# Global Information Assurance Certification Paper

**Understanding Wireless LAN Technology and its Security Risks**

Julie Schuller

GIAC Security Essentials Certification (GSEC) v1.4b

March 31, 2003

Abstract

Wireless technology is a significant, emerging technology that is certain to play an ever-increasing role in the network environment. According to an article published by SC Infosecurity News, "Half of senior IT security managers recently surveyed by IT security provider Defcom said they are looking to deploy a WLAN system within the next 12 months [1]." Many private businesses and government agencies are attracted to wireless local area networks (WLANs) for the mobility they offer workers, as well as convenience and rapid installation. However, putting these favorable benefits aside, WLAN technology used alone without proper security measures can provide an open door for anyone with a laptop, antenna, and appropriate software to infiltrate a network.

This paper will attempt to explain wireless LAN technology, what it is and how it is used, as well as identify the security issues that accompany the technology. The intent is to provide a comprehensive overview of the technology in order to educate and familiarize readers with the benefits and drawbacks of WLANs and the measures that should be implemented to secure them.

What is a Wireless LAN (WLAN)?

WLANs are very similar to traditional wired LANs, except with WLANs, authorized users do not need hard-wired connections such as a RJ-45 ports to access the network. WLANs use radio waves to send and receive data through the air, reducing the need for wired connections that are a necessity in traditional wired LANs.

WLAN technology was first introduced by researchers at the University of Hawaii in 1971 when they constructed a packet based radio communications network called ALOHNET. The first WLAN consisted of seven computers that connected four of the Hawaiian Islands [2]. In the late 1980s, WLAN technology began to emerge and was initially viewed as a cheaper alternative to traditional wired LANs in that it eliminated the need to hard wire buildings. Today, mobility and convenience are the primary reasons that wireless is becoming more widely used, providing anywhere, anytime network connectivity.

How WLAN Technology Works

WLANs predominately use spread spectrum technology to transmit and send data through the air; similar to the way a radio receives signals from a broadcaster. Infrared (IR) technology is also used in WLANs but on a smaller scale. WLAN speeds can range from 1 Mbps found in the original IEEE 802.11 standard up to 54 Mbps that is typical for the more current 802.11a standard. The range for typical WLAN systems varies from approximately 150 feet indoors to 1,500 feet outdoors. Coverage can be extended to several miles through microcells (similar to the cell architecture used by cellular telephone systems) using special high-gain antennas [3].

WLAN is based on the IEEE 802.11 (shared Ethernet) standard. There are many different flavors of 802.11. The 802.11b standard is the most prevalent standard used today with 802.11a fast gaining ground. There are some major differences between the two standards; 802.11a is five times faster than 802.11b, however, is not interoperable with previously deployed 802.11b products because it operates on a different frequency band. 802.11a also utilizes more transmission channels to offer more bandwidth to support more users than 802.11b.

Listed below are descriptions of WLAN standards, including standards currently in use and those in development phase:

802.11 is the original WLAN standard developed in 1997 and designed for 1-2 Mbps.

802.11a (a.k.a WiFi5) was developed in 1999 and operates at the 5GHz band, supporting 54Mbps. 802.11a is not subject to radio interference from appliances such as microwaves, cordless phones, Bluetooth devices, etc., which is the case for 802.11b. Disadvantages include shorter range, limited operability, and more expensive than 802.11b. 802.11a uses OFDM instead of FHSS or DSSS (see next section on Physical Layers) [7].

802.11b (a.k.a WiFi) was also developed in 1999 but predominated the market faster than 802.11a. It operates in the 2.4-2.48GHz band and supports 11Mbps [5]. Major flaws include limited bandwidth, radio interference from other devices and networks, and security concerns. 802.11b uses DSSS as its physical layer.

802.11c is the standard for bridge operation procedures used in manufacturing Access Points (APs) for wireless LANs [22]. Used mainly by manufacturers in developing products.

802.11d was developed to promote the spread of 802.11 by providing manufacturers of 802.11 products a standard for 802.11 PHY requirements, especially in other countries where the use of the 5GHz bands differ significantly [22]. Used mainly by manufacturers in developing products.

802.11e was developed to improve audio and video transmission in 802.11. Industry experts are currently modifying the standard which will be backwards compatible with existing 802.11 wireless LANs by the simple installation of firmware upgrades to existing APs [22].

802.11f is a standard that outlines specifications for users roaming from one access point to another. 802.11f will allow a WLAN to be comprised of APs from multiple vendors without experiencing interoperability problems. Currently, the use of a single vendor for APs is recommended to prevent roaming issues [22].

802.11g is still in draft and operates in the 2.4GHz waveband. 802.11g supports up to 54Mbps and is backwards compatible with 802.11b products. Final approval of

the standard is expected sometime in early to mid 2003. According to an article in Information Week, "802.11g provides 4-1/2 times the speed of 802.11b and for only a 10% to 15% price premium." [8] The down side to 802.11g is that is has a shorter range than 802.11b, as much as 10 percent. 802.11g uses OFDM for its physical layer.

802.11h was developed to facilitate the sale of 802.11a WLANs in Europe. 802.11h addresses the requirements of European regulatory organizations in order to prevent interference of 802.11a with satellite communications in Europe [22].

Other important and related standards for WLAN are listed below:

802.1x standard was developed to provide additional security for WLANs by providing a means for a centralized authority to verify users or workstations. 802.1x uses an existing protocol, the Extensible Authentication Protocol (EAP [RFC 2284]) that runs on Ethernet, Token Ring or WLAN [9]. 802.1x is supported by Windows XP and most major access point manufacturers [16].

802.11i is another standard being developed (still in draft) to enhance security in both wired and wireless LANs. 802.11i employs user authentication and encryption key distribution. It can be used to restrict access to a network until the user has been authenticated. [10]. "802.11i will solve the two primary security problems with WEP: weak encryption and static keys" [16].

Bluetooth is a standard for short-range digital radio and outlines how various technologies such as mobile phones, computers, and personal digital assistants (PDAs) should interface with traditional office equipment (printers, faxes, telephones) and with computers using short-range wireless connections. Bluetooth uses the 2.45 GHz frequency band and has a throughput of up to 720 kbps. Drawbacks include interference from other devices and low data rates [3]. Bluetooth uses FHSS as its physical layer. It should be noted that Bluetooth is used mainly with ad hoc network topologies (reference the Ad Hoc Network Topology graphic).

WLAN offers various physical layers, each having distinctive characteristics:

Direct Sequence Spread Spectrum (DSSS) – DSSS is a type of spread spectrum radio used by 802.11b that spreads the signal over many frequencies [4, 5].

Frequency Hopping Spread Spectrum (FHSS) – FHSS is type of spread spectrum radio that is used by Bluetooth. Its signal is not spread like DSSS; instead, it hops around from frequency to frequency, avoiding interference. Since the sub channels are smaller than DSSS, more LANs can run simultaneously in the same band [4, 5].

Orthogonal Frequency Division Multiplexing (OFDM) – OFDM is a modulation technique that 802.11a and 802.11g uses for transmitting large amounts of data via radio waves. The benefits of OFDM include resistance to radio frequency

interference and a more efficient use of bandwidth. OFDM works especially well with multimedia applications, which require a lot of bandwidth [5, 6].

Infrared (IR) – IR uses invisible infrared light to transmit data. IrDA (Infrared Data Association) is the standard used in short-range data connections between various computer devices. IR is not susceptible to radio frequency interference and cannot penetrate through walls making it unlikely to be picked up by unknown sources outside a building. IR is utilized on a smaller scale than spread spectrum and is used with devices such as notebooks, cordless computer keyboards & mice, modems, and PDAs. [11]

WLAN Environment

There are three main components used in the WLAN environment:

Wireless Network Interface Card (NIC) – provides the interface between the network operating system and the antenna.

Access Point (AP) – an AP is similar to a LAN hub, except that it is wireless. An AP uses an antenna to transfer data between wireless devices and is connected to a traditional wired LAN backbone with a standard Ethernet cable. The AP is usually mounted high on a wall or ceiling [12].

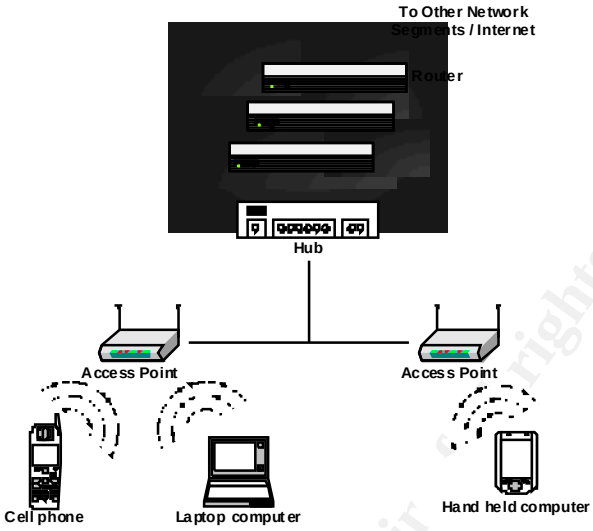
Outdoor WLAN Bridge – device used to connect WLANs in different buildings. WLAN bridges support high data rates and ranges of several miles with the use of line-of-site directional antennas. In some cases, APs can also be used as a bridge between buildings in close proximity [12].

In order to set up a WLAN, wireless network interface cards (NICs) must be installed in client workstations. NICs use radio modems to communicate to an access point (AP) that connects to a wired Ethernet LAN via an RJ-45 port. Wireless clients consist of desktops, laptops, and will eventually include handheld devices such as personal digital assistants (PDAs), text-messaging devices, and smart phones. Access Points that are wired to the LAN backbone must be installed in order for clients to access the traditional network.

There are two WLAN topologies: Infrastructure Network and Ad Hoc Network topologies.

The *infrastructure network* is the most common WLAN topology. It uses APs to connect client workstations to the wired LAN and the Internet. See graphic depicted on the following page:

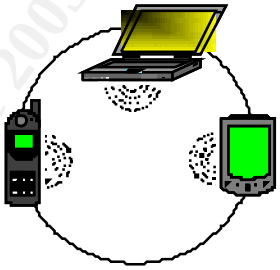
Infrastructure Network Topology




*Graphic adapted from the NIST Wireless Network Security document [3].*

The other network topology is called an *ad hoc network* that connects mobile devices in close proximity and allows the transfer of data between devices without the need of an AP. One example of an ad hoc network is Bluetooth.

Ad Hoc Network Topology



*Graphic adapted from the NIST Wireless Network Security document [3].*

802.11 Security

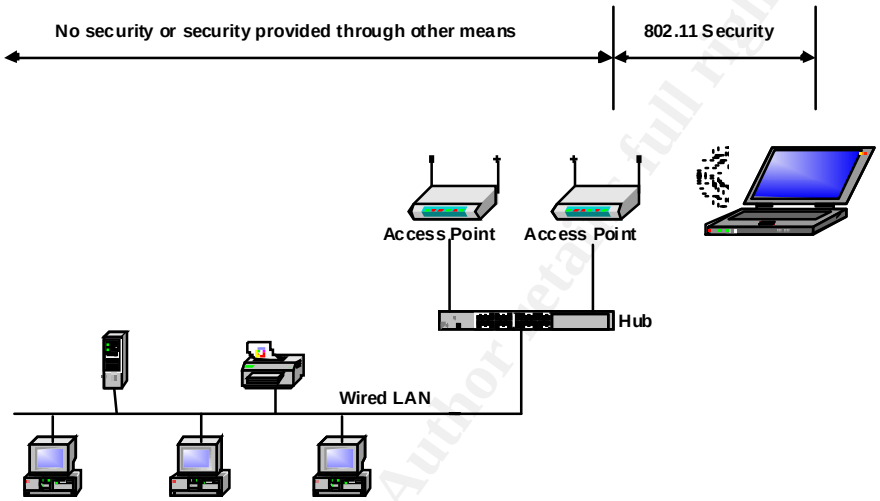
While WLANs offer benefits such as user mobility, rapid installation, flexibility, and scalability, there are also disadvantages such as the vulnerability to radio interference that may degrade data transfer and various security and data integrity issues that will be outlined later in this document.

The security features of 802.11 include SSID, short for Service Set Identifier. SSID is basically a 32 character ID used by wireless clients to connect to an AP. The SSID distinguishes one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

Another security feature is MAC address filtering, which allows access to only those MAC addresses known to the WLAN. A MAC address is a serial number that is burned onto each client machine's network interface card (NIC) that uniquely identifies it from other NICs.

A major security component of 802.11 is WEP (Wired Equivalent Privacy), which provides security for the wireless portion of the WLAN connection.

Wireless Security of 802.11 in a Typical Network




*Graphic adapted from the NIST Wireless Network Security document [3].*

WEP is basically a *no trespassing* sign for the WLAN infrastructure that protects from eavesdropping and prevents unauthorized access to the network. WEP uses keys to encrypt data before it is sent and performs integrity checks to verify that the data has not been changed during transit. However, many publications have been released that detail the security flaws in WEP encryption. Researchers at the University of California Berkeley have documented several successful attempts to comprise WEP security using multiple attack methods. One attack involves modifying driver configurations: "Although most 802.11 equipment is designed to disregard encrypted content for which it does not have the key, we have been able to successfully intercept WEP-encrypted transmissions by changing the configuration of the drivers. We were able to confuse the firmware enough that the cipher text (encrypted form) of unrecognized packets was returned to us for further examination and analysis." [14]

Weaknesses of WEP include weak encryption and the fact that the WEP keys for NICs and APs are not changed automatically and updating the keys is very tedious for network administrators. WEP is also often turned off on many APs; however, it is important that it be enabled despite its weaknesses. Since there are numerous WEP vulnerabilities, it is recommended that WEP be used in conjunction with SSID and MAC address filtering, especially for networks with high security requirements [16]. In

addition, the use of traditional LAN security measures such as Intrusion Detection Systems (IDS) and firewalls are also highly recommended.

It should also be noted that new WLAN security is being developed based on the 802.11i standard that will replace WEP. This new security is called WPA (WiFi Protected Access). WPA currently uses R4 encryption but will eventually use the more secure Advanced Encryption Standard (AES). In addition, WPA will also provide more flexibility in the use of authentication methods than WEP [18].

Security Risks

Wireless presents various security risks and data integrity issues that need to be fully understood before deciding upon deploying a WLAN. Improperly configured and/or unprotected WLANs can allow a network to be accessed by unauthorized users, thus endangering data integrity, network availability, and possibly disclosing sensitive data. In addition, there is always the possibility that unencrypted data may be intercepted when transmitted between wireless clients. Data can also be corrupted due to improper synchronization.

WLAN risks include the interception of signals by individuals outside the building. This is known as wardriving, an activity which seems to be more of a sport for some than for malicious intent. Wardriving is where an individual drives or walks around searching for WLAN signals. Once a signal is located, the individual will attempt to gain access to the network or intercept data being transferred over the WLAN. Network administrators should be aware that wardriving activity is increasing, with many websites providing in-depth instructions on how to wardrive and even more listing wireless hotspots. Anyone with a laptop that has a wireless NIC, sniffer software such as NetStumbler, an antenna, and a GPS can infiltrate an unprotected and/or improperly configured WLAN.

According to an article found on WindowSecurity.com by Robert J. Shimonski entitled *Wireless Attacks Primer*, "In general, attacks on wireless networks fall into four basic categories: passive attacks, active attacks, man-in-the middle attacks, and jamming attacks." [21]

One example of a passive attack is called eavesdropping, which is where an intruder monitors a network and examines data being transmitted over the WLAN. Although eavesdropping is very common and is not always intended to cause harm, it can pose significant threat to an organization by exposing confidential and/or sensitive information. An intruder can monitor network traffic and gather information such as passwords and network configurations that can eventually be used to gain unauthorized access to the network, known as an active attack.

In active attacks, some intruders may use a ploy known as MAC address spoofing where they attempt to gain access to a WLAN by using an altered MAC address to represent themselves as an authorized AP or wireless client. These attackers take advantage of the fact that most wireless NIC manufacturers allow modification of their card's MAC addresses by use of drivers. Even on WLANs where only authorized MAC

addresses are allowed access, the intruder can monitor network traffic to expose authorized MAC addresses and then use them to gain access to the network. It should be noted that there are available tools that network administrators can use to monitor WLAN network activity to detect MAC address spoofing such as AirJack, FakeAP, and Wellenreiter tools [17].

Another form of an active attack is the Denial of Service (DoS) attack where an intruder creates a situation that makes the network unavailable to legitimate users. In this attack, the intruder usually cares less about stealing information, and more about hindering a company's operations, many times causing disastrous financial after effects.

Another type of attack is the man-in-the-middle (MITM) attack. This occurs when an intruder with a laptop and custom software positions themselves between an AP and an authorized client to monitor the network traffic being transmitted between the two. The attacker then disconnects the authorized client from the network forcing them to reconnect. When the authorized clients attempts to logon again, the attacker can then capture the client's SSID and MAC address, which is all that the attacker needs to gain access to the network. One way to prevent the MITM attack is to turn off the SSID broadcast feature on APs [20].

The jamming attack involves an attacker using a strong radio frequency to disrupt the WLAN. The good thing about these type of attacks are that they are not very common because of the expensive equipment needed to produce the strong signal. It should be noted that jamming may also occur accidentally by the use of devices such as cordless phones and Bluetooth devices that are used near WLANs. It is recommended that organizations develop policies that prohibit the use of these devices to prevent disruptions to WLANs [21].

Security Measures

To implement a secure WLAN installation and ensure the confidentiality, integrity, and availability of a network, it is crucial that the following security measures be implemented before deployment of the WLAN. While no network installation can be viewed as completely immune from unauthorized access and attackers, implementing the following security measures will make it extremely difficult, if not impossible, for the casual intruder to infiltrate the network.

To prevent interception of WLAN signals, APs should be mounted on interior walls instead of outside walls or near windows. It is also a good idea to mount the APs out of sight, if possible, such as above ceiling tiles making it more difficult for unauthorized access. Network staff may also want to test the range of their APs to ensure that signals are not being transmitted outside of the building. Even by following these recommendations, wardrivers may still be able to eavesdrop using high-gain antennas. The use of strong encryption with key sizes of at least 128 bits are highly recommended to prevent this.

Before deployment, passwords for APs should also be changed from the default password. The standard password rules should apply when creating the password: passwords with at least 8 characters that include both upper and lower case characters as well as numbers and special characters if possible. In addition, AP keys should be changed on a regular basis, more frequently if there is a high employee turn over rate. APs should never be connected to a LAN's hub instead of a switch. An Ethernet hub will transmit data to every node on the network, including the WLAN segment. An intruder will not only be able to see data transmitted over the WLAN but also from the LAN [13].

AP configurations should also be periodically audited to ensure security mechanisms are being properly implemented. There are various tools on the market that can be used for capturing AP configurations. WEP should be activated on all devices just for the simple fact that some security is better than none at all. The AP's SSID broadcast feature should be disabled to prevent attackers from capturing this data from network traffic.

Other AP configuration changes should include maximizing the beacon interval, which is the interval that an AP regularly transmits signals to wireless devices to authenticate them on the WLAN. The beacon interval should be set to the longest interval possible. Also, to prevent denial of service (DoS) from radio interference from APs that are located within close proximity, the channels of APs should also be changed from the default setting. If the AP supports logging, enable it and monitor logs regularly [3].

AP installations should be inventoried and network administrators should be on the look out for unauthorized AP installations, which can provide an open door for intruders. A company policy should be implemented that outlines the organization's stance on unauthorized WLANs [13].

Periodic assessment of recent WLAN changes/additions should be conducted to ensure that modifications have not exposed the network to intruders. Network administrators may also want to regularly scan the network to detect unauthorized devices

Another recommended security measure is to restrict AP connections to only those devices with approved MAC addresses. A MAC (media access control) address is unique identifier that is burned onto each network interface card (NIC) in a client workstation. The AP uses a client's MAC address to verify if it should be granted access to the network.

Internal procedures should also be developed to ensure that all software and hardware patches are applied in a timely manner to all network cards, APs, client machines, etc. to ensure that all security vulnerabilities have been corrected.

In addition, to ensure a secure connection, it is recommended that WEP be supplemented with a virtual private network (VPN) solution that provides an encrypted tunnel from the client machine to the server. VPN clients should be installed on all

attached devices. Firewalls should be installed between WLANs and traditional LANs and should implement a block all, allow few rule set. All WLAN clients should also have personal firewall software installed.

It is strongly recommended that DHCP (Dynamic Host Configuration Protocol) should *not* be used with wireless networks. DHCP works by automatically assigning IP addresses to clients. DHCP does not know which clients are authorized or not, making it possible for an attacker with a laptop with a wireless NIC to access the WLAN. For this reason it is important that static IP addresses be used [3].

The use of remote SNMP should also be prohibited where possible. SNMP (Simple Network Management Protocol) is a tool that many network administrators use to manage and monitor network devices. Many APs use SNMP. The exception to this is SNMPv3 which incorporates strong security. SNMP versions prior to SNMPv3 use authentication that is based on plain text which is not secure and should not be used on wireless LANs [3].

## Conclusion

While wireless LAN technology offers numerous benefits such as worker mobility, ease of installation, and convenience, the risks associated with wireless technology are considerable, especially if the WLAN will be used to transmit confidential or sensitive information. It must be understood that maintaining a secure wireless network requires greater effort than other traditional wired networks. Organizations must frequently assess security controls when wireless technologies are deployed. In addition, due to the numerous security vulnerabilities inherent in 802.11, various security measures outlined in this document should be implemented before deploying any WLAN installation.

## References


[1] "IT Managers to Increase WLAN Usage in 2003." SC Infosecurity News. 10 January 2003.
URL: http://www.infosecnews.com/sgold/news/2003/01/10_06.htm (27 January 2003)

[2] Foster, Matt. "Wireless Local Area Networking: An Introduction." 22 August 2001.
URL: http://www17.tomshardware.com/network/20010822/index.html#a_brief_history (23 December 2002)

[3] Karygiannis, Tom. Owens, Les. "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices." National Institute of Standards and Technology (NIST). November 2002
URL: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (27 December 2002)

[4] Geier, Jim. "Spread Spectrum: Frequency Hopping vs. Direct Sequence", Wireless-Nets Consulting Services. May 1999.
URL: http://www.wireless-nets.com/articles/whitepaper_spread.htm (27 December 2002)

[5] Webopedia.
URL: http://www.webopedia.com/ (December 2002)

[6] Geier, Jim. "Enabling Fast Wireless Networks with OFDM". Communication Systems Design, 1 February 1 2001.
URL: http://www.commsdesign.com/story/OEG20010122S0078 (29 December 2002)

[7] Geier, Jim. "802.11a: An Excellent Long Term Solution." 802.11 Planet. 31July 2002.
URL: http://www.80211-planet.com/tutorials/article.php/1436331 (3 January 2003)

[8] Keizer, Greg. "Linksys Rolls Out High-Speed 802.11g Wireless Line." TechWeb News. 21 November 2002.
URL: http://www.informationweek.com/story/IWK20021121S0007 (3 January 2003)

[9] Roshan, Pejman. "802.1x Authenticates 802.11 Wireless." Network World. 24 September 2001.
URL: http://www.nwfusion.com/news/tech/2001/0924tech.html (23 December 2002)

[10] Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial." Communication Systems Design. 26 November 2002.
URL: http://www.commsdesign.com/design_corner/OEG20021126S0003 (23 December 2002)

[11] Infrared Data Association
URL: http://www.irda.org/use/index.asp (29 December 2002)

[12] "IEEE 802.11b High Rate Wireless Local Area Networks: Networks as Mobile as the People Who Use Them." Intel. date unknown.
URL: http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/np1692-01.pdf (5 January 2003)

[13] "Wireless LAN Security: 802.11b and Corporate Networks." Internet Security Systems. date unknown.
URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (30 January 2003)

[14] Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP Algorithm." University of California Berkeley. date unknown.
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (11 January 2003)

[15] Conyard, Jason. "Wireless LAN Security for Today and Tomorrow." Wireless Future Magazine. September/October 2002.
URL: http://www.wirelessfuturemagazine.com/lansecurity.html (30 January 2003)

[16] Geier, Jim. "Wi-Fi Spies." Network World. 25 March 2002
URL: http://www.nwfusion.com/wifi/2002/sideonline2.html (27 January 2003)

[17] Wright, Joshua. "Detecting LAN MAC Address Spoofing." Johnson & Wales University. 21 January 2003.
URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf (28 March 2003)

[18] Weinschenk, Carl. "Keeping Pace with Wireless Security Developments." ZDNet.com. 25 March 2003.
URL: http://techupdate.zdnet.co.uk/story/0,,t507-s2132402,00.html (28 March 2003)

[19] Potter, Bruce. Fleck, Bob. "802.11 Security: Attacks and Risks." SearchNetworking.com. 1 December 2002.
URL:
http://searchnetworking.techtarget.com/infoCenter/tip/0,294276,sid7_gci877526_tax293470,00.html
(28 March 2003)

[20] Vamosi, Robert. "How Hackers can Break into a 'Secure' Wireless Net." ZDNet.com. 4 September 2002.
URL: http://www.zdnet.com/anchordesk/stories/story/0,10738,2879081,00.html

[21] Shimonski, Robert J. "Wireless Attacks Primer." WindowSecurity.com. 24 February 2003.
URL: http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html

[22] Geier, Jim. "802.11 Alphabet Soup." 802.11 Planet. 5 August 2002.
URL: http://www.80211-planet.com/tutorials/article.php/1439551 (31 March 2003)