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

Special Publication 800-48

Wireless Network Security

802.11, Bluetooth and Handheld Devices

Tom Karygiannis
Les Owens

NIST Special Publication 800-48

Wireless Network Security

802.11, Bluetooth and Handheld Devices

Recommendations of the National Institute of Standards and Technology

Tom Karygiannis and Les Owens

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

November 2002

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

Acknowledgments

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

Table of Contents

Executive Summary **1**

1. Introduction **1-1**

1.1 Authority 1-1
1.2 Document Purpose and Scope 1-1
1.3 Audience and Assumptions 1-2
1.4 Document Organization 1-2

2. Overview of Wireless Technology **2-1**

2.1 Wireless Networks 2-1
2.1.1 Wireless LANs 2-1
2.1.2 Ad Hoc Networks 2-1
2.2 Wireless Devices 2-2
2.2.1 Personal Digital Assistants 2-2
2.2.2 Smart Phones 2-3
2.3 Wireless Standards 2-3
2.3.1 IEEE 802.11 2-3
2.3.2 Bluetooth 2-3
2.4 Wireless Security Threats and Risk Mitigation 2-4
2.5 Emerging Wireless Technologies 2-6
2.6 Federal Information Processing Standards 2-6

3. Wireless LANs **3-8**

3.1 Wireless LAN Overview 3-8
3.1.1 Brief History 3-8
3.1.2 Frequency and Data Rates 3-9
3.1.3 802.11 Architecture 3-9
3.1.4 Wireless LAN Components 3-11
3.1.5 Range 3-11
3.2 Benefits 3-12
3.3 Security of 802.11 Wireless LANs 3-13
3.3.1 Security Features of 802.11 Wireless LANs per the Standard 3-13
3.3.2 Problems With the IEEE 802.11 Standard Security 3-17
3.4 Security Requirements and Threats 3-19
3.4.1 Loss of Confidentiality 3-20
3.4.2 Loss of Integrity 3-21
3.4.3 Loss of Network Availability 3-22
3.4.4 Other Security Risks 3-22
3.5 Risk Mitigation 3-22
3.5.1 Management Countermeasures 3-23
3.5.2 Operational Countermeasures 3-23
3.5.3 Technical Countermeasures 3-24
3.6 Emerging Security Standards and Technologies 3-36
3.7 Case Study: Implementing a Wireless LAN in the Work Environment 3-37
3.8 Wireless LAN Security Checklist 3-40
3.9 Wireless LAN Risk and Security Summary 3-42

4. Wireless Personal Area Networks **4-1**

4.1 Bluetooth Overview 4-1
4.1.1 Brief History 4-3
4.1.2 Frequency and Data Rates 4-3
4.1.3 Bluetooth Architecture and Components 4-4
4.1.4 Range 4-4
4.2 Benefits 4-5
4.3 Security of Bluetooth 4-6
4.3.1 Security Features of Bluetooth per the Specifications 4-7
4.3.2 Problems with the Bluetooth Standard Security 4-13
4.4 Security Requirements and Threats 4-14
4.4.1 Loss of Confidentiality 4-14
4.4.2 Loss of Integrity 4-17
4.4.3 Loss of Availability 4-17
4.5 Risk Mitigation 4-17
4.5.1 Management Countermeasures 4-17
4.5.2 Operational Countermeasures 4-18
4.5.3 Technical Countermeasures 4-18
4.6 Bluetooth Security Checklist 4-20
4.7 Bluetooth Ad Hoc Network Risk and Security Summary 4-22

5. Wireless Handheld Devices 5-26

5.1 Wireless Handheld Device Overview 5-26
5.2 Benefits 5-27
5.3 Security Requirements and Threats 5-28
5.3.1 Loss of Confidentiality 5-28
5.3.2 Loss of Integrity 5-30
5.3.3 Loss of Availability 5-30
5.4 Risk Mitigation 5-31
5.4.1 Management Countermeasures 5-31
5.4.2 Operational Countermeasures 5-32
5.4.3 Technical Countermeasures 5-33
5.5 Case Study: PDAs in the Workplace 5-36
5.6 Wireless Handheld Device Security Checklist 5-36
5.7 Handheld Device Risk and Security Summary 5-38

Appendix A— Common Wireless Frequencies and Applications A-1

Appendix B— Glossary of Terms B-1

Appendix C— Acronyms and Abbreviations C-1

Appendix D— Summary of 802.11 Standards D-1

Appendix E— Useful References E-1

Appendix F— Wireless Networking Tools F-1

Appendix G— References G-1

List of Figures

Figure 2-1. Notional Ad Hoc Network 2-2
Figure 3-1. Fundamental 802.11b Wireless LAN Topology 3-10
Figure 3-2. 802.11b Wireless LAN Ad Hoc Topology 3-10
Figure 3-3. Typical Range of 802.11 WLAN 3-11
Figure 3-4. Access Point Bridging 3-12
Figure 3-5. Wireless Security of 802.11b in Typical Network 3-13
Figure 3-6. Taxonomy of 802.11 Authentication Techniques 3-14
Figure 3-7. Shared-key Authentication Message Flow 3-15
Figure 3-8. WEP Privacy Using RC4 Algorithm 3-16
Figure 3-9. Taxonomy of Security Attacks 3-19
Figure 3-10. Typical Use of VPN for Secure Internet Communications From Site-to-Site 3-33
Figure 3-11. VPN Security in Addition to WEP 3-34
Figure 3-12. Simplified Diagram of VPN WLAN 3-35
Figure 3-13. Agency A WLAN Architecture 3-39
Figure 4-1. Typical Bluetooth Network—A Scatter-net 4-2
Figure 4-2. Bluetooth Ad Hoc Topology 4-4
Figure 4-3. Bluetooth Operating Range 4-5
Figure 4-4. Bluetooth Air-Interface Security 4-6
Figure 4-5. Taxonomy of Bluetooth Security Modes 4-8
Figure 4-6. Bluetooth Key Generation from PIN 4-9
Figure 4-7. Bluetooth Authentication 4-10
Figure 4-8. Bluetooth Encryption Procedure 4-12
Figure 4-9. Man-in-the-Middle Attack Scenarios 4-16

List of Tables

Table 3-1. Key Characteristics of 802.11 Wireless LANs 3-8
Table 3-2. Key Problems with Existing 802.11 Wireless LAN Security 3-18
Table 3-3. Wireless LAN Security Checklist 3-40
Table 3-4. Wireless LAN Security Summary 3-43
Table 4-1. Key Characteristics of Bluetooth Technology 4-2
Table 4-2. Device Classes of Power Management 4-5
Table 4-3. Summary of Authentication Parameters 4-11
Table 4-4. Key Problems with Existing (Native) Bluetooth Security 4-13
Table 4-5. Bluetooth Security Checklist 4-21
Table 4-6. Bluetooth Security Summary 4-23
Table 5-1. Wireless Handheld Device Security Checklist 5-37
Table 5-2. Handheld Device Security Summary 5-38
Table D-1. Summary of 802.11 Standards D-1

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 offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

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

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

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 agency's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- 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 movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- 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 subsequently be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use third-party, untrusted wireless network services to gain access to an agency's or other organization's network resources.
- Internal attacks may be possible via ad hoc transmissions.

This document provides an overview of wireless networking technologies and wireless handheld devices most commonly used in an office environment and with today's mobile workforce. This document seeks to assist agencies in reducing the risks associated with 802.11 wireless local area networks (LAN), Bluetooth wireless networks, and handheld devices.

The National Institute of Standards and Technology (NIST) recommends the following actions:

Agencies should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Moreover, it is important that agencies assess risks more frequently 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 backups of data frequently.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards that enhance security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

Agencies should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

As described in this document, the risks related to the use of wireless technologies are considerable. Many current communications protocols and commercial products provide inadequate protection and thus present unacceptable risks to agency operations. Agencies must actively address such risks to protect their ability to support essential operations, before deployment of wireless technologies. Furthermore, many organizations poorly administer their wireless technologies. Some examples include deploying equipment with "factory default" settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or employing a security architecture suitable to the wireless environment (e.g., one with firewalls between wired and wireless systems, blocking of unneeded services/ports, use of strong cryptography). 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 toward more robust, open, and secure solutions for the near future. For these reasons, it may be prudent for some agencies to simply wait for these more mature solutions.

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

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

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Agencies 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 be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

Appropriate management practices are critical to operating and maintaining a secure wireless network. Security practices entail the identification of an agency's or 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:

- Agency-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 software release that includes security feature enhancements and patches for discovered vulnerabilities.
- Standardized configurations to reflect the security policy, to ensure change of default values, and to ensure consistency of operation.
- Security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies (including the fact that robust cryptography is essential to protect the "radio" channel, and that simple theft of equipment is a major concern).

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

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

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

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. As with many newer technologies (and some mature ones), the security features available may not be as comprehensive or robust as necessary. Because the security features provided in some wireless products may be weak, to attain the highest levels of integrity, authentication, and confidentiality, agencies should carefully consider the deployment of robust, proven, and 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. Although these protection mechanisms have weaknesses described in this publication, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means. As currently defined, the security of neither 802.11 nor 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 secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect that information, regardless of whether the nonvalidated data link security protocols are used.

NIST expects that future 802.11 (and possibly other wireless technologies) products will offer Advanced Encryption Standard (AES)-based data link level cryptographic services that are validated under FIPS 140-2. As these will mitigate most concerns about wireless eavesdropping or active wireless attacks, 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 subnetwork. 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 such as strategically locating access points, ensuring firewall filtering, and blocking and installation of antivirus software are typically necessary. Agencies must be fully aware of 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. 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. Agencies should be aware of the security risks associated with wireless technologies. Agencies need to develop strategies that will mitigate risks as they integrate wireless technologies into their computing environments. This document discusses certain 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 agencies that process sensitive information. They are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

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 agencies with guidance for establishing secure wireless networks.[1] Agencies are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements.

The document addresses two wireless technologies that government agencies 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 out of the scope of this document.

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. Therefore, it is essential to remain abreast of

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

the current and emerging trends in the technologies and in the security or insecurities of these technologies. Again, this guideline does not cover security of other types of wireless or emerging wireless technologies such as third-generation (3G) wireless telephony.

1.3 Audience and Assumptions

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

Hence, the following list highlights how people with differing backgrounds might use this document. The intended audience is varied and includes the following:

- Government managers who are planning to employ wireless networked computing devices in their agencies (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 that 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 six appendices. This subsection is a roadmap describing the document structure.

- Section 1 is composed of an authority, purpose, scope, audience, assumptions, and document structure.
- Section 2 provides an overview of wireless technology.
- Section 3 examines 802.11 WLAN technology, including the benefits and security risks of 802.11 and provides guidelines for mitigating those risks.
- Section 4 examines 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 and abbreviations used in this document.

- Appendix D describes the differences between the various 802.11 standards.
- Appendix E provides a list of useful Universal Resource Locators (URL).
- Appendix F provides a list of useful wireless networking tools and URLs.
- Appendix G contains the references used in the development of the document.

2. Overview of Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) 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. A brief overview of wireless networks, devices, standards, and security issues is presented in this section.

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: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN 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, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR. 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.) This document focuses on 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 (approximately 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 to even "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. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks. It also controls 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

[2] Appendix A provides an overview of wireless frequencies and their use.

reconfigured on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks.

Figure 2-1 illustrates an example of a Bluetooth-enabled mobile phone connecting to a mobile phone network, synchronizing with a PDA address book, and downloading e-mail on an IEEE 802.11 WLAN.

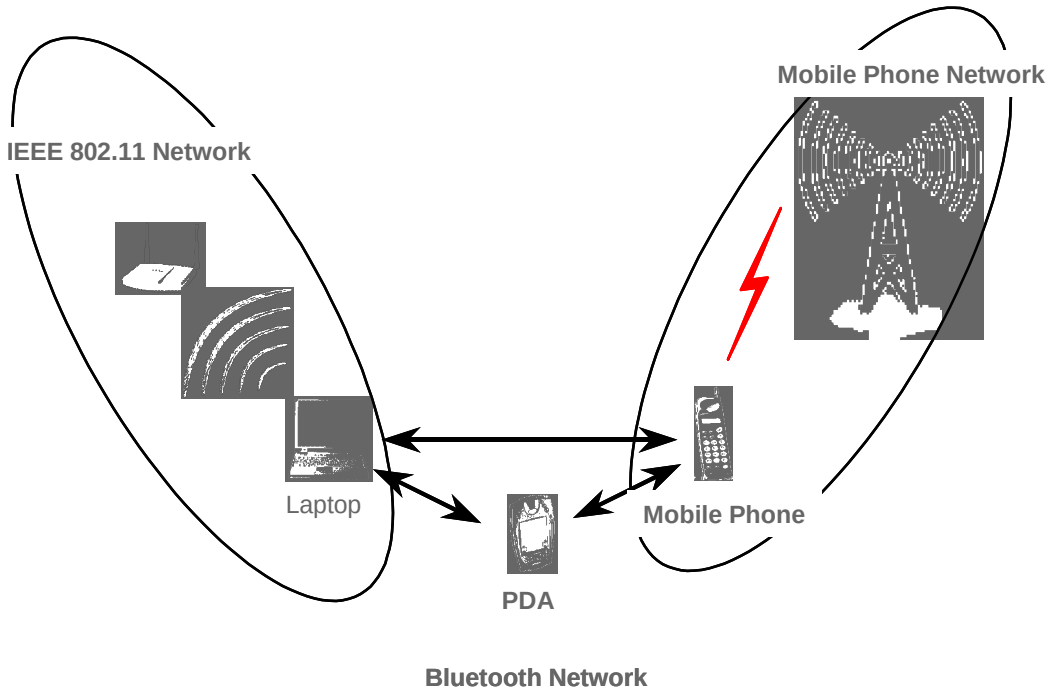

Figure 2-1. Notional Ad Hoc Network

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.[3]

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. 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 device via the Internet and wireless network.

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

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 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.

2.3 Wireless Standards

Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. For this document, the discussion of wireless standards 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 Special Interest Group (SIG). These standards are described 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.

802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. 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. These weaknesses will be discussed in Section 3.3.2. Another standard, 802.11g, still in draft, operates in the 2.4 GHz waveband, where current WLAN products based on the 802.11b standard operate.[4]

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 a very popular ad hoc network standard today. 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

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

headsets and car kits. The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 720 kbps.[5] 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 generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy.[6] All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's 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 agency or organization (although users within an agency or 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. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions.

Attacks resulting from these threats, if successful, place an agency's systems—and, more importantly, its data—at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all government security policies and practices. NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems*, states that information must be protected from unauthorized, unanticipated, or unintentional modification. Security requirements include the following:

- **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.
- **Nonrepudiation**—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.

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

[5] Next generation of Bluetooth will have a theoretical throughput of up to 2 Mbps.

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

> *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.*[7]

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, agencies 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 that 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 agency can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The agency should periodically reassess the policies and measures that 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 SP 800-12, *An Introduction to Computer Security*, and 800-30, *Risk Management Guide for IT Systems*.) To date, the list below includes 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 agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that 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 as them 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 physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- 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 subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

[7] ISO/IEC 7498-2.

- Malicious entities may use a third party, untrusted wireless network services to gain access to an agency's network resources.
- Internal attacks may be possible via ad hoc transmissions.

As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network.

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 merging. 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 global positioning system (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 global system for mobile communications-based (GSM-based) technologies such as General Packet Radio Service (GPRS), Local Multipoint Distribution Services (LMDS), 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.

2.6 Federal Information Processing Standards

FIPS 140-2 defines a framework and methodology for NIST's current and future cryptographic standards. The standard provides users with the following:

- A specification of security features that are required at each of four security levels
- Flexibility in choosing security requirements
- A guide to ensuring that the cryptographic modules incorporate necessary security features
- The assurance that the modules are compliant with cryptography-based standards.

The Secretary of Commerce has made FIPS 140-2 mandatory and binding for U.S. federal agencies. The standard is specifically applicable when a federal agency determines that cryptography is necessary for protecting sensitive information. The standard is used in designing and implementing cryptographic modules that federal departments and agencies operate or have operated for them. FIPS 140-2 is applicable if the module is incorporated in a product or application or if it functions as a standalone device. As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.

Federal agencies, industry, and the public rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, nonrepudiation, identification, and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance.

Both federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module can result in insecure products.

In 1995, NIST, established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to FIPS 140-2, Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are six National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-2 compliance testing.[8]

[8] These labs are listed on the following Web site: http://csrc.nist.gov/cryptval/140-1/1401labs.htm.

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 the RF spectrum available to industry. During the 1980s and early 1990s, growth was relatively slow. Today, however, WLAN technology is experiencing tremendous growth. The key reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standard. 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), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.[9]
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 technologies. The 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. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps.

[9] These numbers will vary immensely depending on the operating environment (obstacles and material construction) and the equipment used. Outdoor ranges, with high gain directional antennas, can exceed 20 miles.

Although this section of the document focuses on the IEEE 802.11 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.[10] For more information on HomeRF, visit the HomeRF Working Group site.[11] 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 IEEE 802.11a standard is the most widely adopted member of the 802.11 WLAN family. It operates in the licensed 5 GHz band using OFDM technology. The popular 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, Scientific, and Medical (ISM) 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 WLAN technology permits transmission speeds of up to 11 Mbits per second. This makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethernet. A summary of the various 802.11 standards is provided in Appendix D.

3.1.3 802.11 Architecture

The IEEE 802.11 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, organizations can achieve broad network coverage. WLAN technology can be used to replace wired LANs totally and 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 transceiver and the logic to interact with the client machine and software. An AP comprises essentially a radio transceiver 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.

[10] For more information see the HiperLAN Alliance site http:///www.hiperlan.com.
[11] For more information see the HomeRF Working Group site http://www.homeRF.org.

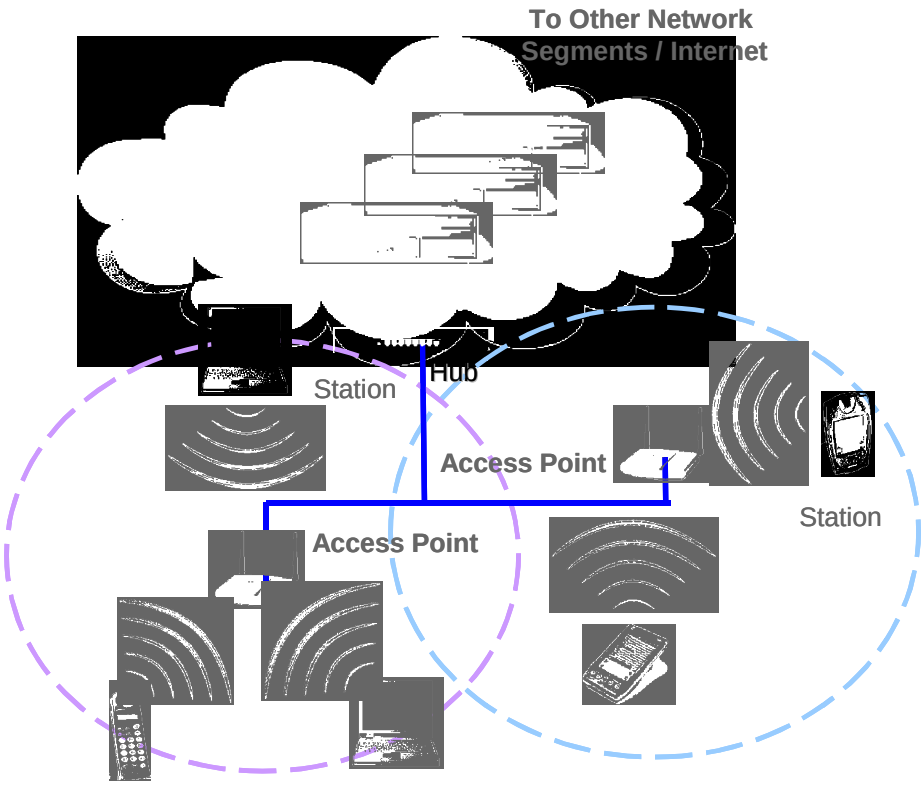

Figure 3-1. Fundamental 802.11 Wireless LAN Topology

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 Internet-worked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an independent basic service set (IBSS). The ad hoc topology is depicted in Figure 3-2 below.

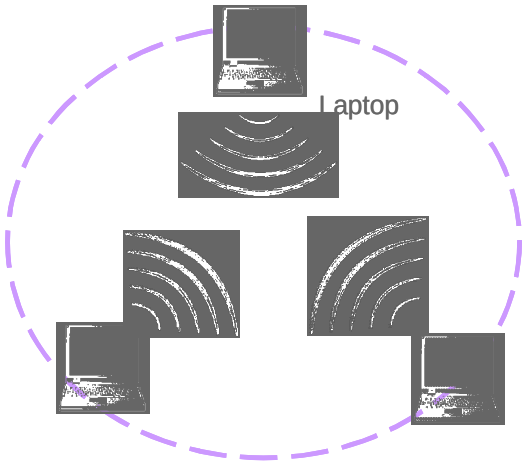

Figure 3-2. 802.11 Wireless LAN Ad Hoc Topology

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 NIC.[12] 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 signals 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 802.11 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 11 Mbps) in a closed office area to 485 meters (for 1 Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11 equipment is approximately 50 meters (about 163 ft.) indoors. A range of 400 meters, nearly ¼ mile, makes WLAN the ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.

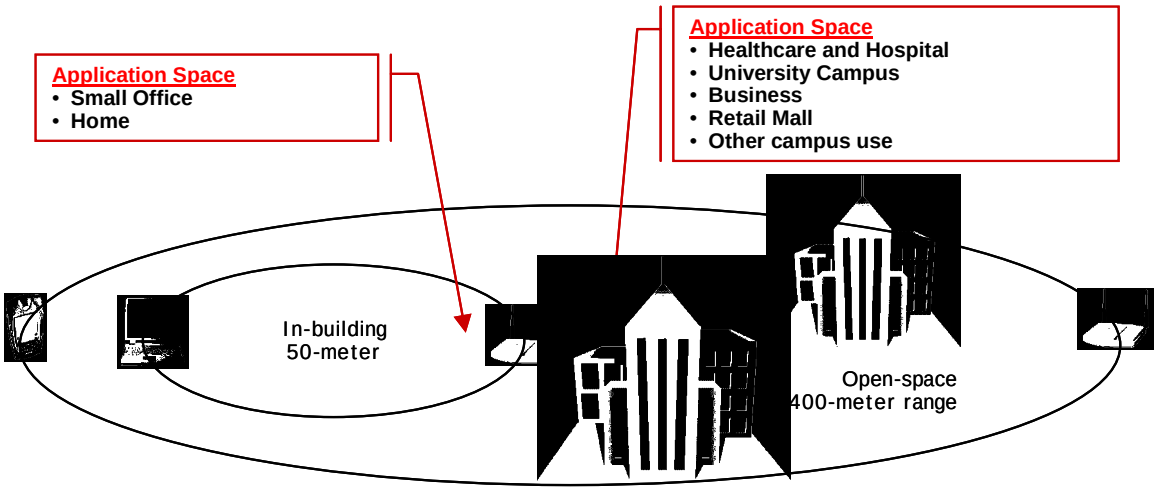

Figure 3-3. Typical Range of 802.11 WLAN

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

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

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's, C's, 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.[13] 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.

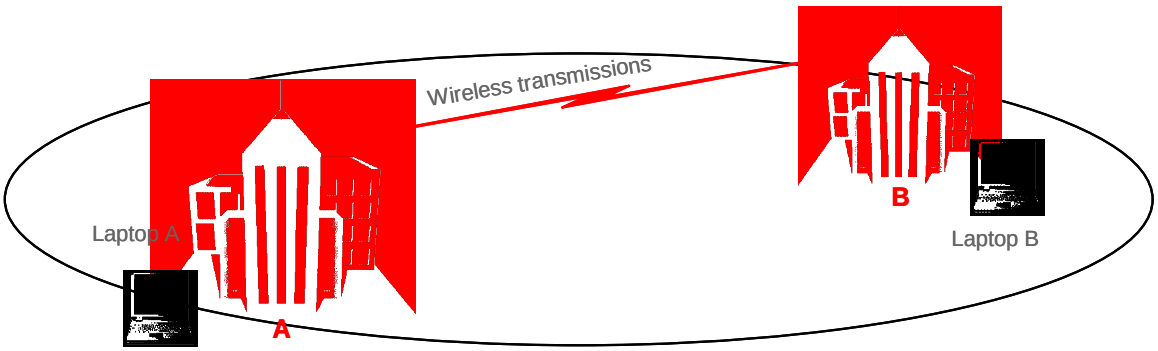

Figure 3-4. Access Point Bridging

3.2 Benefits

WLANs offer four primary benefits:

- **User Mobility**—Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.
- **Rapid Installation**—The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules.
- **Flexibility**—Enterprises can also enjoy the flexibility of installing and 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 peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

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

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

3.3 Security of 802.11 Wireless LANs

This section discusses the built-in security features of 802.11. 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 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure 3-5.

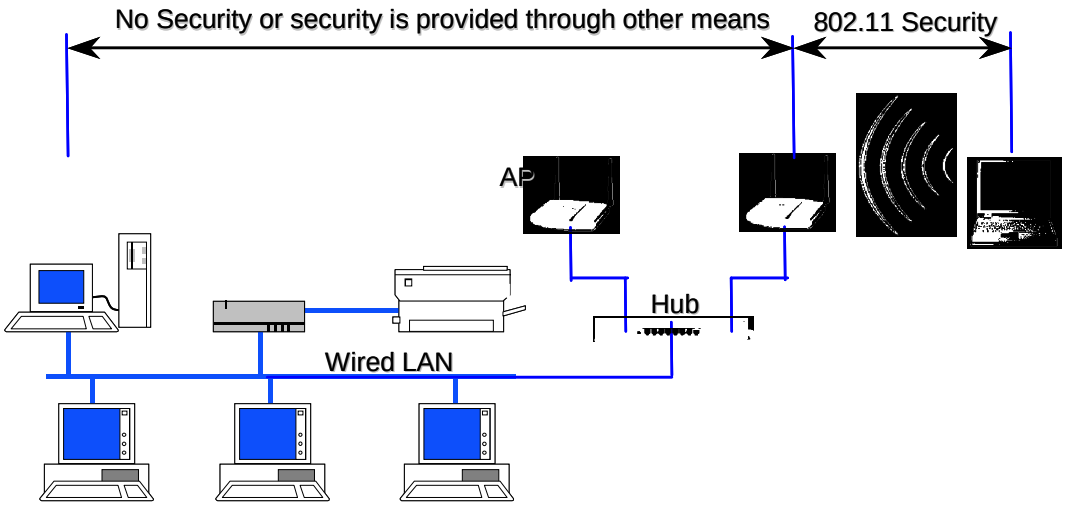

Figure 3-5. Wireless Security of 802.11 in Typical Network

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 provides access control to the network by 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 nonrepudiation. The security services offered by 802.11 are described in greater detail below.

3.3.1.1 Authentication

The IEEE 802.11 specification defines two means to "validate" wireless users attempting to gain access to a wired network: open-system authentication and shared-key authentication. One means, shared-key authentication, is based on cryptography, and the other is not. The open-system authentication technique is not truly authentication; the access point accepts the mobile station without verifying the identity of the station. It should be noted also that the authentication is only one-way: only the mobile station is authenticated. The mobile station must trust that it is communicating to a real AP. A taxonomy of the techniques for 802.11 is depicted in Figure 3-6.

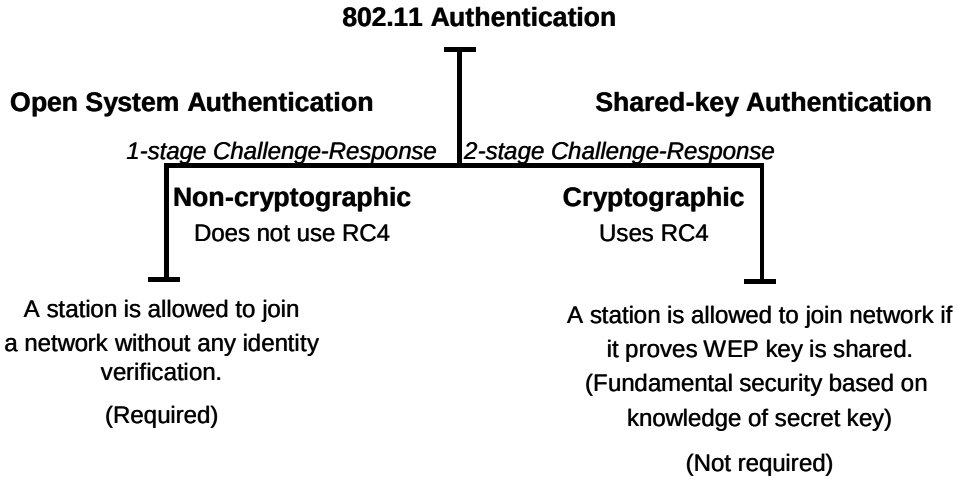

Figure 3-6. Taxonomy of 802.11 Authentication Techniques

With Open System authentication, a client is authenticated if it simply responds with a MAC address during the two-message exchange with an access point. During the exchange, the client is not truly validated but simply responds with the correct fields in the message exchange. Obviously, with out cryptographic validatedation, open-system authentication is highly vulnerable to attack and practically invites unauthorized access. Open-system authentication is the only required form of authentication by the 802.11 specification.

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 conceptually 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 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 and for the generation of the 128-bit challenge text 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. Lastly, the IEEE 802.11 specification does not require shared-key authentication.

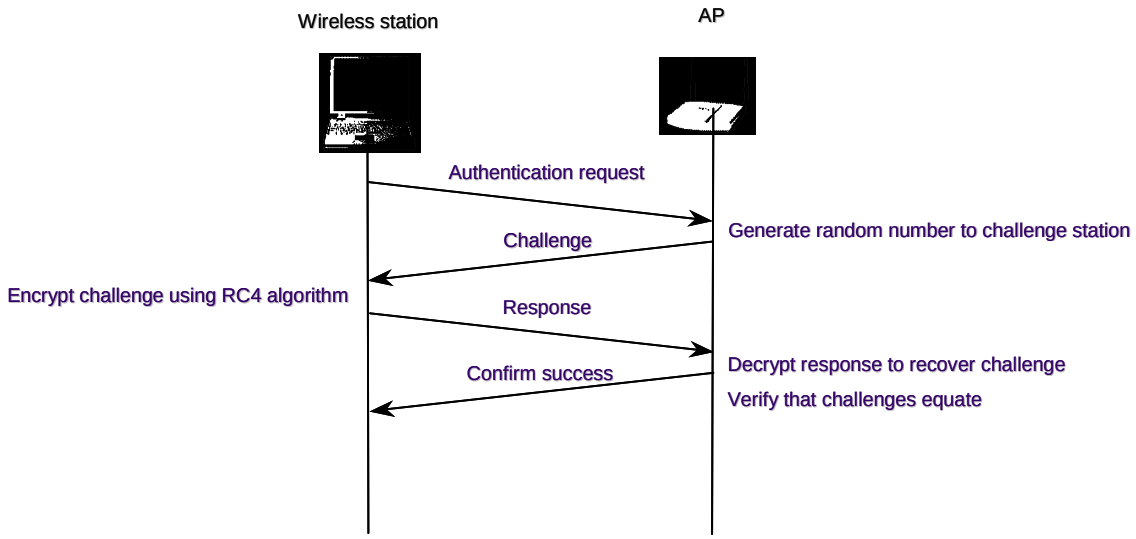

Figure 3-7. Shared-key Authentication Message Flow

3.3.1.2 Privacy

The 802.11 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 “key stream” is simply added modulo 2 (exclusive-OR-ed) 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 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).

As defined in the 802.11 standard, WEP supports only a 40-bit cryptographic keys size for the shared key. However, numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits. At least one vendor supports a keysize of 128 bits. The 104-bit WEP key, for instance, with a 24-bit Initialization Vector (IV) becomes a 128-bit RC4 key. In general, all other things being equal, increasing the key size increases the security of a cryptographic technique. However, it is always possible for flawed implementations or flawed designs to prevent long keys from increasing security. Research has shown that key sizes of greater than 80-bits, for robust designs and implementations, make brute-force cryptanalysis (code breaking) an impossible task. For 80-bit keys, the number of possible keys—a keyspace of more than 10^{26}—exceeds contemporary computing power. 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. However, the cryptographic, standards, and vendor WLAN communities have developed enhanced WEP, which is available as a prestandard vendor-specific implementations. The attacks mentioned above are described later in the following sections.

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

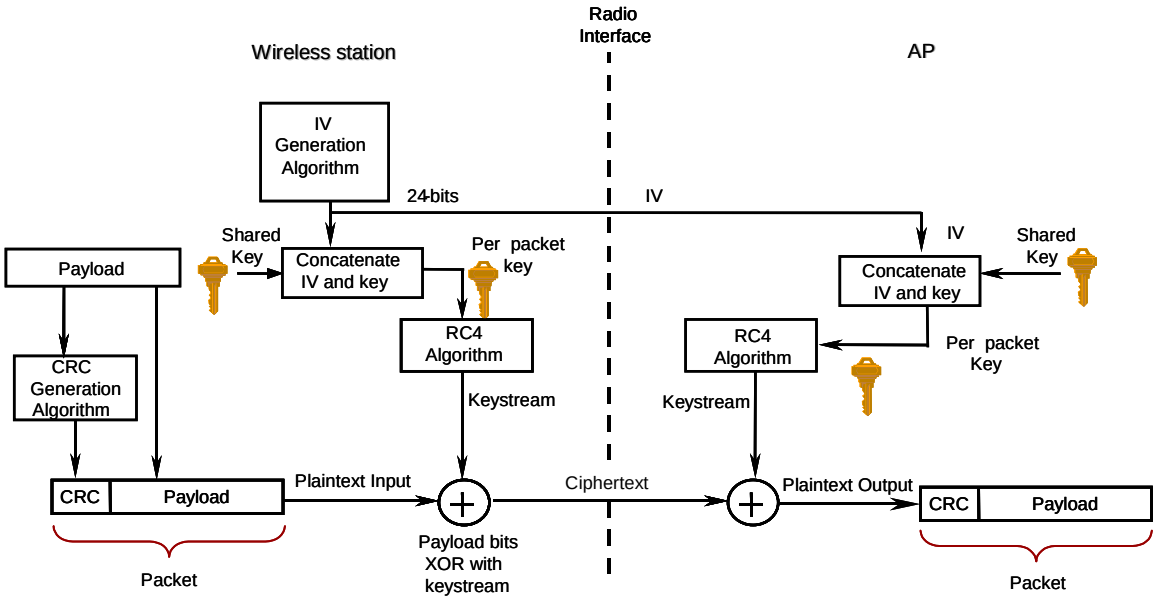

Figure 3-8. WEP Privacy Using RC4 Algorithm

3.3.1.3 Integrity

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

The IEEE 802.11 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. Key management (probably the most critical aspect of a cryptographic system) for 802.11 is left largely as an exercise for the users of the 802.11 network. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original 802.11 specification, with the key distribution unresolved, WEP-secured WLANs do not scale well. 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 significant challenge. It is has been suggested that the only practical way to distribute keys in a large dynamic environment is to publish it. However, a fundamental tenet of cryptography is that cryptographic keys remain secret. Hence

we have a major dichotomy. This dichotomy exists for any technology that neglects to elegantly address the key distribution problem.

3.3.2 Problems With the IEEE 802.11 Standard Security

This section discusses some known vulnerabilities in the standardized security of the 802.11 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 104-bit keys and even 128-bit keys. With the addition of the 24-bit IV, the actual key used in the RC4 algorithm is 152 bits for the 128 bits WEP key. It is worthy to note that some vendors generate keys after a keystroke from a user, which, if done properly, using the proper random processes, can result in a strong WEP key. Other vendors, however, have based WEP keys 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 plain text), 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 enough traffic on a busy network.[14]

Security problems with WEP include 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, if 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 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 cipher-text.

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 successful analytic attack, that recovers the key, after intercepting and analyzing only a relatively small amount of traffic. This attack is publicly available as an attack script and open source code.

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 acknowledge packets with the correct checksum. The combination of noncryptographic checksums with stream ciphers is dangerous and often introduces vulnerablities, as is the case for

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

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 is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.

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

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

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

Security Issue or 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. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent 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 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of 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 because signals can be more easily intercepted.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to “man-in-the-middle” attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

Security Issue or Vulnerability	Remarks
11.The client does not authenticate the AP.	The client needs to authenticate the AP to ensure that it is legitimate and prevent the introduction of rogue APs.

3.4 Security Requirements and Threats

As discussed above, the 802.11 WLAN—or WiFi—industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11 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 802.11 WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that expose organizations to security risks. 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.

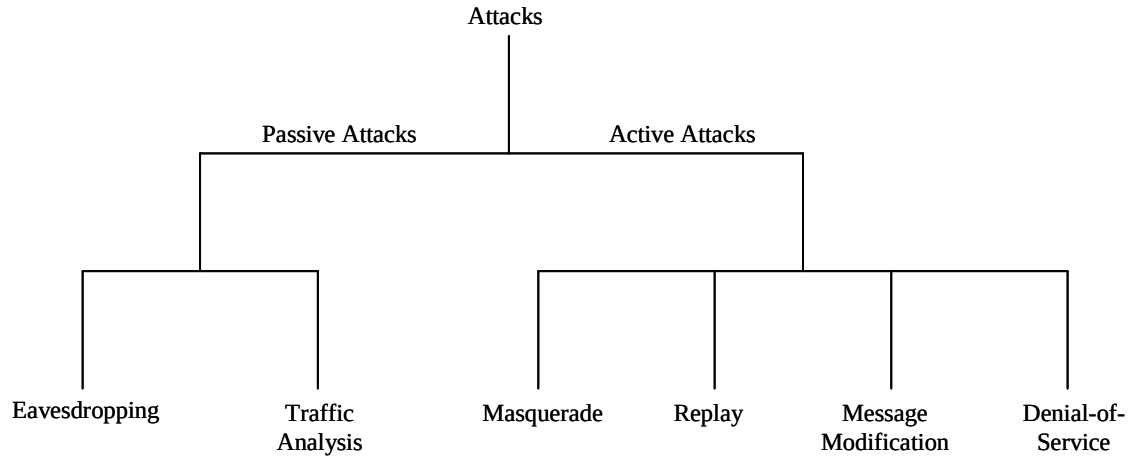

Figure 3-9. Taxonomy of Security Attacks

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 gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.
  - **Eavesdropping**—The attacker 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.

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

3.4.1 Loss of Confidentiality

Confidentiality is the property with which 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 technology, confidentiality is a more difficult security requirement to meet in a wireless network. 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 802.11 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 802.11 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 802.11 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. 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 that was provided for implementation of RC4, which forms part of the original 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 100 MB of network packets have been *sniffed*.[15] On a highly saturated network, collecting this amount of data may only take three or four hours; if traffic volume is low, it may take a few days. For example, a busy data access point transmitting 3,000

[15] See "Tools Dumb Down Wireless Hacking," *The Register*, August 2001 (www.theregister.co.uk).

bytes at 11 Mbps will exhaust the 24-bit IV space after approximately 10 hours.[16] If after ten hours the attacker recovers two cipher texts that have been using the same key stream, both data integrity and confidentiality may be easily compromised. After the network packets have been received, the fundamental keys may be guessed in less than one second.[17] Once the malicious user knows the WEP 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. Airsnort may not be able to take advantage of the enhanced key-scheduling algorithm of RC4 in a pre-standard implementation.

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. Switches, on the other hand, can be configured to prohibit certain attached devices from intercepting broadcast traffic from other specified devices. For example, if a wireless access point were connected to an Ethernet hub, a wireless device that is monitoring broadcast traffic could intercept data intended for wired and wireless clients. Consequently, agencies should consider using switches instead of hubs for connections to wireless access points.[18]

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 purchased or publicly and readily available tools. 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 or irresponsible user could, physically and surreptitiously, insert a rogue AP into a closet, under a conference room table, or any other hidden area within a building. The rogue AP could then be used to allow unauthorized individuals to gain access to the network. As long as its location is in close proximity to the users of the WLAN, and it is configured so as to appear as a legitimate AP to wireless clients, then the rogue AP can successfully convince wireless clients of its legitimacy and cause them to send traffic through it. 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.[19] It is also important to note that rogue access points need not always be deployed by malicious users. In many cases, rogue APs are often deployed by users who want to take advantage of wireless technology without the approval of the IT department. Additionally, since rogue APs are frequently deployed without the knowledge of the security administrator, they are often deployed without proper security configurations.

3.4.2 Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Because organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. 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. This can be detrimental to an organization if important e-mail is widely distributed among e-mail recipients. Because the existing security features of the 802.11 standard do not provide for strong message integrity, other

[16] 10 hours = (3,000 bytes x ((8 bits/byte)/(11 x 106 bits/sec)) x 24) = 36,600 seconds.)
[17] For more information from AirSnort, visit their Web page at http://airsnort.shmoo.com.
[18] See Internet Security Systems, "Wireless LAN Security: 802.11b and Corporate Networks."
[19] See http://iss.net.

kinds of active attacks that compromise system integrity are possible. As discussed before, the WEP-based integrity mechanism is simply a linear CRC. Message modification attacks are possible when cryptographic checking mechanisms such as message authentication codes and hashes are not used.

3.4.3 Loss of Network Availability

A denial of 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 may also be inadvertently caused by cordless phone or microwave oven emissions. Jamming results in a breakdown in communications because legitimate wireless signals are unable to communicate on the network. Nonmalicious 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, agency security policies should limit the types and amounts of data that users are able to download on wireless networks.

3.4.4 Other Security Risks

With the prevalence of wireless devices, more users are seeking ways to connect remotely to their own organization's networks. One such method is the use of untrusted, third-party networks. 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, hotels, and even some coffee franchises are beginning to deploy 802.11 based publicly accessible wireless networks for their customers, even offering VPN capabilities for added security.

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-gain antennas to improve reception and increase coverage area, thus allowing malicious users to eavesdrop more readily on their signals.

By 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. Agencies may want to consider protecting 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). However, in most agencies, this is unnecessary since the information is indeed public already. For private resources, agencies should consider using a VPN solution to secure their connections because 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 agencies 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 agency, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no "one size fits all

solution" when it comes to security. Some agencies may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in money spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some agencies 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:

- Identify who may use WLAN technology in an agency
- 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 all wireless devices
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines for the protection of wireless clients to minimize/reduce theft
- Provide guidelines on the use of encryption and key management
- Define the frequency and scope of security assessments to include access point discovery.

Agencies should 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. 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 "war driving," 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. Agencies 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, agencies 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 because 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. This is useful if the required coverage range is not broad because, for example, 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. Agencies could additionally use directional antennas to control emanations. However, directional antennas do not protect network links; they merely help control coverage range by limiting signal dispersion.

Although mapping the coverage area may yield some advantage relative to security, it 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.[20] 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.[21] It should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions.

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.

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

[21] It should be noted that the software and hardware countermeasures identified in this document could arguably fit into either category.

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 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 agency'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 agency should consider using an automated password generator. 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 agency's security requirements, number of users, and budget constraints. Given the need to ensure good password authentication and policies, it is important to note the critical importance of ensuring that the management interface has the proper cryptographic protection to prevent the unauthorized disclosure of the passwords over the management interface. Numerous mechanisms exist that can be exploited to ensure that encrypted access protects those critical "secrets" in transit. Secure Shell (SSH) and SSL are two such mechanisms.

Establishing proper encryption settings. Encryption settings should be set for the strongest encryption available in the product, depending on the security requirements of the agency. Typically, APs have only a few encryption settings available: none, 40-bit shared key, and 104-bit shared key (with 104-bit shared key 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, agencies 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. It is important to note that products using 128-bit keys will not interoperate with products that use 104-bit keys.

Controlling the reset function. The reset function poses a particular problem because it allows an individual to negate any security settings that 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. Agencies can detect threats by performing regular security audits. Additionally, reset can be invoked remotely over the management interface on some products. For

this reason, there is a greater need to have proper password administration and encryption on the management interface.

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.[22] 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. Additionally, most products only support a limited number of MAC addresses in the MAC ACL. The size of the access control list may be insufficient for medium-to-large networks.

Changing the SSID. The SSID of the AP must be changed from the factory default. The default values of SSID used by many 802.11 wireless LAN vendors have been published and are well-known to would-be adversaries. The default values should be changed (always a good security practice) to prevent easy access. Although an equipped adversary can capture this identity parameter over the wireless interface, it should be changed to prevent unsophisticated adversary attempts to connect to the wireless network.

Maximize the Beacon Interval. The 802.11 standard specifies the use of "Beacon frames" to announce the existence of a wireless network. These beacons are transmitted from APs at regular intervals and allow a client station to identify and match configuration parameters in order to join a wireless network. APs may not be configured to suppress the transmission of the Beacon frames and its mandatory SSID field. However, the interval length may be set to its highest value that results in approximately a 67 second interval. While the security improvement is marginal, it does make it somewhat more difficult to passively "find a network" because the AP is quieter and the SSID is not transmitted as frequently. Using a longer Beacon interval forces an adversary to perform what is referred to as "active scanning" using Probe messages with a specific SSID. Hence, where possible, wireless networks should be configured with the longest beacon interval.

Disable broadcast SSID feature. The SSID is an identifier that is sometimes referred to as the "network name" and is often a simple ASCII character string. The SSID is used to assign an identifier to the wireless network (service set). Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. The SSID, typically a null-terminated ASCII string, has a range from 0 to 32 bytes. The zero-byte case is a special case called the "broadcast" SSID. A wireless client can determine all the networks in an area by actively scanning for APs with the use of broadcast Probe Request messages with a zero SSID. The broadcast SSID probe triggers a Probe Response from all 802.11 networks in the area. Disabling the broadcast SSID feature in the APs causes the AP to ignore the message from the client and forces it to perform active scanning (probing with a specific SSID).

[22] Dave Molta, "WLAN Security On the Rise," http://www.networkcomputing.com.

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 forms 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, agencies should change the shared key from the default setting because it is easily exploited. In general, agencies should opt for the longest key lengths (e.g., 104 bits). Finally, a generally accepted principle for proper key management is to change cryptographic keys often and when there are personnel changes.

Using SNMP. Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP, SNMPv1 and SMPv2 support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security are highly recommended. If SNMP is not required on the network, the agency should simply disable SNMP altogether. If an agency must use a version of SNMP besides version 3, they must recognize and accept the risks. It is common knowledge that the default SNMP community string that SNMP agents commonly use is the word "public" with assigned "read" or "read and write" privileges. Using this well-known default string leaves devices vulnerable to attack. If an unauthorized user were to gain access and had read/write privileges, that user could write data to the AP, resulting in a data integrity breach. Agencies that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure and are not recommended. Agencies should use SNMPv3.[23]

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. Agencies that incur radio interference need to determine if one or more nearby AP(s) are using the same channel or a channel within five channels of their own and then choose a channel that is in a different range.[24] For example, channels 1, 6, and 11 can be used simultaneously by APs that are close to each other without mutual interference. Agencies must perform a site survey to discover any sources of radio interference. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP.

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.

---

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

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

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 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 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, many vendors have "security alert" e-mail lists to advise customers of new security vulnerabilities and attacks. Administrators should sign up for these critical alerts. Lastly, administrators can check with the NIST ICAT[25] vulnerability database 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*.

An example of a software or firmware patch is 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 Fast Packet Keying Solution uses a hashing technique that rapidly generates the per packet keys. The IEEE has approved the fast packet keying technology as one fix to the 802.11 protocol. Vendors have started applying the fix to new wireless products and have developed software patches for many existing products. Agencies should check with their individual vendors to see if patches are available for the products they have already purchased.

Another example of a software or firmware patch that will be available as early as late 2002 is WiFi Protected Access (WPA).[26] WPA, which is being promoted by the WiFi Alliance, is an interim security solution that does not require a hardware upgrade in existing 802.11 equipment. WPA is not a perfect solution but is an attempt to quickly and proactively deliver enhanced protection–to address some of the problems with WEP– prior to the full-blown security techniques of IEEE 802.11 TGi. WiFi Protected Access, a subset of the TGi solution, includes two main features:

- 802.1X
- Temporal Key Integrity Protocol (TKIP)

The 802.1X port-based access control provides a framework to allow the use of robust upper layer authentication protocols. It also facilitates the use of session keys–since cryptographic keys should change often. TKIP includes four new algorithms to enhance the security of 802.11. TKIP extends the IV space, allows for per-packet key construction, provides cryptographic integrity, and provides key derivation and distribution. TKIP, through these algorithms, provides protection against various security attacks discussed earlier, including replay attacks and attacks on data integrity. Additionally, it addresses the critical need to change keys. Again, the objective of WPA is to bring a standards-based security solution to the marketplace to replace WEP while giving the IEEE 802.11 Task Group i enough time to complete

[25] See http://icat.nist.gov/icat.cfm.
[26] WiFi means "wireless fidelity" and is a synonym for 802.11b.

and finalize the full 802.11i Robust Security Network (RSN), an amendment to the existing wireless LAN standard. RSN, to be available in the 4th quarter of 2003, will also include the Advanced Encryption Standard (AES) for confidentiaility and integrity. The RSN solution will require hardware replacements. For additional information, refer to Section 3.6.

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, or PKI; or a combination of solutions (e.g., smart cards with PKI).[27] 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 this document.

All agencies should implement a strong password policy, regardless of the security level of their operations. Strong passwords are simply a fundamental measure in any environment. Agencies should also 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.[28] 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 guidelines. Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage them. 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, agencies may still need additional layers of protection. Users that access public wireless networks in airports or conference centers, for example, should use a personal firewall. Personal firewalls also provide additional protection against rogue access points that can be easily installed in public places.

3.5.3.1.5 Intrusion Detection System (IDS)

An intrusion detection system (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 be host-based, network-based, or hybrid, the hybrid combining features of host- and network-based IDS. 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

---

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

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

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*.)

IDS technology on wired networks can have the following limitations if used to protect wireless networks:

- Network-based IDS sensors that have been placed on the wired network behind the wireless access point will not detect attacks directed from one wireless client to another wireless client (i.e., peer to peer) on the same subnet. The wireless access point switches traffic directly between wireless clients. The traffic does not enter the wired network, it is WEP encrypted, and wired-network IDS sensors do not have an opportunity to capture clear-text packets for analysis. As a result, an adversary that successfully connects an unauthorized wireless client to the network can perform discovery and attack against other wireless hosts without detection by the network-based IDS sensor. In this scenario, the data on the other wireless clients is at risk and information gathered from the other clients may be used to form an attack on the wired network.

- IDS sensors on the wired network usually will not detect attempts to “deassociate” (to end an association relationship with) a legitimate client from the wireless network and will not detect the association of an unauthorized wireless client with the wireless network. Flooding, jamming, and other DoS attacks against wireless devices use physical and data-link layer techniques that are not visible to the IDS sensor at a packet level and generally would not be routed onto the wired network.

- IDS technology for wired networks generally only detects attacks once packets are directed at hosts on the wired network from a compromised wireless client. At that point, the wireless network has already been compromised, and risk to the wired network is imminent. An important goal is to detect and send an alarm on unauthorized wireless activity before it affects the wired network.

- IDS technology on wired networks will not identify the physical location of rogue access points within the building. These rogue access points can act as entry points for unauthorized wireless access from remote locations.

- IDS technology will not detect an authorized wireless device communicating peer-to-peer with an unauthorized wireless device. This scenario can create a bridge into the wired network by allowing an adversary to connect to a wireless device that is operating in “ad hoc” mode. The ad hoc mode allows a wireless device to be used to relay traffic to the network and creates a number of potential attack scenarios.

Expansion of a wired network by connecting one or more wireless networks significantly expands the network’s security perimeter and introduces risk that may not be addressed by existing intrusion detection

devices on the wired network. Agencies that want to expand network functionality by adding a wireless capability should examine the existing IDS architecture and consider additional solutions to address the above-mentioned risks. Agencies should consider implementing a wireless IDS solution that provides the following capabilities:

- Identification of the physical location of wireless devices within the building and surrounding grounds
- Detection of unauthorized peer-to-peer communications within the wireless network that are not visible to the wired network
- Analysis of wireless communications and monitoring of the 802.11 RF space and generation of an alarm upon detection of unauthorized configuration changes to wireless devices that violate security policy
- Detection of and alarming for when a rogue access point goes live within the agency's security perimeter
- Detection of flooding and deassociation attempts before they successfully compromise the wireless network
- Provision of centralized monitoring and management features with potential for integration into existing IDS monitoring and reporting software to produce a consolidated view of wireless and wired network security status.

Agencies that require high levels of security should consider deploying an IDS because it provides an added layer of security. Agencies that currently employ IDSs should consider the addition of the capabilities above to supplement their existing capabilities. The deployment of IDS obviously comes at a cost and should be considered if financially feasible. In addition to the cost of the system itself, an IDS requires experienced personnel to monitor and react to IDS events and to provide general administration to the IDS database and components. Agencies should also consider using a correlation engine, which receives standard real-time security events from a variety of sensors, such as IDS, firewall, and virus systems. Correlation engines combine in real-time and analyze a wide variety of threats. These threats can include several classes of attacks, such as Distributed Denial of Service (DDoS) attacks.

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 setting. The setting of 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.[29] 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.[30] 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, it is recommended nonetheless as a good practice. Again, users of 802.11 APs and wireless clients should be vigilant about checking with the vendor regarding upgrades to firmware and software as they may overcome some of the WEP problems.

---

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

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

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 agencies 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, to determine if wireless products are transmitting correctly and on the correct channels. Administrators should periodically check within the office building space (and campus) for rogue APs and against other unauthorized access. Agencies may also consider using an independent third party to conduct the security audits. Independent third-party security consultants are often 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 agency 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.[31] For more information on network security, see NIST Draft Special Publication 800-42, *Guideline on Network Security Testing*.[32] It is worth noting that agencies 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.

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. Agencies can use smart cards in conjunction with username or password or by themselves. They can use smart cards in two-factor authentication (see above). Agencies 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.

3.5.3.2.2 Virtual Private Networks

VPN technology is a rapidly growing technology that provides 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

---

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

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

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.

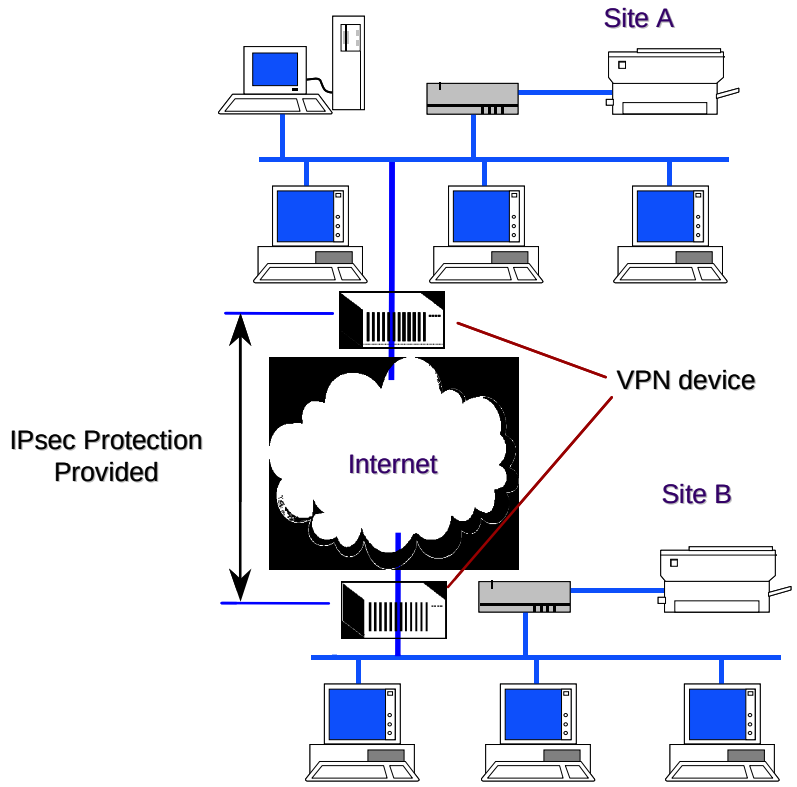

Figure 3-10. Typical Use of VPN for Secure Internet Communications From Site-to-Site

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
- Integrity
- Data origin authentication
- 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. 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 allow for secret keys and other protection-related

parameters to be exchanged prior to a communication without the intervention of a user.[33] IKEv1 is in the process of being replaced by IKEv2.[34]

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 agency 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.[35]

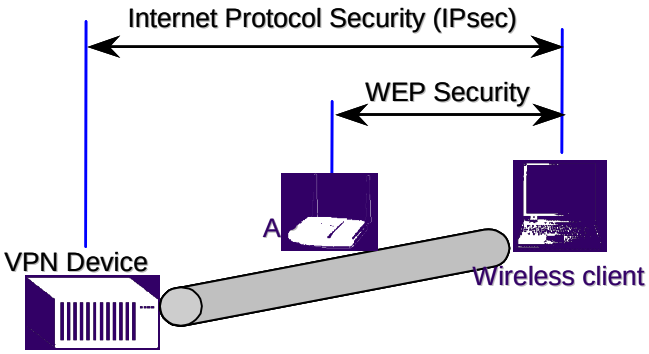

Figure 3-11. VPN Security in Addition to WEP

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 instead of 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 (public-key based) certificates for wireless client device authentication. The reader should recognize that an organization that uses preshared keys for a VPN solution will encounter the same scalability and key distribution problems present in WEP. Additionally, user authentication to the VPN gateway can occur using remote authentication dial-in user service (RADIUS) or one-time-passwords (OTP). The VPN gateway may or may not have an integral firewall to restrict traffic to certain locations within the enterprise network. Today, most VPN devices have integrated firewalls that work together to protect both the network from unauthorized access and the user data going over the network. Integrated VPNs and firewalls save costs and reduce administrative burden. 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.

---

33 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.

34 For more information on IKEv2, see http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-02.txt.

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

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 enterprise applications are not always addressed with this security solution. Some VPN devices can use user-specific policies to require authentication before accessing enterprise applications. Agencies may want to seek assistance in developing a comprehensive enterprise security strategy.

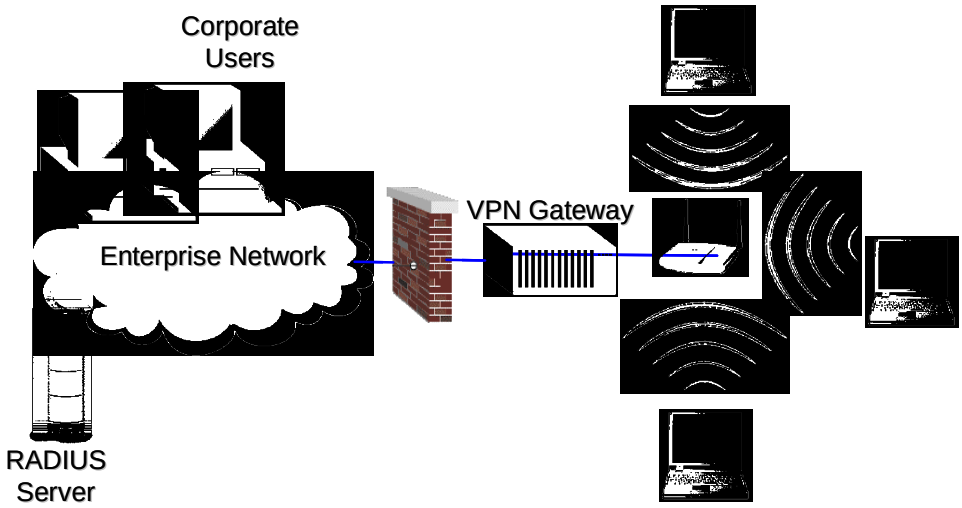

Figure 3-12. Simplified Diagram of VPN WLAN

3.5.3.2.3 Public Key Infrastructure (PKI)

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 nonrepudiation, 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, which can be used with application-level security, to sign and encrypt messages. Smart cards provide even greater utility since the certificates are integrated into the card. Smart cards serve both as a token and a secure (tamper-resistant) means for storing cryptographic credentials. 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 provide an added layer of protection when used either alone or along with another security solution. For example, for agencies 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.

3.6 Emerging Security Standards and Technologies

Like the security industry, standards organizations have responded to the flurry over insecurities in 802.11 WLANs. Activity is occurring in the Internet Engineering Task Force (IETF) and 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 additional ciphers 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 many of 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—WiFi Protected Access (WPA)—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, requiring only changes to firmware and software drivers. The third initiative from IEEE is the introduction of a new standard, IEEE 802.1X-2001, a generic framework for port-based network access control and key distribution, approved in June 2001. By defining the encapsulation of EAP (defined in RFC 2284) over IEEE 802 media, IEEE 802.1X enables an AP and station to mutually authenticate one another. See also Section 3.5.3.1.2 for a brief discussion on WPA and TKIP.

Since IEEE 802.1X was developed primarily for use with IEEE 802 LANs, not for use with WLANS, the IEEE 802.11i draft standard defines additional capabilities required for secure implementation of IEEE 802.1X on 802.11 networks. These include a requirement for use of an EAP method supporting mutual authentication, key management, and dictionary attack resistance. In addition, 802.11i defines the hierarchy for use with the TKIP and AES ciphers and a "four way" key management handshake used to ensure that the station is authenticated to the AP and a back-end authentication server, if present. As a result, to provide adequate security, it is important that IEEE 802.1X implementations on 802.11 implement the IEEE 802.11i enhancements, as well as the basic IEEE 802.1X standard.

IEEE 802.1X can be implemented entirely on the AP (by providing support for one or more EAP methods within the AP), or it can utilize a backend authentication server. The IEEE 802.1X standard supports authentication protocols such as RADIUS, Diameter, and Kerberos. RADIUS, described in RFC 2865-2869, and RFC 3162, enables authentication, authorization, and accounting for Network Access Server (NAS) devices, including dial-up, xDSL, and 802.11.

The 802.1X standard can be implemented with different EAP types, including EAP-MD5 (defined in RFC 2284 and supporting only one-way authentication without key exchange) for Ethernet LANs and EAP-TLS (defined in RFC 2716, supporting fast reconnect, mutual authentication and key management via certificate authentication). Currently a new generation of EAP methods are being developed within the IETF, focused on addressing wireless authentication and key management issues. These methods support additional security features such as cryptographic protection of the EAP conversation, identity protection, secure ciphersuite negotiation, tunneling of other EAP methods, etc. For the latest developments on the status of each specification, the reader is encouraged to refer to the IEEE 802.11 standards web site.[36]

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

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

Agency 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, Agency A has its computer security department perform a risk assessment in accordance with NIST Special Publication 800-30.[37] 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 Agency 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 Agency 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. Additionally, only network administrators have access to the network devices.

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, 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 104-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. The NIST ICAT Vulnerability Database or an equivalent source for a comprehensive list of known vulnerabilities in major software packages and hardware products is

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

checked. 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. Also, 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 Agency A incorporate the use of an IDS. The IDS would 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 Agency A's network and, more importantly, the data that traverses it. The IDS is aprt of an overall defense-in-depth strategy and is not relied on to detect all attacksagainst or misuse of the network.

The security department presents the manager with the risk assessment, which includes the countermeasures described above (and listed below) and a diagram (see 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 agency 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 an 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, the solution that is most secure and cost-effective, for the enterprise can be determined.

Agency A’s proposed countermeasures follow:

- Adopt personal identification system for physical access control.
- Disable file and directory sharing on PCs.
- Ensure that sensitive files are password protected and encrypted.
- Turn off all unnecessary services on the AP.
- If practical, power off the AP(s) when not in use.
- If the AP supports logging, turn it on and review the logs regularly.
- Secure AP configuration as follows:
  - 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 802.11 products with best long-term wireless security strategy and longevity in marketplace.
- Select products with SNMPv3 (or other encrypted management capabilities) on the APs and the integrated firewall-VPN device.
- Seek expert assistance in conducting a security assessment after deployment.

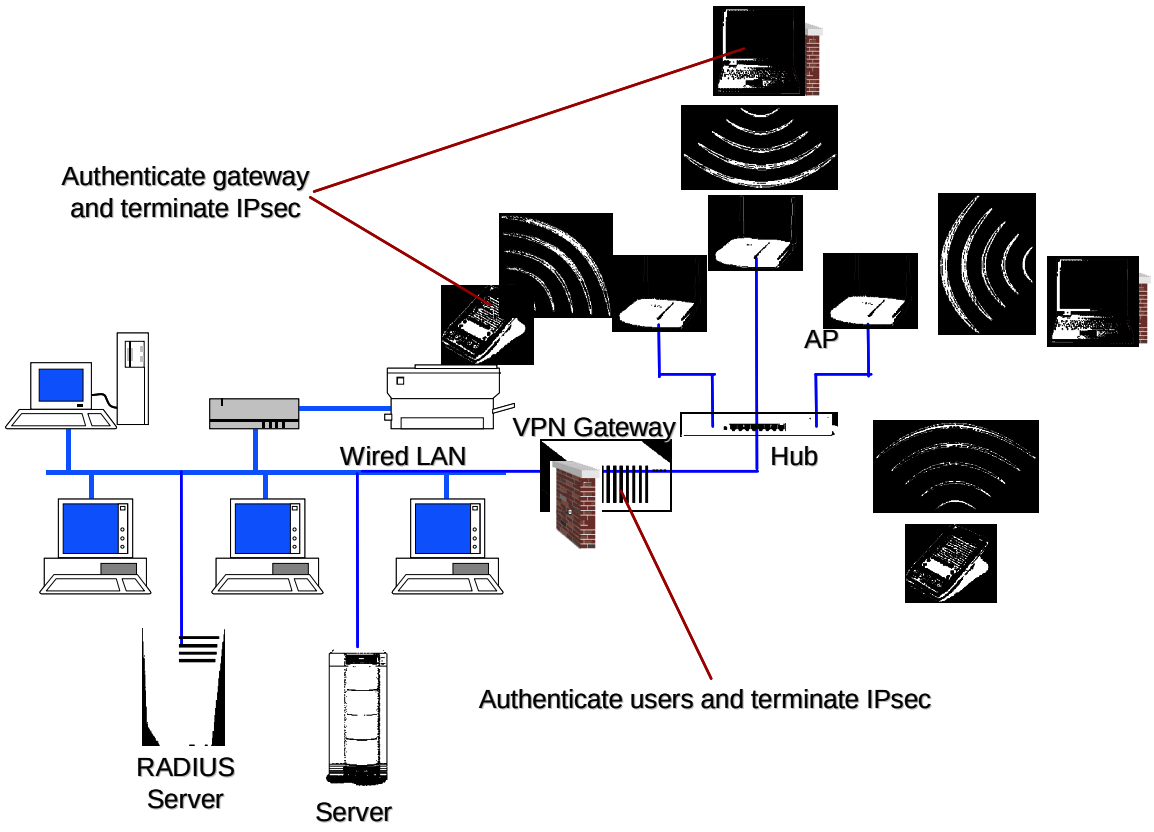

Figure 3-13. Agency A WLAN Architecture

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 recommended for all agencies. The second column, the "Should Consider" column, if checked, means the recommendation is something that an agency should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some sort of additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the "Should Consider" column is checked, agencies need to carefully consider the option and weigh the costs versus the benefits. The last column, the "Status" column, is intentionally left blank and allows an agency 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 agency, asking "Have I done this?"

Table 3-3. Wireless LAN Security Checklist

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8.	Complete a site survey to measure and establish the AP coverage for the agency.	✓		
9.	Take a complete inventory of all APs and 802.11 wireless devices.	✓		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	✓		
11.	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.	✓		
12.	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	✓		
Technical Recommendations				
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
14.	Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).	✓		
15.	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	✓		
16.	Restore the APs to the latest security settings when the reset functions are used.	✓		
17.	Change the default SSID in the APs.	✓		
18.	Disable the broadcast SSID feature so that the client SSID must match that of the AP.		✓	
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	✓		
20.	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
21.	Understand and make sure that all default parameters are changed.	✓		
22.	Disable all insecure and nonessential management protocols on the APs.	✓		
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.	✓		
24.	Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	✓		
27.	Install antivirus software on all wireless clients.	✓		
28.	Install personal firewall software on all wireless clients.	✓		
29.	Disable file sharing on wireless clients (especially in untrusted environments).	✓		
30.	Deploy MAC access control lists.		✓	
31.	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	✓		
32.	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.		✓	
33.	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	✓		
34.	Fully test and deploy software patches and upgrades on a regular basis.	✓		
35.	Ensure that all APs have strong administrative passwords.	✓		
36.	Ensure that all passwords are being changed regularly.	✓		
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		✓	
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.	✓		
39.	Use static IP addressing on the network.		✓	
40.	Disable DHCP.		✓	
41.	Enable user authentication mechanisms for the management interfaces of the AP.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
42.	Ensure that management traffic destined for APs is on a dedicated wired subnet.	✓		
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	✓		
	Operational Recommendations			
44.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	✓		
45.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	✓		
46.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.		✓	
47.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.		✓	
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		✓	
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
51.	Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.	✓		
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
53.	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.		✓	
54.	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		✓	
55.	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	✓		
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	✓		

3.9 Wireless LAN Risk and Security Summary

Table 3-4 lists security recommendations for 802.11 wireless LANs. For each recommendation, narrative is provided that addresses the security need, requirements or justification for that rcommendation.

Table 3-4. Wireless LAN Security Summary

	Security Recommendation	Security Needs, Requirements, or Justification
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable architecture, implementation, and uses for 802.11 wireless technologies.
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., 802.11).	A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.
4.	Ensure that the client NIC and AP support firmware upgrades so that security patches may be deployed as they become available (prior to purchase).	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	The external boundaries should be secured to prevent malicious physical access to an organization's information system infrastructure such as a fence or locked doors.
7.	Deploy physical access controls to the building and other secure areas (e.g., using photo IDs or card badge readers).	Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.
8.	Complete a site survey to measure and establish the AP coverage for the agency.	Proper placement of Access Points will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP and that ensures that the coverage range does not expose APs to potential malicious activities.
9.	Take a complete inventory of all APs and 802.11 wireless devices.	A complete inventory list of APs and 802.11 wireless devices can be referenced when conducting an audit for unauthorized use of wireless technologies.
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	Security policy enforcement is vital for ensuring that only authorized APs and 802.11 wireless devices are operating in compliance with the organization's wireless security policy.
11.	Locate APs on the interior of buildings instead of near exterior walls and windows.	Locating APs near exterior walls and windows provides a better range of access to potential external malicious users. Choosing the location wisely to balance security and coverage should be considered.
12.	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Physically securing the APs, putting them "out of reach," prevents unauthorized access by potential malicious users.

	Security Recommendation	Security Needs, Requirements, or Justification
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	By empirically testing the AP coverage range for an agency, a level of risk associated with the access range by potential malicious users can be better understood.
14.	Make sure that APs are turned off while they are not being used (e.g., after hours, weekends).	Shutting down APs when not in use minimizes potential exposure to malicious activity.
15.	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	The reset function allows an individual to negate any security settings administrators have configured on an access point.
16.	Restore the APs to the latest security settings when the reset functions are used.	Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.
17.	Change the default SSID in the APs.	Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to 802.11 networks using the default SSID.
18.	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Malicious users can more easily detect and exploit APs that are broadcasting the SSID. Disabling the broadcast SSID feature minimizes exposure of the AP to malicious users.
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	The SSID should be somewhat difficult for malicious users to use to determine the organization or agency that owns the AP. The SSID should also be long and difficult to guess.
20.	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	Radio interference between APs can result in a denial of service. So, using channels in a different range ensures service availability.
21.	Understand and make sure that all default parameters are changed.	Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.
22.	Disable all insecure and nonessential management protocols on the APs.	Management protocols that are enabled on APs but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an access point.
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy features.	Enabling built-in security features provides greater security than the default settings.
24.	Ensure that encryption key sizes are at least 128 bits or as large as possible.	Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit provides an "intractable" key space against cryptanalysis, if the algorithm and implementation are sound.
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	Changing default shared keys periodically decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	A firewall can enforce a security policy on the information flow between the wired network and the wireless network.
27.	Install antivirus software on all wireless clients.	Antivirus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.

	Security Recommendation	Security Needs, Requirements, or Justification
28.	Install personal firewall software on all wireless clients.	Personal firewalls help to protect against wireless network attacks.
29.	Disable file sharing on wireless clients (especially in untrusted environments).	Malicious users can potentially exploit wireless clients enabled for file sharing.
30.	Deploy MAC access control lists.	The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.
31.	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	The use of layer 2 switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.
32.	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.	The use of IPsec-based VPN provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.
33.	Ensure that encryption being used is sufficient with the sensitivity of the data on the network and the processor speeds of the computers.	Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirement and overhead cost related to processor capability.
34.	Fully test and deploy software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.
35.	Ensure that all APs have strong administrative passwords.	Administrator passwords on APs should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.
36.	Ensure that all passwords are being changed regularly.	Passwords should changed regularly to reduce the risk of a compromised password being exploited.
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.
38.	Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use a different vendor.	The “ad hoc mode” for 802.11 can be exploited. Users of hosts with “ad hoc mode” enabled may unintentionally allow users to inadvertently or maliciously connect to those systems.
39.	Use static IP addressing on the network.	Using static IP addressing makes it more difficult for a hostile user to connect to the network.
40.	Disable DHCP.	If DHCP is disabled, then hosts are forced to use a static IP address.
41.	Enable user authentication mechanisms for the management interfaces of the AP.	User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.
42.	Ensure that management traffic that is destined for APs is on a dedicated wired subnet.	Passing management traffic over an “out of band’ network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	SNMPv3 has enhanced security features relative to its predecessor SNMP protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of APs.

	Security Recommendation	Security Needs, Requirements, or Justification
44.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	Agencies that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Agencies should use SNMPv3.
45.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	AP management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.
46.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	By using a local serial port interface for AP configuration ensures that sensitive management information do not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.
47.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.	Use of authentication mechanisms such as RADIUS and Kerberos can improve the security and simplify user management.
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or network-based agents) deployed on the wireless network can detect and respond to potential malicious activities.
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.
51.	Enable use key-mapping keys rather than default keys so that sessions use distinct WEP keys.	The use of distinct WEP keys provides more security than default keys and reduces the risk of key compromise.
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.
53.	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.	An appointed individual designated to track the latest technology enhancements, standards, and risks will help to ensure the continued secure implementation of wireless technology.
54.	Wait for future releases of 802.11 WLAN technologies that incorporate fixes to the security features, or provide enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the 802.11 products with major security vulnerabilities that have not been fixed.
55.	When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Sensitive or proprietary configuration settings should be cleared from access points before removing them from use or disposing to prevent inadvertent disclosure of the information to potentially malicious users.
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	Ensure that the APs are set to perform logging. Also, review of audit and logging data helps to ensure user accountability.

	Security Recommendation	Security Needs, Requirements, or Justification
57.	If the access point supports logging, turn it on and review the logs on a regular basis.	Access point logs should be enabled and regularly reviewed for malicious activity.

4. Wireless Personal Area Networks

This section provides a detailed overview of Bluetooth technology—an ad hoc networking technology. As mentioned earlier, ad hoc networks are a relatively new paradigm of wireless communications in which no fixed infrastructure exists 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 that enable devices to communicate with each other. Devices within an ad hoc network control the network configuration, and they maintain and share resources. Ad hoc networks are similar to peer-to-peer (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 networks rely 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 applications, within a wireless 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 wireless 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, 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 locate each other, but making connections with other devices and forming networks requires user action.

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 scatter-nets, 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 or 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 – 2.4835 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1 Mbps (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 for confidentiality, challenge-response for 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. Signals leak outside desired boundaries.

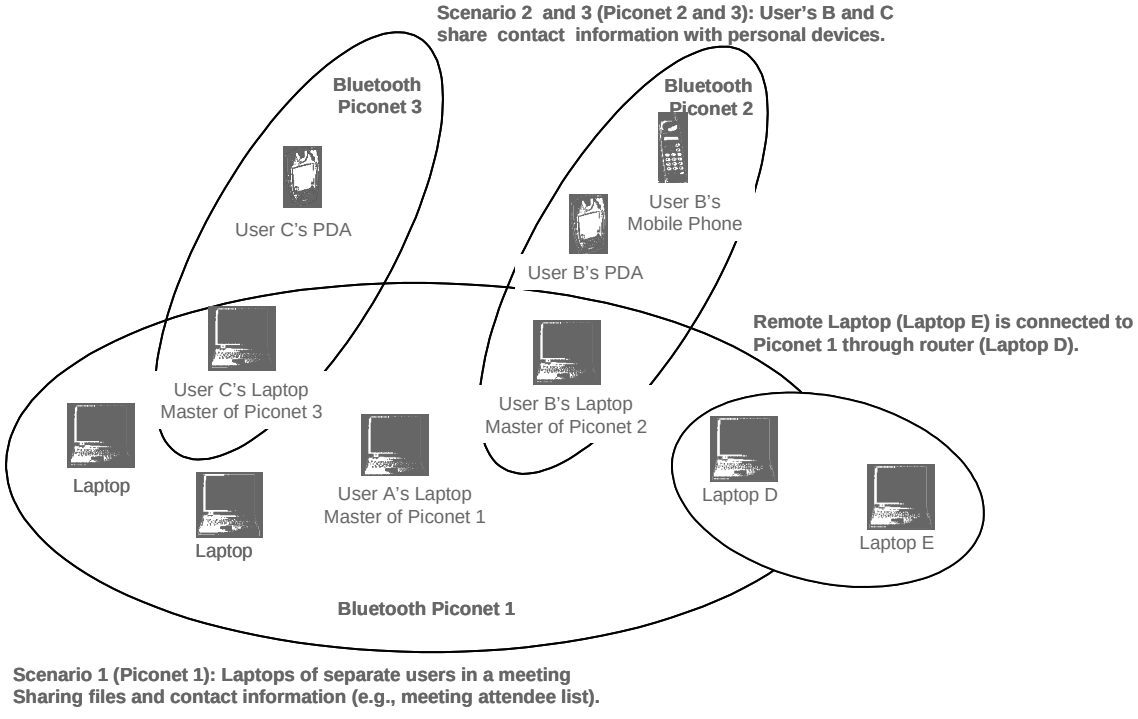

Figure 4-1. Typical Bluetooth Network—A Scatter-net

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 2.4 GHz, 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 1 Mbps. However, in reality the networks cannot support such data rates because of communication overhead. The second generation of Bluetooth technology is expected to provide a maximum bandwidth of 2 Mbps.

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-switching technology and circuit-switching technology. 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 scatter-net.

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 Web site provides numerous links to other Web sites with additional information.[38] The IEEE Web site provides updates on the IEEE 802.15 Working Group.[39] This is the Working Group that develops Personal Area Networking consensus standards for short distance wireless networks, or WPANs.

4.1.2 Frequency and Data Rates

The designers of Bluetooth like those of the 802.11 WLAN standard designed Bluetooth to operate in the unlicensed 2.4 GHz–2.4835 GHz 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

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

order to another channel for another 625 microsecond transmission; this process is repeated continuously. As stated previously, the ISM band has become popular for wireless communications because it is available worldwide and does not require a license.

In the ISM band, Bluetooth technology permits transmission speeds of up to 1 Mbps and achieves a throughput of approximately 720 kbps. Although the data rates are low compared to those of 802.11 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 the future.

4.1.3 Bluetooth Architecture and Components

As with the IEEE 802.11 standard, Bluetooth permits devices to establish either P2P networks or networks based on fixed access points with which mobile nodes can communicate. In this document, however, we only discuss the ad hoc network topology. 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 inter-networked 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.

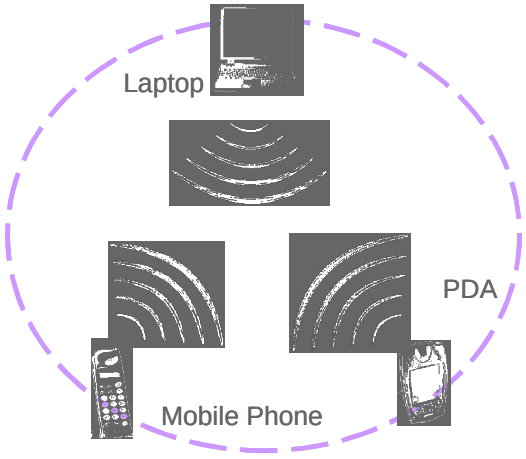

Figure 4-2. Bluetooth Ad Hoc Topology

Unlike a WLAN that comprises both a wireless station and an access point, with Bluetooth, there are only wireless stations or clients. 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

Bluetooth provides three different classes of power management. Class 1 devices, the highest power devices, operate at 100 milliwatt (mW) and have an operating range of up to 100 meters (m). Class 2 devices operate at 2.5 mW and have an operating range of up to 10 m. Class 3, the lowest power devices, operate at 1 mW and have an operating range of from 1/10 meter to 10 meters. These three levels of operating power are summarized in Table 4-2.

Table 4-2. Device Classes of Power Management

Type	Power	Power Level	Operating Range
Class 1 Devices	High	100 mW (20 dBm)	Up to 100 meters (300 feet)
Class 2 Devices	Medium	2.5 mW (4 dBm)	Up to 10 meters (30 feet)
Class 3 Devices	Low	1 mW (0 dBm)	0.1–10 meters (less than 30 feet)

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 100 m, or about 300 ft. Additionally, as with the data rates, it is anticipated that even greater distances will be achieved in the future.

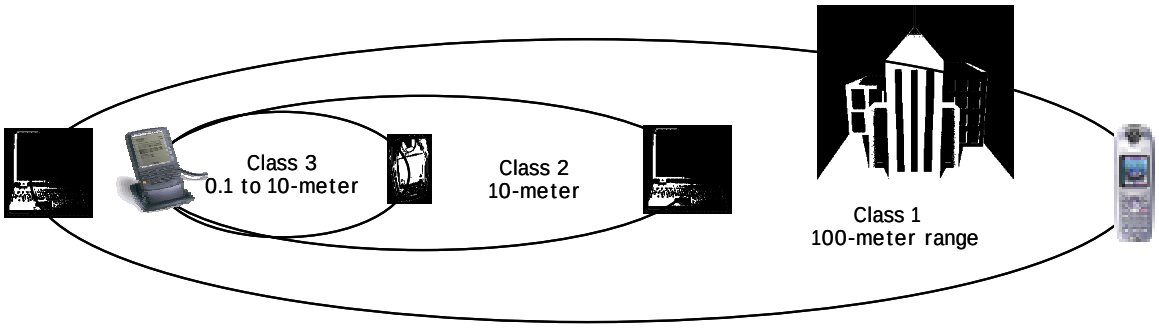

Figure 4-3. Bluetooth Operating Range

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 those of peripheral devices (i.e., mouse and keyboard computer connections), USB at 12 Mbps (USB 1.1) up to 480 Mbps (USB 2.0); printers and modems, usually at 4 Mbps; 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.[40]

- **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.

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

- **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 inbox of the laptop, the individual, once back in a service area (i.e., having landed), would activate a mobile phone or any other 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.

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

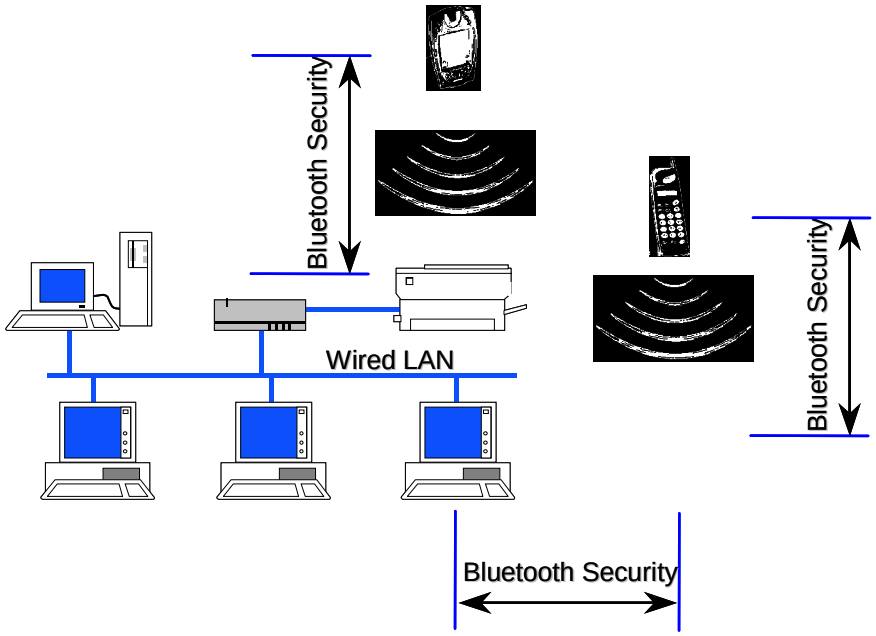

Figure 4-4. Bluetooth Air-Interface Security

As shown in the illustration, security for Bluetooth is provided on the various wireless links—on the radio paths only. In other words, link authentication and encryption may be provided, but true end-to-end

security is not possible without providing higher layer security solutions on top of Bluetooth. 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:

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

As with the 802.11 standard, Bluetooth does not address other security services such as audit and nonrepudiation. 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 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—that is the process of deciding if device A is allowed to have access to service X—is introduced.

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.

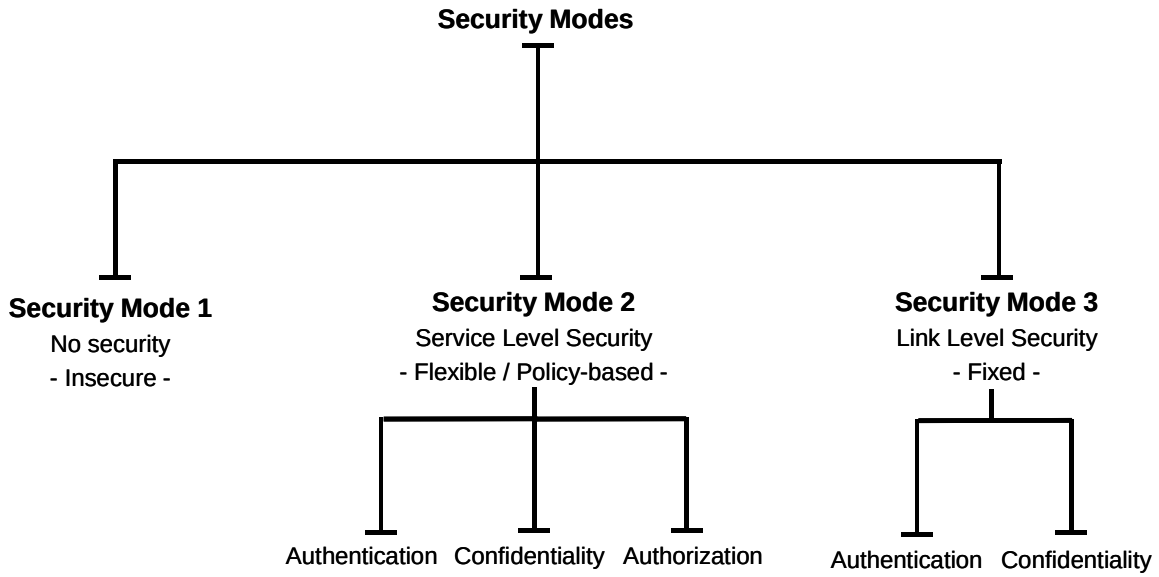

Figure 4-5. Taxonomy of Bluetooth Security Modes

4.3.1.1 Link Key Generation—Bluetooth Bonding

The link key is generated during an initialization phase, while 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 4-6. After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4-digit PIN may be sufficient for some applications; however, longer codes may be necessary.[41]

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

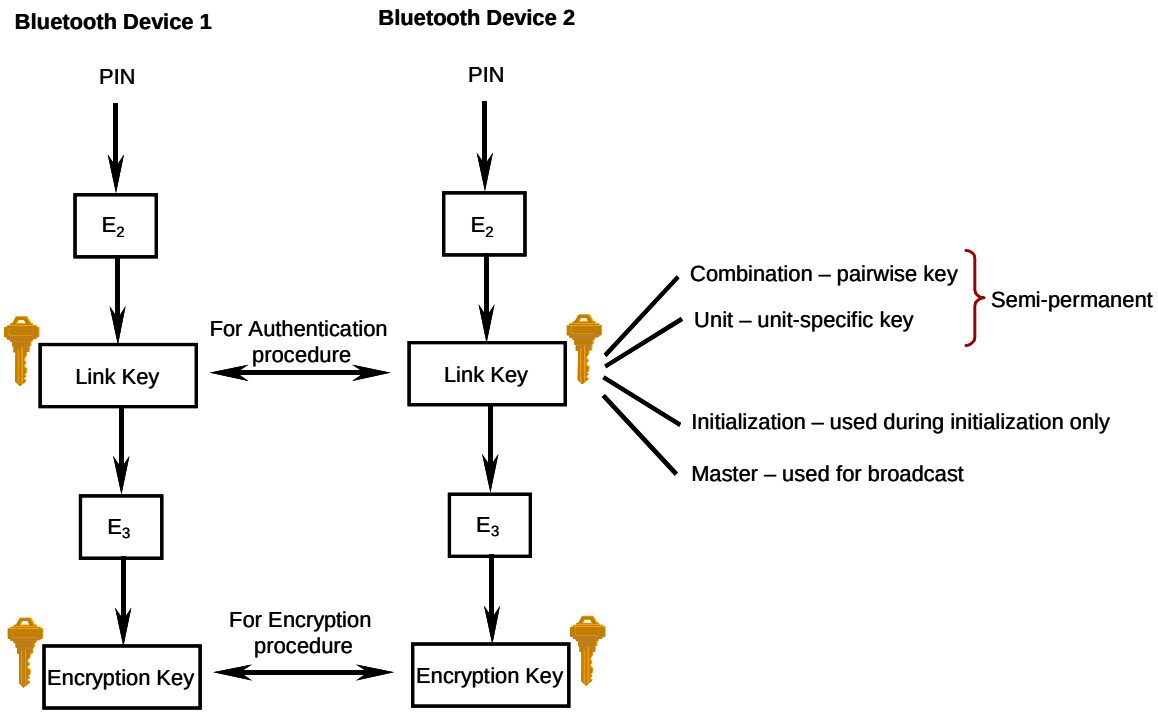

Figure 4-6. Bluetooth Key Generation from PIN

4.3.1.2 Authentication

The Bluetooth authentication procedure is in the form of a "challenge-response" scheme. Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The 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 4-7. As shown, one of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier).

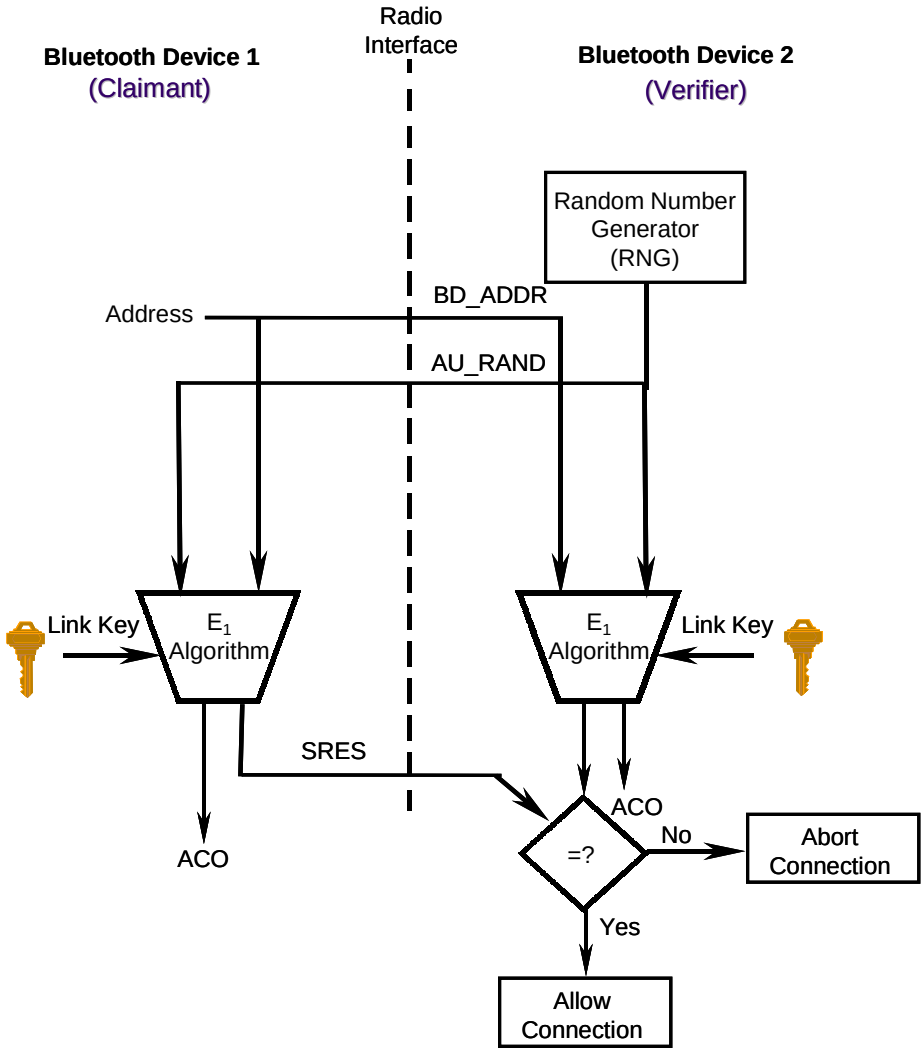

Figure 4-7. Bluetooth Authentication

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 E_1 authentication function used for the validation is based on the SAFER+ algorithm.[42]

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

4.3.1.3 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 in Figure 4-8, the Bluetooth encryption procedure is based on a stream cipher, E_0. A key stream output is exclusive-OR-ed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR).[43] 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 although the other variables remain static.

As shown in Figure 4-8, 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

[42] 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.

[43] 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.

cipher offset, is another output produced during the authentication procedure shown in Figure 4-7. 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.

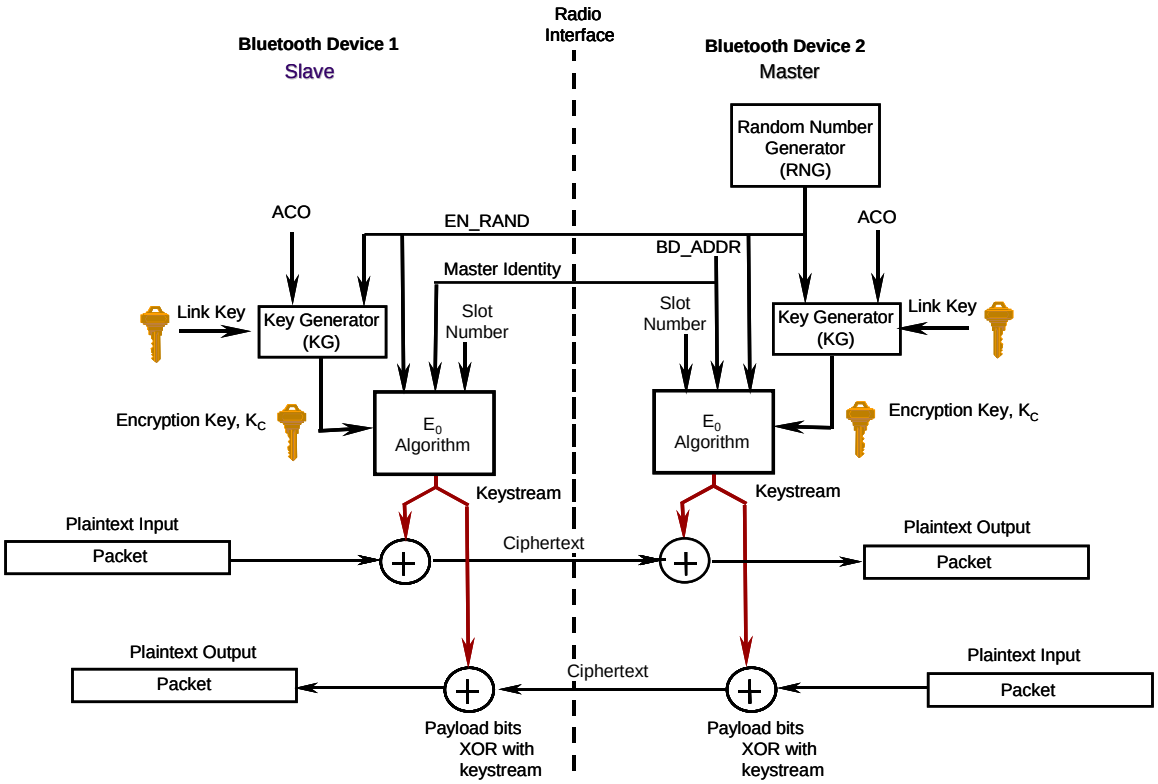

Figure 4-8. Bluetooth Encryption Procedure

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 devices 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, making 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 according to the individual link keys.
- **Encryption Mode 3**—All traffic is encrypted according to the master link key.

4.3.1.4 Trust Levels, Service Levels, and Authorization

In addition to the three security modes, Bluetooth allows two levels of trust and three levels of service security. The two 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 or Vulnerability	Remarks
1	**Strength of the challenge-response pseudo-random generator is not known.**	The Random Number Generator (RNG) may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
2	**Short PINS are allowed.**	Weak PINs, which are used for the generation of link and encryption keys, can be easily guessed. Increasing the PIN length in general increases the security. People have a tendency to select short PINs.
3	**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.
4	**Encryption key length is negotiable.**	The Bluetooth SIG needs to develop a more robust initialization key generation procedure.
5	**Unit key is reusable and becomes public once used.**	Use a unit key as input to generate a random key. Use a key set instead of only one unit key.

	Security Issue or Vulnerability	Remarks
6	**The master key is shared.**	The Bluetooth SIG needs to develop a better broadcast keying scheme.
7	**No user authentication exists.**	Device authentication only is provided. Application-level security and user authentication can be employed.
8	**Attempts for authentication are repeated.**	The Bluetooth SIG needs to develop a limit feature to prevent unlimited requests. The Bluetooth specification requires a time-out period between repeated attempts that will increase exponentially.
9	**E_0 stream cipher algorithm is weak.**	The Bluetooth SIG needs to develop a more robust encryption procedure.
10	**Key length is negotiable.**	A global agreement must be established on minimum key length.
11	**Unit key sharing can lead to eavesdropping.**	A corrupt user may be able to compromise the security between (gain unauthorized access to) 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, is disclosed.
12	**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.
13	**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.
14	**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.
15	**Security services are limited.**	Audit, nonrepudiation, 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, agencies 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, agencies need to address security concerns for confidentiality, data integrity, and network availability. Moreover, since Bluetooth devices are more likely to be managed by users that are less security conscious than administrators, they are more likely to contribute to involuntary security lapses. This subsection will briefly cover some of the risks to security, i.e., attacks on confidentiality, integrity, and network availability.

4.4.1 Loss of Confidentiality

See Figure 3.9 in the 802.11 wireless section for a general taxonomy of security attacks, to understand some of the attacks against Bluetooth.

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.[44]

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, incidents have been recorded 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 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 malicious user does not have to be in close proximity to the user to intercept traffic. 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. If in addition the malicious user obtains knowledge of the user IDs and password of the targeted network, then a compromised device can be used to gain access to the network. This scenario requires a number of security lapses before a malicious user can gain access to the network. Using Bluetooth secure links and additional layers of security on top of Bluetooth would mitigate the risk of such an attack.

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 that 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 reasons for the connections between Devices A and B and between Devices A and C may be completely unrelated, and the level of confidentiality may even be different. However, once Device C knows the unit key, it can use a fake device address to calculate the encryption key and monitor traffic between Devices A and B without their knowledge. The man-in-the-middle attack does not require costly or special equipment. 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

[44] 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/bluearticles/cc1_security1.asp for more information.)

Bluetooth devices as they enter the transmission range, no instances of such attacks have been documented.

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

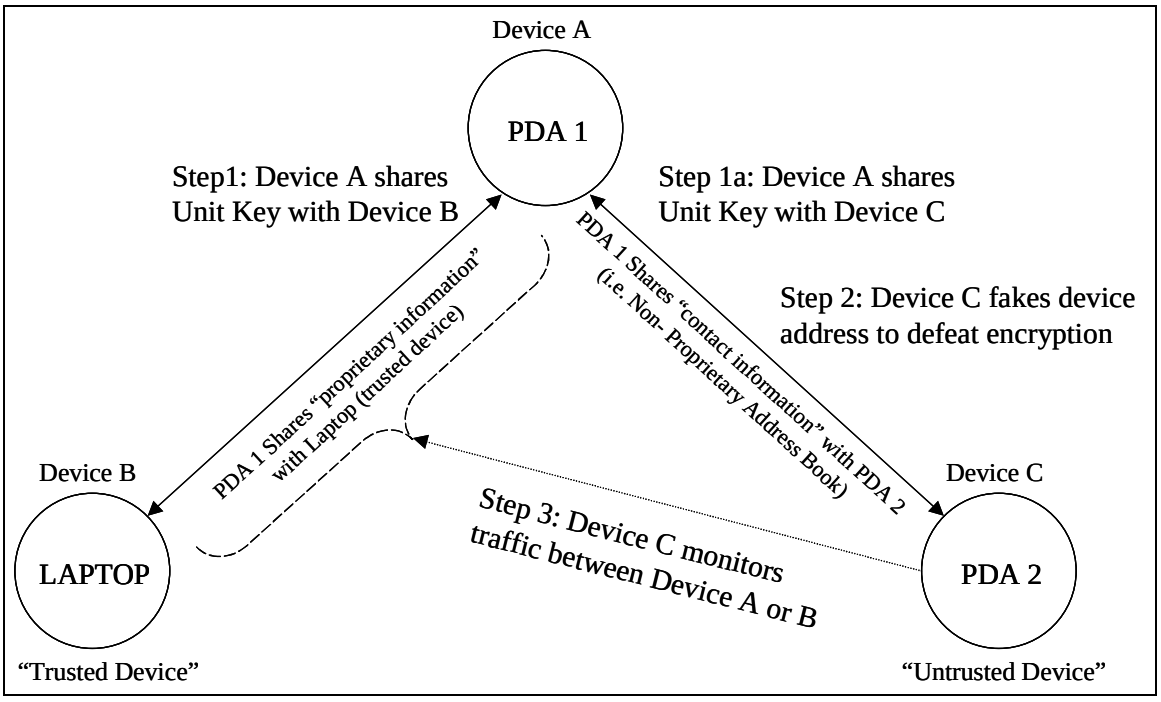

Figure 4-9. Man-in-the-Middle Attack Scenarios

To date, no software is available for monitoring such intrusions, and Bluetooth devices are invisible to network administrators.[45] 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. Since Bluetooth devices are unlikely to be administered by network administrators, users should be aware of the security implications of their use in environments that process sensitive data. Although privacy violations are not directly a security threat, agencies 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. Secure logging ensures device authentication (i.e., we have no proof who was operating the device, therefore, an individual can deny participation in the network since the address that is logged belongs to the device and not an individual). However, it also allows organizations to monitor and track what an individual does on the network.[46] Nonrepudiation of individuals requires strong authentication, such as client digital signatures that can be verified in a PKI (Public Key Infrastructure).

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

4.4.2 Loss of Integrity

Violations of integrity result from the corruption of an organization's 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's or network administrator's knowledge. Information that is subject to 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 agency (or user) losing confidence in its data and system. Users should verify that their Bluetooth product does not allow automatic data synchronization to prevent the alteration of any information without the acknowledgement of the device user.

4.4.3 Loss of Availability

DoS and DDoS attacks cause 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., those involving 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 2.4 GHz 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 on-site users. Remote users must contend with the same interference that users experience in the office. Further, 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.[47] 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. Agencies 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

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

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 agency'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 (with a class 3 device). Agencies that require both high levels of security and low levels of security should maintain a secure perimeter so that on-site network users can maintain secure connections in their office spaces. Agencies 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 security solutions 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. Again, it should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions.

4.5.3.1 Software Solutions

Software solutions inherent in Bluetooth technology include the Bluetooth PIN and private authentication. Bluetooth enforces Bluetooth PINs 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, in effect, 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 PIN 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 from a single device or use the Bluetooth PIN of both devices. Because the PINs are necessary for authentication and for link security, administrators should ensure that Bluetooth devices use PINs other than the default, or lowest, setting (e.g., 0000).

According to the Bluetooth specification, the Bluetooth PIN is not a value that comes with a device, except if fixed PINS are used. In this case, the fixed PIN must be used. This is a weak procedure, but it is allowed for devices that do not have a user interface. Normally, when two devices pair, they use the same PIN number, which is generated ad hoc and forgotten immediately afterwards and not used again. If two devices have different fixed PINs, they cannot pair.

Since Bluetooth devices can store and automatically access link-level PINs 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. Agencies with both high-end users 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 802.11 WLANs may be appropriate for Bluetooth devices as well. These software solutions are outlined in Section 3. Because Bluetooth is a relatively new wireless communications technology, supplemental software solutions (e.g., application security tool kits, 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 printer cable replacements, the enhanced security may be 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 that this is a 6-byte public parameter—serves several purposes such as generating 128-bit link keys and encryption keys. For example, a key-generating algorithm (defined by the Bluetooth standards) with a randomly generated number and the Bluetooth device address creates the unit and combination keys.

Link keys, the 128-bit random numbers that form the basis of Bluetooth security, are in the form of a unit key, a master link key, or a combination key. Only dumb devices use unit keys. More advanced devices establish combination keys with peers. Master devices generate master link keys that are transported to slaves protected by pair-wise link keys. 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, agencies 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. Even if the unit key of one of the devices is compromised, the link is still not compromised. The unit key and combination keys are functionally indistinguishable; the difference is merely in the ways 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 a great deal of electromagnetic interference occurs. 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. 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. Biometrics can be a part of a multi-factor authentication whereby the user is required to provide more than one form of authentication. Some devices that have Bluetooth applications, especially mobile phones and PDAs, already employ a form of voice authentication. Voice authentication can help agencies 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 related devices. Information on securing WLANs and devices, PDAs, and cell phones can be found in Sections 3 and 5.

Bluetooth is still a relatively new standard. Given that a number of vulnerabilities have been discovered, the standard is likely to continue to evolve and improve the built-in hardware security mechanisms. 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. Some of the hardware solutions outlined for 802.11 WLANs in Section 3 may also be appropriate for Bluetooth devices.

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 operating system, the device could connect to a network and immediately be shared by devices with different operating systems (e.g., Windows, Macintosh, and 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 has 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.

4.6 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 that this entry represents something recommended for all agencies. The second column, the “Should Consider” column, if checked, means that the entry’s recommendation is something that an agency should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the “Should Consider” column is checked, agencies should carefully consider the option and weigh the costs versus the benefits. The last column, the “Status” column, is intentionally left blank and allows an agency 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 agency, asking, “Have I done this?”

Table 4-5. Bluetooth Security Checklist

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1	Develop an agency security policy that addresses the use of wireless technology including Bluetooth technology.	✓		
2	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (i.e., Bluetooth).	✓		
3	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4	Perform comprehensive security assessments at regular intervals to fully understand the wireless network security posture.	✓		
5	Ensure that the wireless "network" is fully understood. With piconets forming scatter-nets with possible connections to 802.11 networks and connections to both wired and wireless wide area networks, an agency must understand the overall connectivity. Note: a device may contain various wireless technologies and interfaces.	✓		
6	Ensure external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
7	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8	Ensure that handheld or small Bluetooth devices are protected from theft.	✓		
9	Ensure that Bluetooth devices are turned off during all hours when they are not used.	✓		
10	Take a complete inventory of all Bluetooth-enabled wireless devices.	✓		
11	Study and understand all planned Bluetooth-enabled devices to understand any security idiosyncrasies or inadequacies.	✓		
Technical Recommendations				
12	Change the default settings of the Bluetooth device to reflect the agency's security policy.	✓		
13	Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency.	✓		
14	Ensure that 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).	✓		
15	Choose PIN codes that are sufficiently random and avoid all weak PINs.	✓		
16	Choose PIN codes that are sufficiently long (maximal length if possible).	✓		
17	Ensure that no Bluetooth device is defaulting to the zero PIN.	✓		
18	Configure Bluetooth devices to delete PINs after initialization to ensure that PIN entry is required every time and that the PINs are not stored in memory after power removal.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
19	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.		✓	
Operational Recommendations				
20	Ensure that combination keys are used instead of unit keys.	✓		
21	Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).	✓		
22	Ensure that encryption is enabled on every link in the communication chain.	✓		
23	Make use of Security Mode 2 in controlled and well-understood environments.	✓		
24	Ensure device mutual authentication for all accesses.	✓		
25	Enable encryption for all broadcast transmissions (Encryption Mode 3).	✓		
26	Configure encryption key sizes to the maximum allowable.	✓		
27	Establish a “minimum key size” for any key negotiation process.	✓		
28	Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.	✓		
29	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.		✓	
30	Use smart card technology in the Bluetooth network to provide key management.		✓	
31	Install antivirus software on intelligent, Bluetooth-enabled hosts.	✓		
32	Fully test and deploy software Bluetooth patches and upgrades regularly.	✓		
33	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.		✓	
34	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
35	Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
36	Designate an individual to track the progress of Bluetooth security products and standards (perhaps via the Bluetooth SIG) and the threats and vulnerabilities with the technology.		✓	
37	Wait until future releases of Bluetooth technology incorporate fixes to the security features or offer enhanced security features.		✓	

4.7 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 mitigations for securing the devices from these threats and vulnerabilities.

Table 4-6. Bluetooth Security Summary

	Security Recommendation	Security Need, Requirement, or Justification
1.	Develop an agency security policy that addresses the use of wireless technology including Bluetooth technology.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable implementations and uses for Bluetooth technology.
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., Bluetooth).	A security awareness program helps users to establish good security practices in the interest of preventing inadvertent or malicious intrusions into an organization's automated information system.
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	Understanding the value of organizational assets and the level of protection required enables the engineering of a wireless solution that provides an appropriate level of security.
4.	Perform comprehensive security assessments at regular intervals (including validating the secure configuration of Bluetooth technology) to fully understand the wireless network security posture.	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.
5.	Make sure the wireless "network" is fully understood. With piconets forming scatter-nets with possible connections to 802.11 networks and connections to both wired and wireless wide area networks, an agency must understand the overall connectivity. Note: a device may contain various wireless technologies and interfaces.	A thorough understanding of the functionalities and configurations of the deployed wireless network technologies allows an organization to identify possible risks and vulnerabilities. These risks and vulnerabilities can then be addressed in the wireless security policy and enforced appropriately.
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	To prevent malicious physical access to an organization's information system infrastructure, the external boundaries should be secured through means such as a fence or locked doors.
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	Identification badges or physical access cards should be deployed to ensure that only authorized personnel have physical access to a facility.
8.	Make sure that handheld and small Bluetooth devices are protected from theft.	The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
9.	Make sure that Bluetooth devices are turned off during all hours when they are not used.	Shutting down Bluetooth devices when not in use minimizes exposure to potential malicious activities.
10.	Take a complete inventory of all Bluetooth-enabled wireless devices.	A complete inventory list of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
11.	Study and understand all planned Bluetooth-enabled devices to understand the security implications.	An understanding of the security implications of Bluetooth will help the organization better address the associated risks.

	Security Recommendation	Security Need, Requirement, or Justification
12.	Change the default settings of the Bluetooth device to reflect the agency's security policy.	Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they are in compliance with the company security policy.
13.	Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency.	Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users.
14.	Ensure that the Bluetooth "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).	The key exchange is a vital security function and requires that users maintain a security awareness of possible eavesdroppers.
15.	Choose PIN codes that are sufficiently random and avoid all weak PINs.	PIN codes should be random so that it would not be easily guessed by malicious users.
16.	Choose PIN codes that are sufficiently long (maximal length if possible).	PIN codes with maximum lengths of 16 bytes make them more resistant to brute force attacks.
17.	Ensure that no Bluetooth device is defaulting to the zero PIN.	Bluetooth devices defaulting to the zero PIN (e.g., 0000) essentially provide no security.
18.	Configure Bluetooth devices to delete PINs after initialization, to ensure that PIN entry is required every time and that PINs are not stored in memory after power removal.	Requiring PIN entry after re-initialization prevents the possibility of a PIN being recovered from the memory of a stolen device.
19.	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.	The overhead associated with key exchange can be minimized by using an alternative protocol such as the Diffie-Hellman or certificate-based key exchange.
20.	Ensure that combination keys are used instead of unit keys.	The use of shared unit keys can lead to successful man-in-the-middle attacks.
21.	Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).	Link encryption should be used to secure all data transmissions during a Bluetooth connection.
22.	Make sure that encryption is enabled on every link in the communication chain.	Every link should be secured because one unsecured link results in compromising the entire communication chain.
23.	Use Security Mode 2 in controlled and well-understood environments.	Security Mode 2 provides authorized access to services.
24.	Ensure device mutual authentication for all accesses.	Mutual authentication is required to provide verification that all users and the network are legitimate.
25.	Enable encryption for all broadcast transmissions (Encryption Mode 3).	Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
26.	Configure encryption key sizes to the maximum allowable.	Using maximum allowable key sizes provides protection from brute force attacks.
27.	Establish a "minimum key size" for any key negotiation process.	Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks.
28.	Ensure that portable devices with Bluetooth interfaces are configured with passwords to prevent unauthorized access if lost or stolen.	Authenticating users to a portable Bluetooth device is a good security practice in the event the device is stolen, which provides a layer of protection for an organization's Bluetooth network.

	Security Recommendation	Security Need, Requirement, or Justification
29.	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.	Application-level encryption and authentication provide security on top of the Bluetooth link encryption; the overlay increases the security of communication.
30.	Use smart card technology in the Bluetooth network to provide key management.	The use of smart card technology can simplify the distribution and management of keys while maintaining strong security.
31.	Install antivirus software on intelligent, Bluetooth-enabled hosts.	Antivirus software should be installed on a Bluetooth-enabled host to insure that known worms and viruses are not introduced to the Bluetooth network.
32.	Fully test and deploy software Bluetooth patches and upgrades on a regular basis.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should be fully tested before implementation to ensure that they work.
33.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong authentication mechanisms can minimize the vulnerabilities associated with passwords and PINs.
34.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or network-based agents) deployed on the wireless network can detect and respond to potential malicious activities.
35.	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements prior to implementation.
36.	Designate an individual to track the progress of Bluetooth security products and standards (perhaps via Bluetooth SIG) and the threats and vulnerabilities with the technology.	An appointed individual designated to track the latest technology enhancements, standards (perhaps via Bluetooth SIG), and risks will help to ensure the continued secure use of Bluetooth.
37.	Wait until future releases of Bluetooth technology incorporate fixes to the security features or offer enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the Bluetooth products with major security vulnerabilities that have not been fixed.

5. Wireless Handheld Devices

Section 5 covers text-messaging devices, PDAs, and smart phone—PDA products because these are the devices most commonly used by the mobile work force 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. However, network administrators can 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. Instead they have become indispensable tools and competitive business advantages for the mobile work force. The use of these devices introduces new security risks to an agency's existing network. Moreover, as these devices begin having their own IP addresses, the devices themselves can become the targets of attacks. Handheld devices have different capabilities and different uses from those of desktop and laptop computers. The differences between handheld devices and desktop and laptop computers that affect the agency's security are summarized below.

- The small size, relatively low cost, and constant mobility of handheld devices 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 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 the 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.
- Handheld device users can download a number of productivity programs, connectivity programs, games, and utilities—including freeware and shareware programs—from untrusted sources. The programs can be easily installed without network administrators being notified. 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. However, as networked PDAs become more affordable and more popular, vendors are beginning to offer more stand-alone and enterprise security solutions.
- Users often subscribe to third-party Wireless Internet Service Providers (WISP) 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 they have 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 they 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 for accessing e-mail, agency 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.

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 work force. 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 network connectivity 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 introduce new security risks to an agency'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 security requirements for confidentiality, integrity, authenticity, and availability 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, or the PC or while being sent over one of the Bluetooth, 802.11, IR, USB, or serial communication ports. Moreover, most handheld devices are shipped with connectivity that is enabled by default. These default configurations are typically not in the most secure setting and should be changed to match the agency's security policy before being used.

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 some concerns might arise 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 often within a few inches. Nonetheless, agencies should not overlook the threat because it could result in a compromise of sensitive information. No attack has been documented 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. However, a Bluetooth device that is not configured properly is susceptible to having a user with a Bluetooth-enabled device pull data from the 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; 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.[48] 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

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

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 agency. Modem-enabled PDAs are still relatively new, and an agency may not have the security services in place to support them. Agencies 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 work space. The data that crosses the network is as secure as the network itself and may be susceptible to network traffic analyzers or sniffers. PDA users can also synchronize through their agency's wireless network. This entails accessing the agency's 802.11-compliant APs to connect to the agency's wired network. Many PDA vendors support or are beginning to support VPN connections using 802.11 APs.

Analog phones using first generation (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, many 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. Digital cellular telephones may also be vulnerable to eavesdropping, but the equipment required to eavesdrop on a digital cellular telephone is much more expensive. TDMA and GSM offer built-in encryption, but its use is at the discretion of the cellular service provider.

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.[49] 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.

Security officers and administrators must also be aware of the threats posed by visitors carrying handheld devices. Many wireless sniffing tools run on handheld devices that can be used by malicious users to help them gather information that might be useful in a future attack. Moreover, many handheld devices come equipped with audio and video recording capabilities that can be used to record sensitive conversations or records images of people or facilities. As the handheld devices become smaller and more capable, some

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

agencies should consider not allowing users to bring handheld devices into their facilities if they pose a potential security risk.

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 applications 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 to 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 already support the use of personal firewalls to protect themselves against certain DoS attacks and other types of 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.[50] 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.[51] 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. However, a virus on a handheld device 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.

---

50 See SP 800-28, *Guidelines on Active Content and Mobile Code*, October 2001, for more information on malware.

51 See *PDA/Wireless Communication Pains*, November 17, 2000, at http://www.sans.org.

Smart phones may lose network connectivity not only when they travel outside a cell coverage area but also when cell phone jammers are used. Many restaurants and movie theaters, for example, now use commercially available jammers to block cell phone communications often without notifying the cell 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 nullify 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., 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, by visiting Web sites that allow users to send text messages free of charge from e-mail applications. Text-messages rely on the service provider's network and are not encrypted, and no guarantees exist 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, agencies 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, agencies need to implement management, operational, and technical countermeasures to safeguard handheld devices and the agency's networks.

5.4.1 Management Countermeasures

Information security officers and network administrators should conduct a risk assessment before handheld devices are introduced into the agency's computing environment. The agency should educate the 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.[52] The policy document should include the approved uses, the type of information that the devices 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. Agencies should also perform random audits to track whether devices have been lost or stolen.

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

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 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 agency's operational countermeasures should make clear the user's responsibilities.

The back of the PDA device should always be labeled with the owning agency'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. Although these measures cannot ensure that a determined thief will not cut these cables or locks, it does prevent an opportunistic thief from walking away with an unattended handheld device. While on travel, room safes should be used, if available, to store handheld devices when not in use.

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 agency's security policy or be restricted from accessing the agency's network. Handheld devices should be distributed to the users with security settings that comply with the agency's security policy and should not be distributed with "out-of-the-box" default settings. A configuration management policy should be established. 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 agency. 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.[53]

In general, users should not store sensitive information on handheld devices. However, if sensitive information is stored on the handheld device, users should be encouraged to delete sensitive information 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 can be read directly from memory.

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

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 agency's security policy is being enforced. As noted in the 802.11 and Bluetooth sections, hardware solutions, which generally have software components, are listed simply as hardware solutions.

5.4.3.1 Authentication

Identification and authentication (I&A) form 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 providing a password, a token, or both. At the most basic level, agencies 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.[54] Password protection is already included with most handheld devices, but is usually not enabled in the default setting. Several Web sites offer software that prompts a user to enter a password when the user has turned the PDA off and turned it back on again.[55] 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 a signature, which is more widely available on paper documents distributed in the normal course of business.

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 passwords 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 Web sites, to 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

---

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

55 The following Web sites 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.

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. However, many PDA users store many of these passwords in a file on the PDA, possibly even naming the file "mypasswords." Once a single password has been given, other user accounts can be identified through various 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. Many software programs are freely available to help users encrypt these types of files for an added layer of security. However, if the data is sensitive, the encryption implementation should be FIPS140-2 validated. Encrypting the file protects it 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 (Forward Error Correction) coding and spread-spectrum techniques add more robust communication error protection and complexity. Agencies 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.[56] All agencies, 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 agency 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 current, properly working virus-scanning software. Most major PC antivirus software vendors have handheld device antivirus software that can be downloaded directly from their Web sites.

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.[57] 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 claimed 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 agency's security requirements. If PKI has already been deployed to provide security services in the wired network of an agency, users

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

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

should be provided a separate and distinct public/private key pair for use on PDAs. This will prevent compromise of the enterprise data in the event of a lost or stolen PDA.

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.[58] Handheld devices are beginning to offer support for personal firewalls and VPN technologies and to 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 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 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. Enterprise security solutions have been introduced that allow the organization to set policies on all handheld devices under the organization's control. Some of the options that are available include defining the type of encryption to use, which application databases to encrypt, password protection, and port protection.

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. The user can usually set this time-out period. 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.

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

5.5 Case Study: PDAs in the Workplace

Agency C is considering purchasing PDAs for its 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 agency's users do not appreciate the implications of losing a PDA and the loss of sensitive agency 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 that 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, risks still exist with the fast pace of PDA evolution and the likelihood that malicious users will try to exploit any new or existing vulnerability. Agency C determines that the operational benefits outweigh the residual risks of the PDAs and moves forward with the purchase.

Agency C considers the protection of sensitive 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, Agency 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 employees also need to update the agency's database from the field and to access their e-mail. It is decided that access to corporate resources will be through a VPN.

Before issuing the PDAs to its employees, the security department ensures that the default settings of the Bluetooth cards are changed to comply with the agency'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 5 minutes of inactivity on all the PDAs. The security team labels the devices and issues them 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 Wireless Handheld Device Security Checklist

Table 5-1 provides a security checklist for PDAs and smart phones. The 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 that the entry represents something recommended for all agencies. The second column, the "Should Consider" column, if checked, means that the recommendation is something that an agency should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some sort of additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the "Should Consider" column is checked, agencies need to carefully consider the option and weigh the costs versus the benefits. The last column, the "Status" column, is intentionally left blank and allows an agency 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 agency wireless environment, asking, "Have I done this?"

Table 5-1. Wireless Handheld Device Security Checklist

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Control				
1.	Develop an agency security policy that addresses the use of all handheld devices.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with handheld devices.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Conduct ongoing, random security audits to monitor and track devices.	✓		
5.	Ensure that external physical boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
6.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
7.	Minimize the risk of loss or theft through the use of physical locks and cables.		✓	
8.	Label all handheld devices with the owner and agency's information.	✓		
9.	Ensure that users know where to report a lost or stolen device.	✓		
10.	Ensure that devices are stored securely when left unattended.	✓		
11.	Make sure that add-on modules are adequately protected when not in use to prevent against theft.	✓		
12.	Enable a “power-on” password for each handheld device.	✓		
13.	Ensure proper password management (aging, complexity criteria, etc.) for all handheld devices.	✓		
14.	Ensure that desktop application-mirroring software is password-protected.	✓		
15.	Store data on backup storage modules in encrypted form.		✓	
16.	Review vendor Web sites frequently for new patches and software releases.	✓		
17.	Install patches on the affected devices and workstations.	✓		
18.	Review security-related mailing lists for the latest security information and alerts.	✓		
19.	Ensure that all devices have timeout mechanisms that automatically prompt the user for a password after a period of inactivity.	✓		
20.	Synchronize devices with its corresponding PC regularly.	✓		
21.	Avoid placing sensitive information on a handheld device. If necessary to do so, delete sensitive data from the handheld device and archive it on the PC when no longer needed on the handheld.	✓		
22.	Turn off communication ports during periods of inactivity when possible.	✓		
23.	Install antivirus software on all handheld devices.	✓		
24.	Install personal firewall software on all networked handheld devices.		✓	

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Technical Control				
25.	Ensure that PDAs are provided with secure authorization software/firmware.		✓	
26.	Install VPN software on all handheld devices that transmit data wirelessly.		✓	
27.	Ensure that a user can be securely authenticated when operating locally and remotely.	✓		
28.	Use robust encryption and password protection utilities for the protection of sensitive data files and applications.	✓		
29.	Use enterprise security applications to manage handheld device security.		✓	
30.	Ensure that security assessment tools are used on handheld devices.		✓	
31.	When disposing handheld devices that will no longer be used by the agency, clear configuration settings to prevent the disclosure of sensitive network information.	✓		

5.7 Handheld Device Risk and Security Summary

Table 5.2 lists security recommendations for handheld devices. For each recommendation, narrative is provided that addresses the security need, requirements or justification for that rcommendation.

Table 5-2. Handheld Device Security Summary

	Security Recommendation	Security Need, Requirement, or Justification
1.	Develop an agency security policy that addresses the use of all handheld devices.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable implementations and uses for handheld devices.
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with handheld devices.	A security awareness program helps users to establish good security practices in the interest of preventing inadvertent or malicious intrusions onto an organization's automated information system.
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	The risk assessment can help the organization identify and determine the value of their information system and data assets, thus allowing the organization to allocate the appropriate level of resources for protection of those systems and assets.
4.	Conduct ongoing, random security audits to monitor and track devices.	Security policy enforcement is vital for ensuring that only authorized handheld wireless devices are operating in compliance with the organization's wireless security policy. Random security audits provide a realistic view of the security environments.
5.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	To prevent malicious physical access to an organization's information system infrastructure, the external boundaries should be secured through means such as a fence or locked doors.

	Security Recommendation	Security Need, Requirement, or Justification
6.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	Identification badges or physical access cards should be deployed to ensure that only authorized personnel have physical access to a facility.
7.	Minimize the risk of loss or theft through the use of physical locks and cables.	As with any portable device, use physical locks and cables to minimize the risk of loss or theft.
8.	Label all handheld devices with the owner's and agency's information.	As with any portable device, label all handheld devices with the appropriate owner and agency information.
9.	Ensure that users know where to report a lost or stolen device.	As with any portable device, a label should be on the device indicating how it can be returned to the rightful owner.
10.	Ensure that devices are stored securely when left unattended.	Handheld devices should be stowed in locked rooms and cabinets especially when left unattended for long periods such as a night.
11.	Ensure that add-on modules are adequately protected when not in use to prevent against theft.	Add-on modules are sometimes as much a target as the primary handheld device. So, it too should also be secured from risk of theft.
12.	Enable a "power-on" password for each handheld device.	Requiring user authentication helps prevent unauthorized device access and potential theft of data.
13.	Ensure proper password management (aging, complexity criteria, etc.) for all handheld devices.	Proper password management helps to ensure security of devices and data contained.
14.	Ensure that desktop application mirroring software is password protected.	Unauthorized access to all handheld components and related software should be prevented through the use of passwords and encryption where feasible.
15.	Store data on backup storage modules in encrypted form.	In case the backup storage is stolen, the information should be stored encrypted.
16.	Fully test and deploy software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.
17.	Install patches on the affected devices and workstations.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patching peripheral devices and workstations related to the handheld device will minimize the risk of attack. Patches should also be fully tested before implementation to ensure that they work.
18.	Review security-related mailing lists for the latest security information and alerts.	Proactively search reports on newly discovered wireless handheld risks and vulnerabilities.
19.	Ensure that all devices have timeout mechanisms that automatically prompt the user for a password after a period of inactivity.	Time-out mechanisms requiring the user to login after a period of inactivity should be implemented to protect them from inadvertent or malicious activities of third-party users.
20.	Synchronize devices with their corresponding PCs regularly.	Synchronization of handheld devices with their corresponding PCs ensures data availability.
21.	Avoid placing sensitive information on a handheld device. If necessary to do so, delete sensitive data from the handheld device and archive it on the PC when no longer needed on the handheld.	Because of the portability of handheld devices and greater threat to loss and theft, sensitive information stored on the device should be off-loaded to the PC and deleted form the handheld device, if possible.
22.	Turn off communication ports during periods of inactivity when possible.	Turning off unused communication ports minimizes the risk of malicious access.

	Security Recommendation	Security Need, Requirement, or Justification
23.	Install antivirus software on all handheld devices.	Antivirus software ensures that the handheld device does not introduce known worms and viruses to the wired network. Also, the handheld device is protected from its communicating hosts.
24.	Install personal firewall software on all networked handheld devices.	The handheld device is a potential target for malicious users.
25.	Ensure that PDAs are provided with secure authorization software/firmware.	Only secured authorization software and firmware should be used with the PDA.
26.	Install VPN software on all handheld devices that transmit data wirelessly.	All wireless communication, if possible, should use strong cryptography, have robust key management, and have strong user authentication.
27.	Ensure that a user can be securely authenticated when operating locally or remotely.	Users should be required to authenticate when operating locally and remotely.
28.	Use robust encryption and password protection utilities for the protection of sensitive data files and applications.	Sensitive data and application data files should be encrypted with the appropriate encryption techniques.
29.	Use enterprise security applications to manage handheld device security.	Handheld devices should also be managed by enterprise security applications.
30.	Ensure that security assessment tools are used on handheld devices.	Handheld devices should undergo security assessments to identify security vulnerabilities.
31.	When disposing handheld devices that will no longer be used by the agency, clear configuration settings to prevent the disclosure of sensitive network information.	Sensitive or proprietary configuration settings should be cleared to prevent inadvertent disclosure of the information to potentially malicious users.

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 (174 MHz–220 MHz) Garage door openers (~40 MHz) Standard cordless telephones (40 MHz–50 MHz) Alarm Systems (~40 MHz) Paging Systems (50 MHz–300 MHz)
UHF: Ultra High Frequency	300 MHz–3 GHz	Paging systems (300 MHz–500 MHz) 1G mobile telephones (824 MHz–829 MHz) 2G mobile telephone (800 MHz–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 (2.4-2.4835 GHz) Home RF (2.4 GHz ISM Band) WLAN (2.4, 5 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 to 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

Advanced Encryption Standard (AES)	The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies.
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-OR-s each plain-text 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 Configuration 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, his/her 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) 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 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.
Wired Equivalent Privacy (WEP)	Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

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 Communications
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
RSN	Robust Security Networks
SIG	Special Interest Group
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRES	Signed Response
SSH	Secure Shell
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 Layer 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
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
WWAN	Wireless Wide Area Network
WPAN	Wireless Personal Area Networks
WPA	Wi-Fi Protected Access

Appendix D—Summary of 802.11 Standards

Table D-1 provides a summary of the various 802.11 standards. For each of the eight standards, a description of the standard, purpose keywords and remarks about the standard, and when the standard and products will be available are provided.

Table D-1. Summary of 802.11 Standards

Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11a	A physical layer standard in the 5 GHz radio band. It specifies eight available radio channels (in some countries, 12 channels are permitted). The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the radio access point increases.	**Higher Performance.** In most office environments, the data throughput will be greater than for 11b. Also, the greater number of radio channels (eight as opposed to three) provides better protection against possible interference from neighboring access points. Conformance is shown by a Wi-Fi5 mark from WiFi Alliance.	Standard was completed in 1999. Products are available now.
802.11b	This is a physical layer standard in the 2.4 GHz radio band. It specifies three available radio channels. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the radio access point increases.	**Performance.** Products are in volume production with a wide selection at competitive prices. Installations may suffer from speed restrictions in the future as the number of active users increase, and the limit of three radio channels may cause interference from neighboring access points.	Standard was completed in 1999. A wide variety of products have been available since 2001.
802.11d	This standard is supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use.** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	Work is ongoing, but see 802.11h for a timeline on 5 GHz WLANs in Europe.

Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11e	This standard is supplementary to the MAC layer to provide QOS support for LAN applications. It will apply to 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QOS for data, voice, and video applications.	**Quality of service.** This standard should provide some useful features for differentiating data traffic streams. It is essential for future audio and video distribution. Many WLAN manufacturers have targeted QOS as a feature to differentiate their products, so there will be plenty of proprietary offerings before 11e is complete. This standard will be greatly affected by the work of Tgi.	The finalized standard is expected in the second half of 2002. Products will be available in the second half of 2003 or later.
802.11f	This is a "recommended practice" document that aims to achieve radio access point interoperability within a multivendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.	**Interoperability.** This standard will work to increase vendor interoperability. Currently few features exist in the AP work. 802.11f will reduce vendor lock-in and allow multivendor infrastructures.	Completed standard is expected in the second half of 2002. Products will be available in the first half of 2003 or later.
802.11g	This is a physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is 54 Mbps per channel whereas 11b has 11 Mbps. The 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Performance with 802.11b backward compatibility.** Speeds similar to 11a and backward compatibility may appear attractive but modulation issues exist: Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group compromised by including both types of modulation in the draft standard. With the addition of support for 11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late, and too complex relative to 11a. However, advantages exist for vendors hoping to supply dual-mode 2.4 GHz and 5 GHz products, in that using OFDM for both modes will reduce silicon cost. If 802.11h fails to obtain pan-European approval by the second half of 2003, then 11g will become the high-speed WLAN of choice in Europe.	Completed standard is expected in the second half of 2002. Products will be available in the first half of 2003 or later.

Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11h	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance.** This is necessary for products to operate in Europe. Completion of 11h will provide better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by ETSI. Although European countries such as the Netherlands and the United Kingdom are likely to allow the use of 5 GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003 or later.	The standard is expected to be finalized by the second half of 2002. Products will be available in the first half of 2003 (firmware implementation), with high availability in the second half of 2003.
802.11i	This standard is supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b, and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of 802.11i.	**Improved security.** Security is a major weakness of WLANs. Vendors have not improved matters by shipping products without setting default security features. In addition, the numerous Wired Equivalent Privacy (WEP) weaknesses have been exposed. The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2003. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility.	Finalization of the TKIP protocol standard is expected to occur in the second half of 2002. Firmware will be available in the first half of 2003. New silicon with an AES cipher is expected to occur by the second half of 2003 or later.

Appendix E—Useful References

Name	URL	Description / Remarks
802.11 Planet	http://http://www.80211-planet.com	Source for WiFi business and technology information
802.11b Networking News	http://80211b.weblogger.com	News and features about the 802.11b networking standard
Air Defense	http://www.airdefense.net/products/index.shtm	This site contains lists of many of the major security products by category.
Air Jack Site	http://802.11ninja.net	Air Jack code and slides from wireless presentation at the 2002 BlackHat Briefings
AirSnort	http://airsnort.shmoo.com	AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys.
AirTraf	http://airtraf.sourceforge.net	AirTraf is a wireless 802.11 network sniffer.
Cellular Network Perspectives	http://www.cnp-wireless.com	Source of technical information about wireless standards and technology
Cellular Telecommunications & Internet Association	http://www.wow-com.com	Cellular Telecommunications & Internet Association Web site
Cquire.net	http://www.cqure.net/tools08.html	This is a link to the WaveStumbler wireless network mapping tool.
Dachb0den Labs	http://www.dachb0den.com/projects/bsd-airtools.html	Wireless BSD tools
Federal Communications Commission	http://www.fcc.gov	Federal Communications Commission web site
Globecom Site	http://www.globecom.net/ietf	This site allows the search of Internet Engineering Task Force documents.
Guidance	http://www.amc.army.mil/amc/ci/matrix/guidance/guidance3_mainpage.htm	This is a military site with many URLs to various publications.
IEEE	http://standards.ieee.org/getieee802	IEEE 802.11 site
JM Projects	http://www.jm-music.de/projects.html	Link to Wavemon, a monitoring application for wireless network devices. Wavemon currently works under Linux with devices that are supported by the wireless extensions by Jean Tourrilhes (included in Kernel 2.4 and higher), e.g., the Lucent Orinoco cards.
Kismet	http://www.kismetwireless.net	Kismet wireless network sniffer site
Mognet	http://chocobospore.org/mognet	Mognet is a free, open source wireless Ethernet sniffer/analyzer written in Java.
Netstumbler.com	http://www.netstumbler.com	Netstumbler 802.11 discovery tool
Prisimstumbler	http://prismstumbler.sourceforge.net	Prismstumbler is a wireless LAN (WLAN) that scans for beacon frames from access points. Prismstumbler operates by constantly switching channels and monitors any frames received on the currently selected channel.

Name	URL	Description / Remarks
Sniffer technologies	http://www.sniffer.com/products/wireless/default.asp?A=5	Sniffer® Wireless was designed in accordance with the IEEE 802.11b interoperability standard. It includes network monitoring, capturing, decoding, and filtering—all of the standard Sniffer® Pro features.
Snort	http://www.snort.org	Snort is an open source intrusion detection system.
Sonar-Security	http://www.sonar-security.com	StumbVerter is a standalone application that allows users to import Network Stumbler's summary files into Microsoft's MapPoint 2002 maps.
Sourceforge.net	http://sourceforge.net/projects/wifiscanner	Link to a passive 802.11b scanner
Talisker Network Security	http://www.networkintrusion.co.uk/wireless.htm	Wireless security tools
Talisker Network Security	http://www.networkintrusion.co.uk	This is a independent site that maintains an extensive list of current security products.
WEPcrack	http://wepcrack.sourceforge.net	WEPCrack is an open source tool for breaking 802.11 WEP secret keys.
WiFi	http://www.wi-fi.com/OpenSection/index.asp	WiFi Web site
WildPackets	http://www.wildpackets.com/products/airopeek	This is a link to WildPackets' wireless protocol analyzer, Airopeek.
Wireless LAN Association	http://www.wlana.com	WLANA provides a clearinghouse of information about wireless local area applications, issues, and trends and serves as a resource for customers and prospective customers for wireless local area products and wireless personal area products and for industry press and analysts.

Appendix F—Wireless Networking Tools

Tool	Capabilities	Website	Linux{ XE "Linux" }/Unix{ XE "Unix" }	Win32	Cost
Aerosol{ XE "Aerosol" }	Wireless Sniffer	http://www.sec33.com/sniph/aerosol.php		✓	Free
	Aerosol{ XE "Aerosol" } is a freeware{ XE "freeware" } wireless LAN{ XE "LAN" } sniffer tool, which can also crack WEP encryption keys. Aerosol operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.				
AirSnort{ XE "AirSnort" }	Wireless Sniffer	http://airsnort.shmoo.com/	✓		Free
	AirSnort{ XE "AirSnort" } is a freeware{ XE "freeware" } wireless LAN{ XE "LAN" } sniffer tool, which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.				
Kismet{ XE "Kismet" }	Wireless Sniffer	http://www.kismetwireless.net/	✓		Free
	Kismet{ XE "Kismet" } is an 802.11b{ XE "802.11b" } wireless network sniffer{ XE "network sniffers" }. It is capable of sniffing using almost any wireless card supported in Linux{ XE "Linux" }.				
Netstumbler	Wireless Sniffer	http://www.netstumbler.com		✓	Free
	Netstumbler is a 802.11b tool that listens for available networks and records data about that access point. A version is available for the Pocket PC.				
Sniffer Wireless{ XE "Sniffer Wireless" }	Wireless Sniffer	http://www.sniffer.com/		✓	$
	A Sniffer Wireless{ XE "Sniffer Wireless" } is a commercial wireless LAN{ XE "LAN" } sniffer that provides network monitoring, capturing, decoding, and filtering capabilities.				
WEPCrack{ XE "WEPCrack" }	WEP encryption cracker	http://sourceforge.net/projects/wepcrack/	✓		Free
	WEPCrack{ XE "WEPCrack" } is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.				
WaveStumbler{ XE "WaveStumbler" }	Wireless Network Mapper	http://www.cqure.net/tools08.html	✓		Free
	WaveStumbler{ XE "WaveStumbler" } is a freeware{ XE "freeware" } console based 802.11 network mapper for Linux{ XE "Linux" }. It reports the basic wireless network characteristics including channel, WEP, ESSID, MAC etc.				

Appendix G—References

Print Publications and 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, *Guidelines on Firewalls and Firewall Policy*, January 2002.

4. Gast, M. *802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks*, O'Reilley Publishing, April 2002.

Articles and Other Published Material

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

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

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

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

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

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

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

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

12. 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.

13. 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." *Information Week*, (www.informationweek.com), December 2001.

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

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

16. 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://www.drizzle.com/~aboba/IEEE/ (Unofficial 802.11 security Web site)
3. http://its.med.yale.edu/computing_services.html (Yale University School of Medicine provides information on wireless applications and future uses)
4. http://xforce.iss.net (X-Force Web site provides information on leading computer threats and vulnerabilities)
5. http://www.cisco.com (Cisco Web site provides information on securing wireless networks)
6. http://www.computeruser.com/resources/dictionary/dictionary.html (reference for technical terms)
7. http://www.computerworld.com (provides white papers, surveys, and reports related to security of wireless networks)
8. http://www.eet.com (technical Web site that serves as a primer for different technologies and applications)
9. http://www.gcn.com (*Government Computer News* provides up-to-date information on wireless and mobile devices and their related security issues)
10. http://www.informationweek.com (provides information on wireless networks, wireless communications, and security solutions in the form of articles and other documents)
11. http://www.infosecuritymagazine.com (provides white papers, surveys, and reports on wireless network security)
12. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (University of California at Berkeley provides "frequently asked questions" on WEP setup, problems, and attacks)
13. http://www.networkcomputing.com (provides white papers, surveys, and reports on wireless network security)
14. http://www.nwfusion.com (Network World Fusion Web site provides white papers, surveys, and reports on wireless network security)
15. http://www.pdadefense.com (PDADefense Web site provides articles and guidance on PDA security)
16. http://www.sans.org/newlook/home.htm (SANS Institute Web site maintains articles, documents, and links on computer security and wireless technologies)

17. http://www.scmagazine.com (*SC Magazine* Web site, an information security online magazine provides information on wireless security issues)

18. http://www.zdnetindia.com (*ZDNet India Magazine* Web site provides white papers, surveys, and reports on wireless network security)