802.11 Wireless And Wireless Security[1]

Cathy Hanus (E-mail: cathyhanus@qwest.net), MS E-Commerce, JD
Michael Hanus (E-mail: mhanus@uswest.net), MS E-Commerce, JD

Abstract

The purpose of this paper is to educate the wireless user or prospective wireless user regarding 802.11 wireless and wireless security. This is achieved by a review of the literature. Our review of the literature includes an overview of the most popular wireless standard, 802.11, some of the benefits of wireless networks, some of the vulnerabilities in wireless networks and some basic security recommendations specific to wireless networks. In addition, the paper gives an overview of some future wireless protocols that are currently being worked on by the various standard developing bodies.

1.0. Introduction

The wireless networking market has taken off in the last couple of years. According to Infonetics Research, $1.7 billion in wireless networking hardware was bought last year with approximately half of that going into home networks. Forecasts indicate the wireless market will continue to grow to $2.7 billion in sales in 2006. It is anticipated that newer, faster wireless products will be a significant portion of sales.[2] Wireless users are discovering the many benefits offered by the use of the wireless network and are fueling this growth; however, they do not always take into account the security risks associated with wireless transmissions.[3]

The purpose of this paper is to educate the wireless user or prospective wireless user by exploring some of the benefits of wireless networks, providing an overview of the most popular wireless standard, and looking at some of the industry's best wireless network security practices. Although there are several wireless standards, this paper will focus on what the industry knows as 802.11 or Wi-Fi (Wireless Fidelity).

2.0. Wireless LAN Overview

2.1. How 802.11 Works

Wireless networks use radio waves to transmit data. 802.11 requires one of three radio bands designated within the industrial, scientific and medical (ISM) band. The original 802.11 standard used the 900 MHz frequency, 802.11b and 802.11g use the 2.4 GHz frequency and 802.11a uses the 5 GHz frequency. These frequencies are also shared with equipment such as microwave ovens and cordless telephones which may sometimes cause interference. The advantage of using the ISM band is that the equipment operator does not require a radio operator's license to use it.

A process known as modulation impresses the wireless radio signal onto the radio frequency. There are three types of modulation used with the 802.11 standard. They are called FHSS (frequency hopping spread spectrum), DSSS (direct sequence spread spectrum) and OFDM (orthogonal frequency division multiplexing).

In FHSS, the transmitter and receiver share a private key containing a "hop" sequence. This sequence shifts channels across the 2.4 GHz band at 1MHz intervals across at least 75 channels while not remaining on any channel longer than 400 milliseconds in a 30-second period. The original 802.11 standard uses FHSS for transmitting.

In DSSS, the signal is spread by dividing the 2.4 GHz band into 14 channels at 22MHz each with 11 channels overlapping the adjacent ones and three non-overlapping channels. It modulates a private key sequence,

shared by the transmitter and receiver, known as the "chipping" code. Generally, DSSS can support higher data rates than FHSS and is more tolerant of interference. The current most popular standard, 802.11b, uses DSSS for transmitting.

OFDM is used for higher-speed wireless signals. It splits the input data into several parallel streams, modulating them onto a separate carrier frequency. The streams are then demodulated at the end of the transmission and recombined to look like the original data. The higher speed standards, 802.11a and 802.11g, use OFDM for transmitting.[4] [5]

2.2. The 802.11 Standards

Although there are other standards developed for wireless LAN, the most commonly used standard is what the industry knows as 802.11 or Wi-Fi. The 802.11 standard was developed by the IEEE (Institute of Electrical and Electronics Engineers) and ratified in 1997. The IEEE is a standards developing body whose members are engineers, scientists and students in electronics and allied fields. Currently, the IEEE has task group committees that continue to refine the 802.11 standards. Each committee uses a letter such as 802.11a or 802.11b and so on to label the developing standard. *Illustration 1 shows a chart with the current activities of each task group.* [6]

The Wi-Fi Alliance is a non-profit group that was established in 1999 to certify interoperability of wireless LAN products based on the IEEE 802.11 specification. Currently products are certified in the 802.11a, 802.11b and 802.11g standards.[7]

Illustration 1. 802.11 Task Group Standard Activities

Standard	Ratified	Band	Speed	Modulation	Comments
802.11	1997	900 MHz	2 Mbps	FHSS	Obsolete
802.11a	1999	5 GHz	Up to 54 Mbps	OFDM	Higher data rates but less transmission distance
802.11b	1999	2.4 GHz	Up to 11 Mbps	DSSS	Most popular Increased speed from 802.11 of 2 Mbps
802.11g	2003	2.4 GHz	Up to 54 Mbps	OFDM	Higher data rates in 2.4 GHz band Backward compatible with b
802.11d	Focused on extending wireless technology to countries not covered by the IEEE.				
802.11e	Focused on improving multi-media transmission & quality of service. Backward compatible.				
802.11f	Focused on enhancing roaming between Access Points and interoperability between vendors.				
802.11h	Focused on frequency selection and power control mechanisms on 5GHz band in some European countries.				
802.11i	Focused on enhancing security with improved key distribution methods and advanced encryption technologies.				

The Wi-Fi Alliance has started certification of "hot spots" it calls Wi-Fi Zones. To qualify as a Wi-Fi Zone, "hot spots" will have to use Wi-Fi certified products and make it possible for someone to connect to a VPN (Virtual Private Network) to secure their data.[8]

3.0. Wireless LAN Benefits

The wireless network market will continue to grow. Individuals and businesses alike recognize the return on investment in wireless products. Wireless networking eliminates the cost of expensive wiring, is easy to set up, provides great mobility and increases productivity. In addition, it provides businesses with increased worker flexibility, faster decision-making ability, higher employee satisfaction and greater accuracy of information.

A recent study by IBM determined if a worker can gain an average of 11 minutes additional productivity a week a wireless network will pay for itself.[9] Gain in productivity is usually much greater than 11 additional minutes a week.[10] All of these benefits, however, come with a price that not all people consider. Since wireless networking works with radio signals, many people may be unwittingly sharing their network with unknown users. Some users do not care or acknowledge sharing their network is a problem. They prefer to leave their wireless LAN "open" to share with their neighbors.[11] The term "open" refers to a network that has no barrier to prevent people from connecting to the wireless network without permission or authority. Leaving the network "open" may also mean the network is insecure and subject to inappropriate snooping and other malicious attacks.

4.0. Common Wireless LAN Vulnerabilities

4.1. Unknown Users

In many ways, wireless security problems are similar to wired security problems. The wireless environment, however, uses an access point that transmits wireless radio signals for a distance of 300-500 feet, including through walls. With a powerful antenna, this distance can be as far as 2000 feet or more.[12] These radio signals can be intercepted allowing access to unknown users.[13] Most businesses are already connected to the Internet and may also allow access to this resource by unknown users. Users should treat the wireless network with the same suspicions as the Internet. Despite the risks, only about one third of wireless networks use security.[14] War driving, war walking and war chalking helped the public to become more aware of wireless insecurities.

4.2. War *ing

Last year, there were several articles on war driving, war walking and war chalking. War driving and war walking is when a device is used to sniff out wireless signals either while driving or walking. Currently, there are even war flyers that fly anything from radio control planes to private single engine planes to sniff out wireless signals.[15]

The Internet has free tools to assist in sniffing out wireless signals. Netstumbler and Kismet are common, free software programs used to sniff out wireless signals. Netstumbler will monitor access points and Kismet can actually intercept network traffic. There are articles and websites that give detailed descriptions on how to build an antenna for searching out wireless signals from a Pringles or beef stew can. [16] With these tools, wireless access points can be mapped by almost any method of moving the antenna around an area.[17]

War walking is sometimes used to war chalk. War chalking is based on a concept used when Hobos marked buildings to tell other Hobos where they were welcomed. It is now used to mark buildings or sidewalks with distinctive symbols telling the knowledgeable person where there are open wireless nodes.[18] This disturbs some executives when they find symbols on their building or sidewalk telling outsiders about the company wireless network. *See Appendix B for War Chalking Symbol link.*

4.3. Session Hijacking

In session hijacking, the hacker waits for the client to authenticate. Then the hacker sends a forged message making it look like it came from the access point. The client thinks he has lost his connection to the access point and the access point thinks the client is still there. This can occur because the client and the access point are not synchronized.

4.4. Man-In-The-Middle

The man-in-the-middle attack occurs when the hacker intercepts the signal and acts as an access point to the client and as a client to the access point. Essentially, the hacker can intercept a transmission, alter it, and send it on as if he was the client.[19]

5.0. Wireless LAN Security

There are numerous things an administrator can do to secure a network and to prevent attacks and unknown users from entering the network. Security is a balance of technology, usability and cost. The following are basic security recommendations specifically addressing wireless networks. It must be stressed that this is not an all inclusive list.

5.1. Establish Good Security Policy

5.1.1. Develop A Dynamic Security Model

A good security policy will give the network administrator a security model for managing the network. It will define limitations for acceptable network operation and performance. These limitations will vary from network to network and so will the resulting security policies. The security model provides a baseline for security policy and must be dynamic to change as technology and security needs change.[20] The security policy will include policy for all aspects of managing a network including the site and infrastructure of the network, administrative issues and the user.[21]

5.1.2. Design The System With Security

It is always best to design a system with security from the start. Consideration should be given to placement of the equipment and what security features are important for the particular situation before the purchase of wireless equipment. Some wireless equipment allows the broadcast feature of the SSID to be shut off, filtering of the MAC addresses or adjustment of the signal strength.[22] Some wireless equipment may even have security enhancements for firewalls, authentication or encryption.[23] If security is not considered from the beginning, some of these features may be missed when purchasing equipment.

5.1.3. Put Technologies Together

Each individual security technology has its own weaknesses. When security technologies are put together the network becomes more secure. This is true for both the wired and wireless network.[24]

5.1.4. Communicate Your Policies

The most secure network can become vulnerable if the users are not aware of security policies. It is important to have a method of communicating and enforcing security policies. Without enforcement, even the best intentioned employee becomes lax in performing his daily tasks in a secure manner. For example, the worker that introduces an improperly secured wireless access point into the business network may not realize the security risk he has introduced to the network.[25]

5.2. Do Not Let People Know Who You Are

5.2.1. Turn Off The Broadcast SSID Function

Each wireless access point has a name called a Set Service Identifier or SSID. In order to connect to this access point, any other device must have that name. Most networks broadcast the SSID, by default, to make these connections easier. If you have a wireless device that allows it, turn off the broadcast function.

5.2.2. Change The SSID Name

Wireless network products are shipped with a default SSID name. It is usually something obvious like the manufacturer's name. Change the SSID to something less obvious. Do not use any information in a name that will

identify you, such as a business name or phone number. Change the name periodically, and your SSID will be even more secure.

5.2.3. Change The Administrator Password

Change the default administrator password on the access point. Use a strong password to protect each access point. *See Appendix B for a link to Password Dos and Don'ts.*

5.3. Limit Access To The Network

5.3.1. Control Your Broadcast Area

Some wireless equipment allows the radio signal strength to be adjusted in different directions. Consider this when purchasing equipment. Whether this is available or not, the access point needs to be set up so the radio signal becomes weaker near the walls. This will weaken the radio signals that are available to unknown users outside the building. This will not stop the user that is using a high strength antenna.

5.3.2. Ban Rogue Access Points

All unauthorized access points must be banned to secure a network. An unauthorized access point that is added to the network is not likely to be configured in such a manner to be secure. This is a policy that must be communicated to users. The network administrator can scan for rogue access points by using software such as Netstumbler to locate unauthorized access points.

5.3.3. Allow Authorized MAC (Media Access Control) Addresses Only

Each networking computer device has a unique MAC address. Some wireless access points allow for filtering of authorized MAC addresses. Determine who should have wireless access and set up the access point so only those MAC addresses are allowed to use that access point. In addition, this is not a very practical security measure in a network of with a high volume of users.

5.3.4. Limit The Number Of DHCP (Dynamic Host Configuration Protocol) Addresses Assigned

If there is a small group of users, the network can be limited to assigning a certain number of DHCP addresses equal to the number of possible users. If everyone is on the network and someone cannot log on, then there is an unauthorized logon.

5.3.5. Use A Firewall

Firewall hardware and software can be configured to allow safe Internet traffic to enter a network and block unsafe Internet traffic. It uses a series of rules to intercept and analyze data to determine whether the traffic is safe to enter either wired or wireless networks. The purpose of a firewall in a notebook using a wireless network is to prevent unsafe traffic from entering not only the notebook but also the network through the notebook.

5.4. Use Authentication And Encryption

5.4.1. WEP (Wired Equivalency Privacy)

802.11 standards have built-in encryption called WEP (Wired Equivalent Privacy). It has been shown that WEP has poor authentication and flaws in the encryption protocol that makes it a weak security tool.[26] Most wireless devices have WEP turned off by default. Even when WEP is turned on, hackers can crack it with minimal effort. *See Appendix B for a link to AirSnort, a UNIX WEP cracking tool available on the Internet as freeware.*

Since WEP is part of the 802.11 standard, it is recommended that it be enabled. Although WEP provides minimal security, it at least provides a way of slowing down the hacker.[27]

5.4.2. Password

A password is a simple means of authentication. It is a secure part of the user's credentials used to access a secured resource. The password should only be known to the user and possibly to the administrator. Either by force and sophisticated guessing methods or by accessing the file where the passwords are stored, hackers can generally get past a password. Passwords should be a combination of easily remembered letters, numbers or symbols. *See Appendix B for a link to Password Dos and Don'ts.*

5.4.3. Kerberos

Kerberos securely authenticates the users request for access to the network. The client contacts the authentication server to get a digital certificate and an encryption key or session key. The session key is then used to request a network service. The digital certificate is embedded in the network protocol which allows the processes implementing the services to know the identity of the users involved. It allows for data stream integrity using Data Encryption Standard (DES). *See Appendix B for a link to MIT Kerberos Information and Distribution.*

5.4.4. RADIUS (Remote Authentication Dial-In User Service)

RADIUS is a protocol for authentication, authorization and accounting of remote access connections. The user inputs his name and password and submits it to the RADIUS server. The RADIUS server determines if the user is authorized to use the network. It can be set up to provide different access levels to the network. Communication between the user and the RADIUS server is encrypted; however, the RADIUS protocol does not provide data encryption. RADIUS is often used with a VPN. *See Appendix B for a link to FreeRADIUS*.[28]

5.4.5. PKI (Public Key Infrastructure)

Public Key Infrastructure is the set of services that are used to support public key cryptography. Public key cryptography or asymmetric cryptography is a strong method of encryption using a key pair called the private and public key. The key pair owner holds the private key secret and makes the public key available to anyone who requests it. If either of the two keys is used to encrypt a message, the other key can decrypt it. For example, if the private key is used to encrypt a message and digitally sign it, the owner's public key is then used to decrypt the message. This ensures the identity of the sender to the recipient. PKI is a trustworthy way to secure Internet transactions and Virtual Private Networks (VPN).

5.4.6. VPN (Virtual Private Network)

The VPN provides a virtual "tunnel" to allow the user to access the corporate network through a public network like the Internet. It does this by authenticating, encrypting and encapsulating data. There are many different ways to set up a VPN, some of which are very costly. To provide a secure environment, the administrator must know how to properly set up the VPN. When the VPN is set up properly, it is generally considered one of the most secure ways to transfer data across the wireless network or the Internet. The VPN usually causes a loss of performance in the network; however, it should improve as hardware acceleration engines for algorithm encryption is built into processors.[29]

5.5. A Look at Future Security Protocols

It is important to note that each of these protocols were developed to take care of weaknesses in current security protocols. Although some of these protocols are not yet ratified, new weaknesses have been demonstrated in all of them.

5.5.1. 802.1x

802.1x is a security protocol ratified by the IEEE. It provides the infrastructure for stronger user authentication and a centralized security model. It restricts access to the network until the user is authenticated by the network. 802.1x helps to fix the static key issues of WEP but since it is only an authentication protocol, it does not fix the encryption weaknesses of WEP.[30] Since 802.1x only uses one-way authentication, it can be subject to some of the same problems as WEP or no wireless security, such as session hijacking and man-in-the-middle attacks, when used by itself.

5.5.2. TKIP (Temporal Key Integrity Protocol)

TKIP is a rapid rekeying protocol that generates a new encryption key with every 10,000 packets and addresses the deficiencies in the WEP algorithms. It also maintains backward compatibility with existing 802.11 products.

5.5.3. AES (Advanced Encryption Standard)

AES is considered the state of the art encryption technology. The IEEE intends to adopt AES in the 802.11i wireless security protocol. AES is not backward compatible with legacy 802.11 products and will require more processing power to handle the encryption and decryption to prevent slowing the performance to an unacceptable level.[31]

5.5.4. WPA (Wi-Fi Protected Access)

The Wi-Fi Alliance, working with the IEEE, has developed an interim security protocol to 802.11i, called WPA. It uses 802.1x for authentication and the stronger encryption protocol, TKIP, which provides a rapid re-keying protocol and improved algorithms over WEP.

In addition, WPA adds Message Integrity Code (MIC) which is a cryptographic checksum that protects against forgery. The transmitter adds the MIC to a packet before it is encrypted and transmitted. The receiver decrypts the packet and verifies the MIC. If the MIC does not match, the packet is dropped. This should be superceded by 802.11i when it is ratified in late 2003.[32]

5.5.5. 802.11i

The 802.11i protocol consists of two layers. The lower layer consists of encryption algorithms, improved over WEP, of the temporal key integrity protocol (TKIP) and the Advanced Encryption Standard (AES) counter mode with CBC-MAC protocol (CCMP). TKIP is used with wireless LAN legacy equipment and CCMP will be used with newer wireless LAN equipment.

The top layer is an authentication protocol. It uses the IEEE 802.1x standard. 802.1x provides for strong user authentication and a centralized security model using encryption key distribution. Radius is an example of an authentication protocol used in 802.1x.[33]

6.0. Conclusion

The 802.11 wireless market is booming. The investment in a wireless network is minimal compared to the benefits achieved in using a wireless network, such as the increase in user productivity and satisfaction. A downside of wireless networks is the difficulty in providing security for a product using radio waves that can be intercepted by anyone with the right tools—especially with the many resources available free on the Internet.

Reviewing the literature it becomes apparent that there are some basic recommendations that can assist in securing a wireless network. Generally, these recommendations are 1) *to establish and enforce a good security*

policy; 2) do not let people know who you are by turning off broadcast functions and changing defaults; 3) *limit access to the network* by controlling the broadcast area, banning rogue access points, filtering MAC addresses, limiting DHCP addresses and using firewalls; and 4) *using authentication and encryption* by turning on the 802.11 standard WEP and considering the use of other stronger methods of authentication and encryption, possibly through the use of a VPN. Although individually each of these recommendations has its weaknesses, together the recommendations can go a long way in securing the wireless network. Future security protocols are already being worked on by standard developing bodies to address the flaws in current protocols. Some of these new security protocols will require more processing power and speed. Wireless is still a relatively new application. As these improvements and others are made to wireless products there will be many more possibilities for the future in the wireless market.

7.0. Suggestions for Future Research

There are three primary areas for research in wireless and wireless security. They include research on current wireless technologies, future wireless technologies and how each of the technologies work together.

Many of the current security technologies in this article provide valuable and interesting areas to research independently. One example of this would be the area of VPNs. The VPN can incorporate a variety of security protocols that can be fairly simple or very complex depending on the needs and the sophistication of the user. Another example would be authentication and encryption. There are many kinds of authentication and encryption and the market can be very confusing. Each individual protocol has its own weaknesses. Research including a good review of the literature and an experimental lab with either of these subjects could prove to be insightful.

Any new and developing area, such as wireless, is a natural area to research. The wireless market is changing rapidly. Future wireless products will have greater speed and processing power to handle higher bandwidth needs. New wireless security protocols are already being developed that require greater speed and processing power. Everyone in the market will want to know how this works.

Finally, an interesting topic for research is how to set up the best security model. The "best security model" will depend on the users individual desires, needs and resources. The most useful research in this area will require choosing a common wireless network, such as a home network, and implementing the basic security recommendations found in this paper and other security features that come to the market. Experimentation might include looking at the least costly versus the most effective way of securing the network. 🕮

Appendix A—Wireless Security Checklist

Establish and enforce a good security policy
1. Develop a dynamic security model
2. Design the system with security
3. Put technologies together
4. Communicate your policies

Do not let people know who you are
5. Turn off the broadcast SSID function
6. Change the SSID name
7. Change the administrator password

Limit access to the network
8. Control your broadcast area
9. Ban rogue access points
10. Allow authorized MAC (Media Access Control) addresses only
11. Limit the number of DHCP addresses assigned
12. Use a firewall

Use Authentication and Encryption
13. Wired Equivalency Privacy (WEP)
14. Password
15. Kerberos
16. Remote Authentication Dial-In User Service (RADIUS)
17. Public Key Infrastructure (PKI)
18. Virtual Private Network (VPN)

A Look at Future Security Protocols
19. 802.1x
20. Temporal Key Integrity Protocol (TKIP)
21. Advanced Encryption Standard (AES)
22. Wi-Fi Protected Access (WPA)
23. 802.11i

Appendix B—Links for Wireless Security Resources

Netstumbler	Monitor Access Points, *http://www.netstumbler.com*.
Kismet	Intercept network traffic, *http://www.kismetwireless.net*.
War Chalking Symbols	*http://www.warchalking.org/story/2002/8/20/17730/3808*.
Cantenna Instructions	Flickenger, Rob. *Antenna on the Cheap (er, Chip), http://www.oreillynet.com/cs/weblog/view/wlg/448*.
Password dos and don'ts	*http://www.pcmag.com/passwords*
AirSnort	Crack WEP, *http://airsnort.shmoo.com*.
FreeRADIUS	RADIUS Authentication, *http://www.freeradius.org*.
MIT Kerberos Information	*http://web.mit.edu/kerberos/www/*.
MIT Kerberos Distribution	*http://web.mit.edu/network/kerberos-form.html*.

End Notes

1. Hanus, Cathy and Michael © 2003.
2. "Superfast Wireless Heads to Homes: First Wireless G Products Hit the Market", February 25, 2003, *http://www.msnbc.com/news/877268.asp*.
3. Hallett, Tony. "Experts: Fear and Laziness Stunt Wi-Fi", *Silicon.com*, March 28, 2003, *http://zdnet.com.com/2100-1103-994500.html.*
4. Stanley, Richard. "Wireless LAN Risks and Vulnerabilities", *Information Systems Control Journal*, Volume 2, 2002.
5. Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.
6. IEEE Standards Association, *http://standards.ieee.org/faqs/wgdev.html*.
7. Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.
8. "Finding Wi-Fi access just got easier: New standards for commercial 'hot spots'", January 10, 2003, *http://storage.itpapers.com/whitepapers/Final3-LinksysWhitePaper10041.pdf*.
9. "Wireless LANs: Linking Productivity Gains to Return on Investment", *Intel*, December 2002, *http://www.intel.com/eBusiness/pdf/it/pp024801.pdf*.
10. Kastner, Peter. "Don't Panic! Intel's New Centrino Notebook Chipset Mean Wi-Fi is Coming Whether You're Ready for It or No", *Internet Week*, March 24, 2003, *http://www.internetweek.com/story/showArticle.jhtml?articleID=8100014*.
11. e.g., Festa, Paul. "Free Wireless Goes Underground", *News.com*, Sep 26, 2001, *http://chkpt.zdnet.com/chkpt/printthisclick/www.zdnet.com/filters/printerfriendly/0,6061,5097452-2,00.html*
12. Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.

13. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
14. Brooks, Jason. "Wireless LAN Lockdown", *http://www.eweek.com/article2/0,3959,857260,00.asp*.
15. Brewin, Bob. "War flying: Wireless LAN sniffing goes airborne", *Computerworld*, August 30, 2002, *http://www.computerworld.com/mobiletopics/mobile/story/0%2C10801%2C73901%2C00.html*.
16. Flickenger, Rob. "Antenna on the Cheap (er, Chip)", July 5, 2001, *http://www.oreillynet.com/cs/weblog/view/wlg/448*.
17. Information & Telecommunications Technology Center, Kansas Applied Remote Sensing Program, 2002, *http://www.ittc.ku.edu/wlan/images.shtml*.
18. Warchalking, *http://www.warchalking.org/story/2002/8/20/17730/3808*.
19. Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.
20. Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.
21. *Maximum Security*, 3rd Ed., SAMS Publishing, Indiana, 2001, p. 596.
22. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
23. Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.
24. Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.
25. Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.
26. Garfinkel, Simson. "The Internet Amenity", *Technology Review*, Cambridge, Mar 2002.
27. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
28. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
29. Tulloch, Mitch. *Microsoft Encyclopedia of Networking*, Microsoft Press, 2000, p. 1009-10.
30. Chu, Francis. "Standards Will Fill Holes in WEP Authentication and Encryption", February 03, 2003, *http://www.eweek.com/article2/0,3959,857267,00.asp*.
31. Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.
32. Emigh, Jacqueline. "WPA: Is Wi-Fi's Security Bandage Going to Win over Network Admins?" *http://www.80211-planet.com/tutorials/article.php/1550561*.
33. Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.

References

1. Barker, Garry. "X Marks the Spot for Hackers", *The Age*, July 8, 2002, *http://www.theage.com.au/articles/2002/07/07/1025667088839.html*.
2. Brewin, Bob. "War flying: Wireless LAN sniffing goes airborne", *Computerworld*, August 30, 2002, *http://www.computerworld.com/mobiletopics/mobile/story/0%2C10801%2C73901%2C00.html*.
3. Brooks, Jason. "Wireless LAN Lockdown", *http://www.eweek.com/article2/0,3959,857260,00.asp*.
4. Chu, Francis. "Standards Will Fill Holes in WEP Authentication and Encryption", February 03, 2003, *http://www.eweek.com/article2/0,3959,857267,00.asp*.
5. Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.
6. Emigh, Jacqueline. WPA: "Is Wi-Fi's Security Bandage Going to Win over Network Admins?" *http://www.80211-planet.com/tutorials/article.php/1550561*.
7. Festa, Paul. "Free Wireless Goes Underground", *News.com*, Sep 26, 2001, *http://chkpt.zdnet.com/chkpt/printthisclick/www.zdnet.com/filters/printerfriendly/0,6061,5097452-2,00.html*
8. "Finding Wi-Fi access just got easier: New standards for commercial 'hot spots'", January 10, 2003, *http://storage.itpapers.com/whitepapers/Final3-LinksysWhitePaper10041.pdf*.

9. Flickenger, Rob. "Antenna on the Cheap (er, Chip)", July 5, 2001, *http://www.oreillynet.com/cs/weblog/view/wlg/448*.
10. Garfinkel, Simson. "The Internet Amenity", *Technology Review*, Cambridge, Mar 2002.
11. Gerulski, David. "Are You Vulnerable?", *Internet Security Systems*, February 2003 Power Point Presentation.
12. Hallett, Tony. "Experts: Fear and Laziness Stunt Wi-Fi", *Silicon.com*, March 28, 2003, *http://zdnet.com.com/2100-1103-994500.html*.
13. IEEE Standards Association, *http://standards.ieee.org/faqs/wgdev.html*.
14. Information & Telecommunications Technology Center, Kansas Applied Remote Sensing Program, 2002, *http://www.ittc.ku.edu/wlan/images.shtml*.
15. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
16. Kastner, Peter. "Don't Panic! Intel's New Centrino Notebook Chipset Mean Wi-Fi is Coming Whether You're Ready for It or No", *Internet Week*, March 24, 2003, *http://www.internetweek.com/story/showArticle.jhtml?articleID=8100014*.
17. MacKenzie, Matthew. "802.11g: Willing, But Still Not Ready", March 17, 2003, *http://www.techweb.com/*.
18. *Maximum Security*, 3rd Ed., SAMS Publishing, Indiana, 2001, p. 596.
19. Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.
20. Stanley, Richard. "Wireless LAN Risks and Vulnerabilities", *Information Systems Control Journal*, Volume 2, 2002.
21. "Superfast Wireless Heads to Homes: First Wireless G Products Hit the Market", February 25, 2003, *http://www.msnbc.com/news/877268.asp*.
22. Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.
23. Tulloch, Mitch. *Microsoft Encyclopedia of Networking*, Microsoft Press, 2000.
24. Warchalking, *http://www.warchalking.org/story/2002/8/20/17730/3808*.
25. Ward, Mark. "Hacking with a Pringles Tube", *BBC News*, March 8, 2002, *http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm*.
26. Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.
27. "Wireless LANs: Linking Productivity Gains to Return on Investment", *Intel*, December 2002, *http://www.intel.com/eBusiness/pdf/it/pp024801.pdf*.

Notes

[1] Hanus, Cathy and Michael © 2003.

[2] "Superfast Wireless Heads to Homes: First Wireless G Products Hit the Market", February 25, 2003, *http://www.msnbc.com/news/877268.asp*.

[3] Hallett, Tony. "Experts: Fear and Laziness Stunt Wi-Fi", *Silicon.com*, March 28, 2003, *http://zdnet.com.com/2100-1103-994500.html.*

[4] Stanley, Richard. "Wireless LAN Risks and Vulnerabilities", *Information Systems Control Journal*, Volume 2, 2002.

[5] Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.

[6] IEEE Standards Association, *http://standards.ieee.org/faqs/wgdev.html*.

[7] Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.

[8] "Finding Wi-Fi access just got easier: New standards for commercial 'hot spots'", January 10, 2003, *http://storage.itpapers.com/whitepapers/Final3-LinksysWhitePaper10041.pdf*.

[9] "Wireless LANs: Linking Productivity Gains to Return on Investment", *Intel*, December 2002, *http://www.intel.com/eBusiness/pdf/it/pp024801.pdf*.

[10] Kastner, Peter. "Don't Panic! Intel's New Centrino Notebook Chipset Mean Wi-Fi is Coming Whether You're Ready for It or No", *Internet Week*, March 24, 2003, *http://www.internetweek.com/story/showArticle.jhtml?articleID=8100014*.

[11] e.g., Festa, Paul. "Free Wireless Goes Underground", *News.com*, Sep 26, 2001, *http://chkpt.zdnet.com/chkpt/printthisclick/www.zdnet.com/filters/printerfriendly/0,6061,5097452-2,00.html*

[12] Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.

[13] Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.

[14] Brooks, Jason. "Wireless LAN Lockdown", *http://www.eweek.com/article2/0,3959,857260,00.asp*.

[15] Brewin, Bob. "War flying: Wireless LAN sniffing goes airborne", *Computerworld*, August 30, 2002, *http://www.computerworld.com/mobiletopics/mobile/story/0%2C10801%2C73901%2C00.html*.

[16] Flickenger, Rob. "Antenna on the Cheap (er, Chip)", July 5, 2001, *http://www.oreillynet.com/cs/weblog/view/wlg/448*.

[17] Information & Telecommunications Technology Center, Kansas Applied Remote Sensing Program, 2002, *http://www.ittc.ku.edu/wlan/images.shtml*.

[18] Warchalking, *http://www.warchalking.org/story/2002/8/20/17730/3808*.

[19] Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.

[20] Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.

[21] *Maximum Security*, 3rd Ed., SAMS Publishing, Indiana, 2001, p. 596.

[22] Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.

[23] Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.

[24] Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.

[25] Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.

[26] Garfinkel, Simson. "The Internet Amenity", *Technology Review*, Cambridge, Mar 2002.

[27] Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.

[28] Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.

[29] Tulloch, Mitch. *Microsoft Encyclopedia of Networking*, Microsoft Press, 2000, p. 1009-10.

[30] Chu, Francis. "Standards Will Fill Holes in WEP Authentication and Encryption", February 03, 2003, *http://www.eweek.com/article2/0,3959,857267,00.asp*.

[31] Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.

[32] Emigh, Jacqueline. "WPA: Is Wi-Fi's Security Bandage Going to Win over Network Admins?" *http://www.80211-planet.com/tutorials/article.php/1550561*.

[33] Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.

References

1. Barker, Garry. "X Marks the Spot for Hackers", *The Age*, July 8, 2002, *http://www.theage.com.au/articles/2002/07/07/1025667088839.html*.
2. Brewin, Bob. "War flying: Wireless LAN sniffing goes airborne", *Computerworld*, August 30, 2002, *http://www.computerworld.com/mobiletopics/mobile/story/0%2C10801%2C73901%2C00.html*.
3. Brooks, Jason. "Wireless LAN Lockdown", *http://www.eweek.com/article2/0,3959,857260,00.asp*.
4. Chu, Francis. "Standards Will Fill Holes in WEP Authentication and Encryption", February 03, 2003, *http://www.eweek.com/article2/0,3959,857267,00.asp*.
5. Eaton, Dennis. "Diving into the 802.11i Spec: A Tutorial", November 26, 2002, *http://www.commsdesign.com/design_corner/OEG20021126S0003*.
6. Emigh, Jacqueline. WPA: "Is Wi-Fi's Security Bandage Going to Win over Network Admins?" *http://www.80211-planet.com/tutorials/article.php/1550561*.
7. Festa, Paul. "Free Wireless Goes Underground", *News.com*, Sep 26, 2001, *http://chkpt.zdnet.com/chkpt/printthisclick/www.zdnet.com/filters/printerfriendly/0,6061,5097452-2,00.html*
8. "Finding Wi-Fi access just got easier: New standards for commercial 'hot spots'", January 10, 2003, *http://storage.itpapers.com/whitepapers/Final3-LinksysWhitePaper10041.pdf*.
9. Flickenger, Rob. "Antenna on the Cheap (er, Chip)", July 5, 2001, *http://www.oreillynet.com/cs/weblog/view/wlg/448*.
10. Garfinkel, Simson. "The Internet Amenity", *Technology Review*, Cambridge, Mar 2002.
11. Gerulski, David. "Are You Vulnerable?", *Internet Security Systems*, February 2003 Power Point Presentation.
12. Hallett, Tony. "Experts: Fear and Laziness Stunt Wi-Fi", *Silicon.com*, March 28, 2003, *http://zdnet.com.com/2100-1103-994500.html*.
13. IEEE Standards Association, *http://standards.ieee.org/faqs/wgdev.html*.
14. Information & Telecommunications Technology Center, Kansas Applied Remote Sensing Program, 2002, *http://www.ittc.ku.edu/wlan/images.shtml*.
15. Karagiannis, Konstantino. "Ten Steps to a Secure Wireless Network", February 25, 2003, *http://www.pcmag.com/article2/0,4149,844020,00.asp*.
16. Kastner, Peter. "Don't Panic! Intel's New Centrino Notebook Chipset Mean Wi-Fi is Coming Whether You're Ready for It or No", *Internet Week*, March 24, 2003, *http://www.internetweek.com/story/showArticle.jhtml?articleID=8100014*.
17. MacKenzie, Matthew. "802.11g: Willing, But Still Not Ready", March 17, 2003, *http://www.techweb.com/*.
18. *Maximum Security*, 3rd Ed., SAMS Publishing, Indiana, 2001, p. 596.
19. Schwartz, Ephraim. "Researchers Crack New Wireless Security Spec", February 14, 2002, *http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html*.
20. Stanley, Richard. "Wireless LAN Risks and Vulnerabilities", *Information Systems Control Journal*, Volume 2, 2002.
21. "Superfast Wireless Heads to Homes: First Wireless G Products Hit the Market", February 25, 2003, *http://www.msnbc.com/news/877268.asp*.
22. Tanzella, Fred. "Wireless LAN Security—How to Protect WLANs", *Air Defense*, November 03, 2002, *http://www.airdefense.net/wirelesslansecurity/wlan_security_whitepaper.html*.

23. Tulloch, Mitch. *Microsoft Encyclopedia of Networking*, Microsoft Press, 2000.
24. Warchalking, *http://www.warchalking.org/story/2002/8/20/17730/3808*.
25. Ward, Mark. "Hacking with a Pringles Tube", *BBC News*, March 8, 2002, *http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm*.
26. Wi-Fi Alliance, *http://www.weca.net/OpenSection/index.asp?noFlash=true*.
27. "Wireless LANs: Linking Productivity Gains to Return on Investment", *Intel*, December 2002, *http://www.intel.com/eBusiness/pdf/it/pp024801.pdf*.

Notes