Global Information Assurance Certification Paper

MINIMIZING THE RISKS ASSOCIATED WITH WIRELESS LOCAL AREA NETWORKS

(with an overview of the standards)

Prepared for:
Practical SANS GIAC Certification
GSEC Version 1.4b

Prepared by:
Cadwallader "Walter" Franklin
September 19, 2002

1. Abstract

The Institute of Electrical and Electronics Engineers (IEEE) 802.11 based wireless LAN (WLAN) technologies has boomed in popularity in business, government agencies, and the private sector over the past year. As is with the positives in life one has to address the negatives and this boom brings with it some security concerns.

In some cases, individuals who are considered novices in the areas of networking and network security are deploying WLANs. These deployments are part of the reason for the security concerns, not to mention the fact that 802.11 by its very nature is a radio transmission of information; broadcasting into the air.

The purpose of this paper is to propose some things that a novice and a network administrator can do to reduce the risks associated with deploying WLANs, regardless of whether the deployment is authorized or un-authorized. Some of the things suggested are simple no cost items while the other items suggested include such things as isolating the WLAN from the wired network resources to monitoring the WLAN.

2. Introduction

IEEE 802.11 wireless local area networks (WLANs) have grown in popularity and are being deployed on corporate networks both large and small. Not only are they being used in the business community, from retail stores to corporate networks, but WLANs are also being used for home networks in conjunction with high-speed Internet access. With the growing popularity of this technology comes the issue of security; how secure are WLANs? More and more individuals are asking this question and are working to minimize the risks associated with this technology. The intent of this paper is to discuss some of the things that a WLAN administrator can do to lower the risks associated with this technology while benefiting from the flexibility and mobility this technology brings to the industry. This paper addresses 802.11 networks configured as an [1] (*Lough*) infrastructure network versus an ad-hoc network, having said that, ad-hoc networks are mentioned in the discussions below.

3. Types of Usage

3.1. Private Sector

With the cost of wireless access under $300, more and more users elect to install wireless in the home supporting their home networks. In many home networks the users have limited knowledge of the security issues and limited resources to protect themselves. This paper lays out some things that can be done to reduce the average home user's risk.

The home user probably chose wireless because it is convenient and it doesn't restrict the user to any one location in the house. Usages of the network in this environment varies from gaming, personal finances, take home work, home business, and school homework. In each of these cases the user may not care about security nor do they feel that there is a risk, however one should be concerned about a neighbor sniffing work or financial related data or just using their network for free.

3.2. Small Business

Like the home environment, small businesses have a need to keep their costs to a minimum. As stated earlier WLAN is a low cost and quick solution for private office networks with fewer than 20 to 25 users with a DSL or cable modem connecting that network to the Internet. This solution can be deployed within a matter of hours if not minutes; no wires to pull and no network drops to install, and expansion is just a matter of buying another wireless network card and access point if necessary.

The risk for a small business is greater than that of the home network. A small business has to consider the cost of losing or altering customer data, and exposing sensitive customer data to a competitor.

3.3. Large Business

Large businesses will, in most cases, have an existing wired network infrastructure, however they may have a need for nomadic type users who move to different places within a single facility. For example, an employee may have a need to move from a desk to a conference room to a temporary workspace all in the course of hours to days. WLANs in this environment offers the flexibility that a nomadic employee with a laptop needs; allowing them to be connected to the network with access to shared resources.

Large businesses are also using WLANs in warehouse and manufacturing type environments where wiring isn't practical or where the employee needs to move between workstations with little to no down time. In this environment the employee can have access to shared resources in real time for functions such as inventorying, ordering, change orders, email, etc.

3.4. Government Agencies

Government agencies; city, state, and federal, are all getting in on the wireless networking roller coaster. They are following the same paradigm as that of the home users and private businesses both large and small. Government agencies will have information about individuals as well as information that is considered government sensitive. This information, if exposed to the public can range anywhere from an embarrassment to a threat to national security.

4. Standards

The IEEE 802 LAN/MAN Standards Committee develops Local Area Network standards and Metropolitan Area Network standards. The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area[2] (*O'Hara*). This document addresses part 11 of the 802 standards and in particular, this section discusses 802.11, 802.11a, 802.11b, 802.11g, and 802.1x.

4.1. 802.11

In 1997 the IEEE ratified the 802.11 standard for wireless LANs operating at 2.4 GHz band at speeds of 1 and 2 Mbps. There were two different types of coding techniques used: (1) frequency hopping spread spectrum (FHSS) and (2) direct sequence spread spectrum (DSSS). FHSS and DSSS are two of the three physical layer units specified with the third being infrared.

4.2. 802.11a

In 1999 the IEEE ratified two physical layer extensions to the original standard, the second of which is the 802.11a standard. The purpose behind 802.11a was to create a higher speed wireless access technology. 802.11a supports connections of up to 54 Mbps in the 5 GHz band using an encoding scheme know as orthogonal frequency division multiplexing (OFDM). OFDM is the reason for the high-speed and stable connections on which the standard is based.

802.11a operates in a 300 MHz spectrum within the 5 GHz band that allows for 12 clear channels for data transmission. The 300 MHZ spectrum is divided up into three sections: (1) a lower band at 5.15 – 5.25 GHz with a power output limit of 50 mW, (2) a middle band at 5.25 – 5.35 GHz with a power output limit of 250 mW, and (3) an upper band at 5.75 – 5.825 GHz with a power output limit of 1 W. Each of the three sections supports four non-overlapping channels with the third section; the upper band, designated for outdoor use[3] (*Massaro, p.39*).

4.3. 802.11b

In 1999 the IEEE ratified two physical layer extensions to the original standard, the first of which is the 802.11b standard. The purpose of 802.11b is to increase the data rate achievable while operating within the framework of 802.11. 802.11b provides for speeds of up to 11 Mbps in the 2.4 GHz band using DSSS.

802.11b was the first widely available wireless technology to provide speeds similar to a typical wired local area network. 802.11b established itself before 802.11a.

802.11b operates in an 83.5 MHz spectrum within the 2.4 GHz band that allows for 11 channels of which only 3 are clear channels; non-overlapping channels. Although 802.11b has fewer clear channels and less of a throughput than

802.11a, it has a range of 400 feet which is greater than the range of 802.11a[4] (*Massaro, p.38*).

4.4. 802.11g

802.11g is currently a draft standard whose purpose is to develop a higher speed physical layer extension to 802.11b. "802.11g actually combines the best of 802.11b and 802.11a standards with the promise of a harmonious future for continued development of 802.11 products"[5] (*Massaro, p.40*).

802.11g offers the high data rates (54 Mbps) of 802.11a while operating in the 2.4 GHz band of 802.11b. This draft standard also calls for the mandatory use of ODFM from 802.11a along with the mandatory modes associated with 802.11b. It is expected that 802.11g will be the bridge between the 802.11b and 802.11a standards.

4.5. 802.1x

802.1x is a draft standard that's expected to be ratified in mid-2002. The purpose of this draft standard is to plug the security holes in 802.11. 802.1x provides strong authentication, access control, and key management. A good way of viewing 802.1x is that it provides the framework on which various authentication methods can work. It also provides port-based network access control for networking technologies.

5. Problem Statement

With the growing use of wireless comes the increasing concern of security. Although WLANs offer great flexibility with no cable plant it also brings to the table the issue of security. The concern that every wireless user should have is security: who can see my data, who can access not only the data on the wireless systems but also the data on systems that are on the wired network that connects to the wireless network. The question is what can be done to minimize the risks associated with using WLANs?

6. Threats to WLANs

WLANs have the same threats as wired LANs plus those that are unique to wireless. The threats introduced by WLANs expose the wired network(s). The following are the threats associated with WLANs:

- Radio frequency interference
- Denial of Services
- Wireless Sniffing
- Improper Configuration

6.1. Radio Frequency Interference

802.11b devices operate at 2.4 GHz. This band "was originally intended for Industrial, Scientific, and Medical use; a sink for waste radiation thrown out by microwave ovens, therapeutic heaters, and radar"[6] (*Dornan, p.3*). This is also

the same frequency as that of cordless phones. 2.4 GHz is an unlicensed frequency and therefore other devices can interfere with the radio signal between the access point and the clients and client to client. Although this is a problem and can result in a denial of services type of situation, this document simply acknowledges that radio frequency interference is a problem.

6.2. Denial of Service

Denial of Service (DOS) attacks is a risk of wired networks as well as wireless. Unlike the previous section where one may experience un-intentional interference, this section speaks to those that are intentional. DOS attacks are perpetrated by individuals who with the proper equipment flood the 2.4 GHz frequency with noise so as to drive the signal to noise ration low enough such that the devices cannot communicate.

DOS attacks can also be perpetrated by using a wireless client to flood either a client or an access point with bogus packets so as to prevent the legitimate traffic from passing. This type of an attack may be accomplished by setting up a rogue client with a legitimate MAC address.[7] (*Klaus p.7*)

6.3. Wireless Sniffing

With the increasing number of wireless network access points popping up both in the home and business environments some individuals are installing wireless sniffers and simply driving by various businesses looking for access points radiating their signal in parking lots and nearby roadways. Some of these access points are rogue devices that were installed without permission from the network administrator.

Some of the rogue access points are configured by novices and are setup using the factory defaults settings. The problem caused by this is that by default these devices are wide open, allowing anyone to connect and most, if not all the vendors default settings are available on the WEB.

Not only are rogue access points of concern but one must realize that drive by sniffing is easy and next to impossible to detect. With a high gain antenna, one can eavesdrop from 200 to 400 feet away. The sniffing devices with the high gain antenna can be located across the street in the window of a vacant building, wooded lot, a vehicle in the parking lot across the street, etc. Having said that one should assume that someone is eavesdropping on the wireless network.

6.4. Improper Configuration

Most if not all the vendors of wireless devices set their default configuration so that the devices will pass traffic with minimum changes on the part of the user when installed out of the box. The paradigm used here is plug and play. The result of this is that there is usually little to no security turn-on therefore making the access point an easy target. The default passwords for things like the SNMP

public and private string and the administrator console is left in place. This information is freely available.

Not only are passwords left in default mode but also the Server Set Identification (SSID) and Wire Equivalent Protocol (WEP) are also left with the default setting. In some devices the SSID is set to broadcast and based on what the SSID is set to one can very easily determine the particular vendors access point being used and immediately know what the other default settings are along with any particular vulnerabilities that device may have. In addition to this the default WEP setting is know as well as passwords.

7. Reducing the Risk Associated with WLANs

Although this can be a large task there are things that a network administrator can do to reduce the risks associated with WLANs. This section describes the things that a network administrator should do to identify and reduce the risks associated with the introduction of WLANs.

7.1. Site Survey

A network administrator should acquire a wireless sniffer and patrol the campus looking for rogue wireless access points. This type of survey should be conducted periodically, at least once a quarter. Working hand and glove with this type of a site survey the administrator should communicate the security issues associated with the use of a rogue access point to the user community. One hopes, that by educating the user community of the security issues, the users will help to mitigate the risks.

In addition to conducting a survey looking for rogue WLANs, the administrator should talk with the user community to see if there is a requirement for wireless. If there is a requirement, then the administrator should consider deploying wireless in the environment in a safe manner. By doing so the administrator minimizes the need for rogue access points.

If it's determined that the newly installed "rogue" access point cannot be removed for whatever reasons, then some key pieces of data needs to be noted during the survey, such as what is the intended coverage area versus the actual coverage area. What one may find is that the intended coverage area is smaller than the actual coverage area. In such a case the power output of the access point should be reduced to correspond with the desired area of coverage. One should also pay attention to where the antenna is located relative to the desired coverage area.

The antenna should be located as far away from an outside wall as possible while achieving the desired coverage. In addition to being concerned about the outside wall, the issue of upper and lower floors in a multi-story facility with various tenants should also be a consideration. In short the goal should be to reduce the signal so that it is only available to the desired users because one

doesn't know who is on the floor above or below intercepting the signal and possible connecting to the network.

Another item that is worth considering is looking at the type of antenna used on the access point. In order to change the characteristics of the radiation pattern, the antenna should be changed from an omni to a directional antenna. The objective here is to make it more difficult for someone to eavesdrop on the network; if the signal isn't radiating beyond the intended boundaries then it can't be sniffed from the air.

Please note, this does not solve the security problems associated with WLANs but it is a start in the right direction of minimizing the risks.

7.2. Turning on Service Set Identification (SSID)

Richard Harada, Sr. Product Manager, Wireless Systems, Psion Teklogix gave the following explanation of SSID:

> Service Set Identification was designed to allow wireless networks to be better managed by ensuring wireless nodes talk only to the right system. Although not intentionally designed to provide security, SSID does provide a first line of defense against intruders. By assigning a SSID to both the access point and the mobile devices, SSID allows multiple RF networks to operate in the same physical area without the threat of accessing the wrong network. If the access point and device SSID do not match, access to the network is denied. If the SSID is known only to those authorized to use the WLAN, it becomes-in essence – a first level of security. While it has been proven that SSID can be overcome, it should be implemented if only to prevent unwanted users from fortuitously accessing the WLAN. Exposing the SSID to eavesdroppers can be minimized by removing it from the access point broadcast beacon.[8] (Harada, p1)

7.3. MAC Control List

Media Access Control (MAC) can be used to prevent unwanted systems from associating with the WLAN. The MAC address of all approved systems must be known and added to the access list in the WLAN access point. Once the MAC is defined then all those approved systems are allowed on the network. This offers what is sometimes called "MAC Level Authentication".[9] (*Harada, p.2*)

Please note that by using MAC it is only a deterrent or "speed bump". The MAC address of the access point is still broadcast in the air and can be sniffed and then forged by a rogue device.

7.4. Enabling WEP

Wired Equivalency Protocol (WEP) was added to the 802.11 standard to address the concern of ease of eavesdropping on WLANs. WEP, as the name suggests is intended to make wireless networks the equivalent of wired networks from a

security standpoint. Although in it's original proposal WEP used 40-bit encryption, it is also available with 128-bit encryption by most vendors. By using WEP the data between the access point and the clients are encrypted therefore making it more difficult to pull intelligent data by simply eavesdropping.

It is important to note that WEP isn't as secure as one would like since the hacker community has developed methods to break the 128-bit encryption by gathering enough traffic through eavesdropping and then determining the encryption key. Because of this it is recommended that the keys be rotated frequently.

Key rotation leads to another issue with WEP. WEP does not have a key manager. In other words, there is no mechanism in WEP that allows for key distribution and key rotation automatically. Because of this the keys associated with WEP have to be changed manually and is distributed using some type of out of band method. For this reason WEP does not scale for large WLAN deployments without the presence of some form of an authentication service.

Some vendors, however, offer products that do dynamic WEP and the administrator can select the interval at which the keys are updated therefore adding an additional layer of difficulty to those who may be trying to eavesdrop on a WLAN and collect data.

7.5. Network Design Consideration

The recommendations mentioned above do not require changes in network architecture, however, there are options that should be considered that require changes to the network architecture, such as placing the access points in a DMZ (De-Militarized Zone). A DMZ is a "network term for a specially designed network segment where external users are allowed to access resources without getting any access to internal networks"[10] (*Macaulay, p.8*). The access point should be placed in front of the firewall thus separating the wireless traffic from the internal network and treating the WLAN as another connection to the Internet.

7.6. Virtual Private Network for WLANs

Implementation of a Virtual Private Network (VPN) in support of the wireless network is a wise approach. Using a VPN with the WLAN adds an additional layer of encryption and opens up a secure hole through the firewall between the DMZ and the internal network. The VPN makes it even more difficult for eavesdropping and gives the WLAN users a secure tunnel to access resources on the internal network. Using the VPN on the WLAN creates an environment where guests to the network and users can co-exist in the same physical space such as a conference room and allow both types of users to conduct their business. The guest user can access the Internet and resources outside the protected internal network while the user of the internal network can retrieve information real time without exposing user specific information on the open network.

This section assumes that the VPN is implemented in such a manner that the necessary user authorization and authentication is handled properly. It also assumes that the VPN is configured without a split-tunnel. The issue associated with a split-tunnel is that logically the system is dual homed and if the host is compromised it can be used as a router to access the internal network.

7.7. User Authentication

Implement some method of user authentication. The network administration needs to know who is on the network and must have a method to authenticate each user. One of the more popular methods is via RADIUS (Remote Authentication Dial-in User Services). The RADIUS can be deployed in conjunction with the DMZ to authenticate users via the VPN or it can be deployed in the absence of a VPN. If used in the latter configuration then it is used to authenticate a user on the wireless network in conjunction with an implementation of MAC where the RADIUS proxies the authentication back to an existing method of authentication such as a Microsoft domain.

Another method used to authenticate users is the Extended Authentication Protocol (EAP). Today not all 802.11b vendors support EAP, however, there are some that do, such as Cisco. Cisco uses Lightweight Extended Authentication Protocol (LEAP). LEAP authenticates a user before granting the associated system an IP address and thus placing the requesting user's system on the network.

There is an exchange of data between the wireless network card and the access point where the network card is granted restricted access therefore passing across the network the challenge and response package. Once the requester is authenticated then the system is assigned an address if it is configured to support DHCP, and the user is then authorized to connect to the network. Please note that this doesn't give a user access to resources that are on that network.

Deploying some method of user authentication with MAC allows for system authorization along with user authentication. If the MAC and user credentials don't match then access is denied. This is useful in the event a MAC address is forged or a users system or network card is stolen; Authentication and authorization is granted based on what you have and what you know.

7.8. Monitoring the WLAN

Implementing the suggested items from the previous sections will help to minimize the vulnerabilities associated with WLANs. With these items in place the next step is to monitor the WLAN. Monitoring the WLAN is an essential part of minimizing the risks associated with WLANs. This capability is an important tool in the tool bag of a network administrator. A special intrusion detection system (IDS) should be deployed to monitor for the following: rogue access

points, unauthorized ad-hoc networks, unauthorized 802.11 cards, and denial of services attacks.

These items in particular need to be monitored at a minimum because they help to identify the when and how an intruder compromised your network and the origin of the attack; inside or outside. Watching for rogue access points will notify you of the appearance of an unauthorized access point by network savvy individuals who may have deployed it out of convenience so as to allow for roaming. This deployment however, may not be secure and therefore your network is now open to anyone.

Another scenario to consider is the rogue or unauthorized ad-hoc network. Detecting the presence of such is just as important as the previous because now there is a system on the WLAN that is advertising its presence by sending out probe requests and beacons looking for associates. With the presence of an unauthorized ad-hoc network all of the work suggested above is mute because this system has now opened your WLAN bypassing most if not all your security measures.

The last scenario to consider is the launching of a denial of service attack. If, as the network administrator, you know that the WLAN is under attack, it then allows you to take the necessary course of action. Knowledge of such an attack gives you the opportunity to inform your user community of the problem in a timely manner and increases the odds of locating the source of the attack and minimize the effects to the network.

7.9. Risk Assessment and Security Policy for WLAN

To complete the cycle every WLAN deployment needs to have a security policy and some form of a risk assessment plan. The security policy defines the acceptable configuration of the WLAN devices. The security policy addresses such things as changing the factory default configuration of the access points (i.e. default passwords for administration of the access point, the simple network management protocol (SNMP) community string, the setting of WEP, and SSID beacon). The security policy should also identify some of the risks associated with WLANs with a plan to mitigate them.

Working hand and glove with the security policy should be some type of a risk assessment of the operational WLANs. The risk assessment is used to audit the installation and correct anything that deviates from the security policy. The risk assessment should include a schedule for auditing and scanning the network for vulnerabilities that may be introduced as a result of changes in the network architecture.

8. Conclusion

Minimizing the risks associated with a wireless local area network is doable. This paper identifies some simple things that can be done up front at no cost,

such as performing a site survey to locate all access points and determine their configuration. If the access points are in the factory default configuration then that needs to change, (i.e. passwords for administration and SNMP monitoring). Also the power output of the access point should be adjusted to match the intended coverage area. During this phase of the process of minimizing the risk of WLANs, the facility boundaries should also be noted; who's on the floor above and below the access point? The objective here is to reduce the range of the signal transmitted therefore making it harder for an eavesdropper to sniff the air.

One should assume however, that someone is sniffing the air. With that assumption in mind, the next layer suggested that SSID be turned on, MAC control lists used and WEP enabled. These items make it even more difficult for an eavesdropper who is sniffing the air. Although it is possible to get around these items it's still recommended that they be in place; remember that minimizing the risk is a layered approach.

Once these items are dealt with then it is time to look at the network architecture and possibly consider redesigning the network to place the WLANs in a DMZ. In addition to network redesign, it is important that some form of user authentication is deployed and a VPN is implemented for users on the WLAN who needs access to resources on the corporate network that are protected by a firewall.

The last but just as important piece of the layer is the deployment of an intrusion detection device specifically for the WLANs. The WLAN should be monitored at all times looking for indications of activities that are in violation of the security policy and risk assessment. Let this also serve as a reminder to prepare a security policy and conduct a risk assessment. The risk assessments should include periodic scans of the WLAN in order to verify the integrity of the installation.

With all the above mentioned actions completed, the WLAN will have its' security risks minimized.

9. References

[1] Lough, Daniel L., T. Keith Blankenship and Kevin J Krizman. "A Short Tutorial on Wireless LANs and IEEE 802.11". http://www.computer.org/students/looking/summer97/ieee802.htm (June 23, 2002).
[2] O'Hara, Bob. "IEEE 802 LAN/MAN Standards Committee". http://www.ieee802.org/ (August 18, 2002).
[3] Massaro, Tiberio. "Understanding WLAN Standards". June 2002. 38 - 40. URL: http://www.wbt2.com (3 August 2000).
[4] Massaro, Tiberio. "Understanding WLAN Standards". June 2002. 38 - 40. URL: http://www.wbt2.com (3 August 2000).
[5] Massaro, Tiberio. "Understanding WLAN Standards" June 2002. 38 - 40. URL: http://www.wbt2.com (3 August 2002).
[6] Dornan, Andy. "Why Wi-Fi Will Die". Network Magazine.com. (July 7, 2002). 1 – 5. URL: http://www.networkmagazine.com/article/NMG2002071S0017.
[7] Klaus, Christopher W. "Wireless 802.11b Security FAQ". Internet Security Systems (ISS). URL: http://www.goonda.org/lists/pen-est/2001-10/msg00069.html (August 27, 2002).
[8] Harada, Richard. "802.11 Wireless LAN Security". Wireless Systems, Psion Teklogix. November 2001. URL: http://partners.psionteklogix.com/assets/downloadable/80211_Security.pdf (June 23, 2002)
[9] Harada, Richard. "802.11 Wireless LAN Security". Wireless Systems, Psion Teklogix. November 2001. URL: http://partners.psionteklogix.com/assets/downloadable/80211_Security.pdf. (June 23, 2002)
[10] Macaulay, Tyson. "Hardening IEEE802.11 wireless networks". February 18, 2002. Available from: URL: http://www.ewa-canada.com/Papers/Hardening_802.11.pdf. (June 23, 2002).
AirDefence, Inc. "Wireless LANs: Risks and Defenses", Available from: http://www.airdefense.net (August 18, 2002)
Albright, Brian. "Enterprise users drive wireless data growth." Frontline Solutions May 2002 (2002): 44-46.
Borisov, Nikita. Ian Goldberg. David Wagner. "Security of the WEP algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (3 August 2002).
Carney, William. "IEEE 802.11g New Draft Standard Clarifies Future of Wireless LAN." URL: http://www.securitytechnet.com/resource/hot-topic/wlan/802_11g_whitepaper.pdf (23 June 2002).
Chandra, Prapul. "802.11 Security." 23 May 2002. URL: http://www.wirelessdevnet.com/articles/80211securit_2 (3 August 2002).
Chandra, Prapul. "Living With 802.11 Security…Securing 802.11 WLANs (Part 2 of 3)." 7 June 2002. URL: http://www.wirelessdevnet.com/articles/80211securit_2 (3 August 2002).
Cheung, Fredy. "Wireless LAN Security Basics." 15 March 2002. URL: http://asian.cnet.com/newstech/wireless/0,39003048,39031910,00.htm (3 August 2002).
Cheung, Fredy. "Wireless LAN Security Basics." URL: http://asia.cnet.com/newstech/wireless/0,39003048,39031910,00.htm (3 August 2002).
Danielyan, Edgar. "IEEE 802.11." The Internet Protocol Journal. Vol. 5 Number 1. March 2002 2 – 13. URL: http://www.cisco.com/warp/public/759/ipj_5-1.pdf (23 June 2002).
Davies, Joseph. "Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000 Internet Authentication Services". March 2002. Available from: http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/80211corp.doc {Accessed June 23, 2002).
Intel. "Wireless Security and VPN: Why VPN is Essential for Protecting Today's 802.11 Networks." URL: http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/WLO_Security_WP_LOWrez1.pdf
Interlink Networks. "A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points." Revision C. URL: http://www.interlinknetworks.com/graphics/news/wireless_detection_and_tracking.pdf (3 August 2002).
Johnson, Brad C. "Wireless 802.11 Security: Questions & Answers to Get Started." URL: http://www.systemexperts.com/tutors/wireless-qanda.pdf (3 August 2002).
Kapp, Steve. "802.11: Leaving the Wire Behind". On the Wire. January/February 2002. URL: http://www.computer.org/internet/v6n1/w102wire2.htm (3 August 2002).

Mishar, Arunesh and William A. Arbaugh. "An Initial Security Analysis of the IEEE 802.1x Standard". CS-TR-4328 UMIACS-TR-2002-10. Department of Computer Science University of Maryland College Park, Maryland 20742. http://www.cs.umd.edu/~waa/1x.pdf (August 3, 2002).
Meserve, Jason. "The scoop on wireless LAN snoops." Network World Fusion 17 September 2001. URL: http://www.nwfusion.com/news/2001/0917infra.html (3 August 2002).
Nobel, Carmen. "Fledgling WLAN spec picks up early support." EWeek July29, 2002 (2002): 1, 14.
Nobel, Carmen. "802.11a networks: Stronger and faster." Eweek May 13, 2002 (2002):25
Snow, Stephen. "Avoid wireless interference." Frontline Solutions May 2002 (2002): 38
Ohkhirst, Frank J. "Wireless Troubleshooter." CRN May 6, 2002 (2002):95
Roshan, Pejman. "802.1X authenticates 802.11 wireless." 24 September 2001. URL: http://www.nwfusion.com/new/tech/2001/0924tech.html (3 August 2002).
Wexler, Joanie. "Security alternatives." Network World Fusion 15 August 2001. URL: http://www.nwfusion.com/newsletters/wireless/2001/00948169.html (3 August 2002).
(23 June 2002).
Signa Services. "Best Practices for Deploying Wireless LANs." URL: http://www.mobileinfo.com/PDF/Best%20Practices%20for%20Deploying%20Wireless%20LANs.pdf (3 August 2002).

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event