrypted and thus can lead to data compromise Default settings allow unauthorized users to gain access to the device Data stored on backup storage modules may be accessed by unauthorized users Data mirrored on PC may be accessed by unauthorized users Remote synchronization from unauthorized PC Eavesdropping on data exchanged between handheld device and network Data is vulnerable to the link between third-party server and network	Require IR ports to be closed when not in use to deter any leaking of information. Encrypt all information leaving the device for an adequate level of protection. Encrypt important data files stored on the device for greater security. Change default settings to reflect the organization's security policy. Encrypt data on storage modules and store in a secure place. Password protect handheld device mirroring software on PC. Password protect handheld device synchronization. Use PKI and VPN.

Area of Concern	Security Threats/Vulnerabilities	Risk Mitigation Solution
Availability	DoS attacks Signal jamming Viruses	Use personal firewalls. Use antivirus software.

Appendix A—Common Wireless Frequencies and Applications

EM Band Designation	Frequency Range	Wireless Device/Application
VLF: Very Low Frequency	9 kHz–30 kHz	
LF: Low Frequency	30 kHz–300 kHz	
MF: Medium Frequency	300 kHz–3 MHz	AM radio stations (535 kHz–1 MHz)
HF: High Frequency	3 MHz – 30 MHz	
VHF: Very High Frequency	30 MHz–300 MHz	FM radio stations VHF television stations 7–13, NTSC Standard (174MHz – 220 MHz) Garage door openers (~40 MHz) Standard cordless telephones (40MHz–50 MHz) Alarm Systems (~40 MHz) Paging Systems (50Mhz–300 MHz)
UHF: Ultra High Frequency	300 MHz–3 GHz	Paging systems (300MHz–500 MHz) 1G Mobile telephones (824MHz–829 MHz) 2G Mobile telephone (800MHz–900 MHz) Global System for Mobile Communication (GSM) Enhanced Data Rates for Global Evolution (EDGE) (800/900/1800/1900 MHz bands) 3G Mobile telephones (international standard) (1,755 MHz– 2200 MHz) Bluetooth devices (2.4 GHz) HomeRF (2.4 GHz) WLAN (2.4 GHz)
SHF: Super High Frequency	3 GHz–30 GHz	Applications in the short range, point-to-point communications including remote control systems, PDAs, etc WLAN (5.8 GHz). Local Multipoint Distribution Services (LMDS), a fixed wireless technology that operates in the 28 GHz band and offers line-of-sight coverage over distances up to 3-5 kilometers.
EHF: Extremely High Frequency	30 GHz–300 GHz	Satellite Communications
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

Data Encryption Standard (DES)	A National Institute of Standards and Technology (NIST) standard secret key cryptography method that uses a 56-bit key encryption. DES is based on an IBM algorithm, which was further developed by the U.S. National Security Agency. It uses the block cipher method, which breaks the text into 64-bit blocks before encrypting them. There are several DES encryption modes. The most popular mode exclusive ORs each plaintext block with the previous encrypted block. DES decryption is very fast and widely used. The secret key may be kept completely secret and reused again, or a key can be randomly generated for each session, in which case, the new key is transmitted to the recipient using a public key cryptography method such as RSA. Triple DES (3DES) is an enhancement of DES that provides considerably more security than standard DES, which uses only one 56-bit key. There are several 3DES methods. EEE3 uses three keys and encrypts three times. EDE3 uses three keys to encrypt, decrypt, and encrypt again. EEE2 and EDE2 are similar to EEE3 and EDE3, except that only two keys are used, and the first and third operations use the same key.
Dynamic Host Control Protocol (DHCP)	The protocol used to assign Internet Protocol (IP) addresses to all nodes on the network.
Hash Function	A computationally efficient algorithm that maps a variable-sized amount of text into a fixed-sized output (hash value). Hash functions are used in creating digital signatures.
Industrial, Scientific, and Medical (ISM) Band	The ISM band refers to the government-allotted bandwidth at 2.450 ± .050 gigahertz (GHz) and 5.8 ± 0.75 GHz.
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.
Institute of Electrical and Electronics Engineers (IEEE)	A worldwide professional association for electrical and electronics engineers that sets standards for telecommunications and computing applications.
International Electrotechnical Commission (IEC)	An organization that sets international standards for the electrical and electronics fields.
International Organization for Standardization (ISO)	A voluntary organization responsible for creating international standards in many areas, including computers and communications.

Jini	An approach to instant recognition that would enable manufacturers to make devices that can attach to a network independently of an operating system. Jini can be viewed as the next step after the Java programming language toward making a network look like one large computer. Each pluggable device in a network will define itself immediately to a network device registry. Using the Jini architecture, users will be able to plug printers, storage devices, speakers, and any other kind of device directly into a network, and every other computer, device, and user on the network will know that the new device has been added and is available through the network registry. When a user wants to use or access the resource, their computer will be able to download the necessary programming from it to communicate with it. In this way, devices on the network may be able to access and use other devices without having the drivers or other previous knowledge of the device.
Local Area Network (LAN)	A network that connects computers in close proximity via cable, usually in the same building.
Medium Access Control (MAC)	On a local area network, the sublayers that control which device has access to the transmission medium at a particular time.
Open Systems Interconnection (OSI)	A model developed by ISO to allow computer systems made by different vendors to communicate with each other.
Personal Digital Assistant (PDA)	A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data is synchronized between a user's PDA and desktop computer by cable or wireless transmission.
Request for Comments (RFC)	A series of numbered documents (RFC 822, RFC 1123, etc.), developed by the Internet Engineering Task Force (IETF) that set standards and are voluntarily followed by many makers of software in the Internet community.
Smart Card	A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.
Spoofing	IP spoofing refers to sending a network packet that appears to come from a source other than its actual source.
Virtual Private Network (VPN)	A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

Wireless Application Protocol (WAP)	A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based web pages. Introduced in 1997 by Phone.com, Ericsson, Motorola, and Nokia, WAP provides a complete environment for wireless applications that includes a wireless counterpart of TCP/IP and a framework for telephony integration, such as call control and telephone book access. WAP features the Wireless Markup Language (WML), which was derived from Phone.com's HDML and is a streamlined version of HTML for small-screen displays. It also uses WMLScript, a compact JavaScript-like language that runs in limited memory. WAP also supports handheld input methods, such as a keypad and voice recognition. Independent of the air interface, WAP runs over all the major wireless networks in place now and in the future. It is also device-independent, requiring only a minimum functionality in the unit to permit use with a myriad of telephones and handheld devices.

Appendix C—Acronyms and Abbreviations

1G	First Generation
2G	Second Generation
2.5G	Two-and-a-Half Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
ACL	Access Control List
ACO	Authenticated Cipher Offset
AES	Advanced Encryption Standard
AH	Authentication Header
AMPS	Advanced Mobile Phone System
AP	Access Point
API	Application Programming Interfaces
ATM	Automatic Teller Machine
BSS	Basic Service Set
CDMA	Code Division Multiple Access
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
DoD	Department of Defense
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EDGE	Enhanced Data GSM Environment
EM	Electromagnetic
ESN	Electronic Serial Number
ESP	Encapsulating Security Protocol
ESS	Extended Service Set
ETSI	European Telecommunications Standard Institute
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
GFSK	Gaussian Frequency Shift Keying
GHz	Gigahertz
GPRS	General Packet Radio System

GPS	Global Positioning System
GSM	Global System for Mobile
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
I & A	Identification and Authentication
IBSS	Interdependent Basic Service Set
ICAT	Internet Categorization of Attack Toolkit
IDC	International Data Corporation
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMT-2000	International Mobile Telecommunication 2000
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	Internet Packet Exchange
IR	Infrared
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
ISS	Internet Security Systems
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
LDAP	Lightweight Directory Access Protocol
LFSR	Linear Feedback Shift Register
MAC	Medium Access Control
Mbps	Megabits per second
MHz	Megahertz
mW	Milliwatt
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
OTP	One-Time Password
P2P	Peer to Peer

PAN	Personal Area Network
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PHY	Physical Layer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-in User Service
RF	Radio Frequency
RFC	Request for Comment
ROM	Read Only Memory
RSA	Rivest-Shamir-Adelman
SIG	Special Interest Group
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRES	Signed Response
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TGI	Task Group I
TKIP	Temporal Key Integrity Protocol
TLS	Transport-Level Security
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications Service
USB	Universal Serial Bus
USC	United States Code
UWC	Universal Wireless Communications
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WEP2	Wired Equivalent Privacy 2
WG-1000	Wireless Gateway 1000
WI-FI	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WML	Wireless Markup Language
WTA	Wireless Telephony Application
WTP	Wireless Transaction Protocol

Appendix D—References

Print Publications

Books

1. NIST Special Publication 46, *Security for Telecommuting and Broadband Communications*, National Institute for Standards and Technology

2. Norton, P. and Stockman, M. *Peter Norton's Network Security Fundamentals*. 2000.

3. Wack, J., Cutler, K., and Pole, J. *NIST Special Publication 41, Guidlines on Firewalls and Firewall Policy*January 2002.

Articles and Other Published Material

1. 3Com. *11 Mbps Wireless LAN Access Point 6000 User Guide*. Version 2.0. May 2001.

4. Arbaugh, W.A., Shankar, N., and Wan, Y.C., "Your 802.11 Wireless Network Has No Clothes." March 30, 2001.

5. Basgall, M. "Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security." http://www.dukenews.duke.edu/research/encrypt.html, (January 1999)

6. Cam-Winget, N., and Walker, J. "An Analysis of AES in OCB Mode." May 2001.

7. Ismadi, A., and Sukaimi, Y.B. *Smart Card: An Alternative to Password Authentication*. SANS, May 26, 2001.

8. Lucent Technologies. *ORINOCO Manager Suite Users Guide*. November 2000.

9. Menezes, A. "Comparing the Security of ECC and RSA." January 2000.

10. Cagliostro, C. *Security and Smart Cards*. www.scia.org, 2001.

11. Cardwell, A., and Woollard, S. "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?" www.itsecurity.com, 2001.

12. Ewalt, D. M. "RSA Patches Hold in Wireless LANs: The fix addresses problems with the Wireless Equivalent Privacy protocol, which encrypts communication over 802.11b wireless networks." *InformationWeek* (www.informationweek.com), December 2001.

13. Leyden, J. "Tool Dumbs Down Wireless Hacking." *The Register* (www.theregister.co.uk), August 2001.

14. Marek, S. "Identifying the Weakest Link." *Wireless Internet Magazine* (www.wirelessinternetmag.com), November/December 2001.

15. Rysavy, P. "Break Free With Wireless LANs." *Network Computing, Mobile and Wireless Technology Feature*, October 29, 2001.

General Internet Resources

1. http://csrc.nist.gov/publications (NIST, Computer Security Resource Center)
2. http://its.med.yale.edu/computing_services.html (Yale University School of Medicine–provides information on wireless applications and future uses
3. http://xforce.iss.net (X-Force website–provides information on leading computer threats and vulnerabilities)
4. www.cisco.com (Cisco website–provides information on securing wireless networks)
5. www.computeruser.com/resources/dictionary/dictionary.html (reference for technical terms)
6. www.computerworld.com (provides white papers, surveys, and reports related to security of wireless networks)
7. www.eet.com (technical website that serves as a primer for different technologies and applications)
8. www.gcn.com (*Government Computer News*–provides up-to-date information on wireless and mobile devices and their related security issues)
9. www.informationweek.com (provides information on wireless networks, wireless communications, and security solutions in the form of articles and other documents)
10. www.infosecuritymagazine.com (provides white papers, surveys, and reports on wireless network security)
11. www.isaac.cs.berkeley.edu/isaac/wep-faq.html (University of California at Berkeley–provides "frequently asked questions" on WEP setup, problems, and attacks)
12. www.networkcomputing.com (provides white papers, surveys, and reports on wireless network security)
13. www.nwfusion.com (Network World Fusion website–provides white papers, surveys, and reports on wireless network security)
14. www.pdadefense.com (PDADefense website–provides articles and guidance on PDA security)
15. www.sans.org/newlook/home.htm (SANS Institute website–maintains articles, documents, and links on computer security and wireless technologies)
16. www.scmagazine.com (*SC Magazine* website, an information security online magazine –provides information on wireless security issues)
17. www.zdnetindia.com (*ZDNet India Magazine* website–provides white papers, surveys, and reports on wireless network security)