Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defence In Depth: Preventing Going Hairless Over Wireless

Wireless networks are fast establishing themselves as a part of the information technology infrastructure. The security mechanisms have yet to provide adequate protection to the data passed by wireless systems and to the "wired" systems to which they connect. Whilst encryption, authentication and authorization are necessary elements in the security equation there are other techniques that can be used in defense. This paper discusses some techniques that utilize modifying radio wave behavior (directional antenna and low...

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

DEFENCE IN DEPTH:
PREVENTING GOING HAIRLESS OVER WIRELESS

Jonathon Berry
Version 1.3
17 April 2002

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Wireless networks are fast establishing themselves as a part of the information technology infrastructure. The security mechanisms have yet to provide adequate protection to the data passed by wireless systems and to the "wired" systems to which they connect. Whilst encryption, authentication and authorization are necessary elements in the security equation there are other techniques that can be used in defense. This paper discusses some techniques that utilize modifying radio wave behavior (directional antenna and low power transmissions) as a means to add depth to security. The paper also presents some options, such as file compression and burst transmissions as considerations for reducing the probability of intercept.

Introduction

Governments, business and home users are increasingly deploying wireless networks. Even the ubiquitous PDA is being attached to these systems that are becoming the default road warrior tool. However, according to Schulz (2002), "given that a large proportion of organizations adopt at least some basic form of security in conventional networks, the all-too-typical neglect of security in wireless networks is in many respects an enigma". Certainly, there has been much written about the plethora of security problems associated with wireless working. But wireless working is popular and has clear business advantages, it would be difficult to abandon wireless, but it can be improved.

The general trends to rectify wireless security problems in wireless are based around stronger encryption and robust authentication. These methods are essential if any confidence is to be placed in wireless working. In this essay I propose some *additional* methodologies that may be used to enhance security in wireless working. These techniques, in effect, add depth to the overall security plan. The technological solutions are needed to defend the vulnerabilities presented by wireless working, but there are also many practical actions that can reduce those vulnerabilities. The issues raised here will hopefully also raise the readers' awareness of wireless vulnerabilities and workings.

Wireless working presents a new medium for connectivity. Instead of the trusty CAT 5 cable radio waves and IR beams are used. This paper focuses mainly on the radio dimension of wireless. With wireless, the worker is no longer bound to the limitations of a physical IT infrastructure. The decision to use wireless is a business risk decision and it is beyond the scope of this paper to identify valid business reasons to adopt wireless working, but it is sufficient to say that there are valid reasons and market pundits predict that wireless usage will increase.

What security is inherent in wireless?

This paper is not intended as a critique of the current set of techniques inherent in wireless protocols, or as an advertisement for third party solutions. Many other writers

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

have described wireless security weaknesses and it is generally accepted that at present wireless working is inherently insecure. For example, by default, systems do not employ encryption. In any case, as noted by Sandberg (2001), wireless uses the "Wired Equivalent Privacy algorithm, or WEP" and some weaknesses have been discovered. Furthermore the authentication is poor, and passwords are sent in plain for most out of the box systems.

What are the threats and vulnerabilities?

The vulnerabilities of wireless, conceptually, are somewhat the same as for cable; interception, interference/manipulation, intrusion and denial. Even the encryption used provides little defense. Verton (2001) quotes a security professional who was able to "read WEP-protected traffic, … inject traffic onto WEP-protected networks, we can modify WEP-protected data". Such activities are increasingly becoming a feature of wireless working and can be problematic to prevent because of the nature of the medium, and the origin of an attack is difficult to isolate.

Wireless working creates a new threat vector and presents new vulnerabilities. Now your network, and the valuable information it holds can be accessed by another means. The techniques and equipment used are different, but the results are the same. Cisco's Systems (2001) provides a good overview of wireless security issues, identifying access control and privacy as key issues. Armstrong (2002) describes vulnerabilities relating to "passive attacks to decrypt traffic" and "active attacks to inject new traffic". Essentially, vulnerabilities may be divided into two camps; vulnerabilities by virtue of receiving traffic (interception) and vulnerabilities by virtue of intrusion. Combinations thereof are most likely, with hackers using captured (intercepted) passwords to enter the network for subsequent actions.

Despite this doom and gloom, wireless is taking off and not necessarily for the right reasons. Lowber (2002) predicts that with respect to email, 90% of the people using wireless don't really need it! That's a lot of traffic that could be better protected elsewhere. It raises concerns about how wireless is being used and demonstrates a lack of policy with respect to its employment. But, the need for security in wireless networks is not news. Part of the problem is, as noted by Kabara (2001) that "most security protocols and architectures are designed for wired networks and may not be effective in wireless networks." Yet invariably, these are what are being deployed.

Perhaps the most publicized exploitation of wireless vulnerabilities has been through what is called "war driving" and "war walking". Where a roaming party connects to wireless LAN by using the commercially available devices. Much has been written about this topic and it is a real threat. However, war driving is not the only method by which access to networks may be gained. A malicious user may gain entry to a poorly secured network from afar using a directional antenna. It is the range and pervasiveness of wireless (radio) that makes it vulnerable.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

To gain a perspective on distance, Kapp (2002) provides some working ranges; "Typical range of 802.11b is 100-150 ft at 11Mbps, 130-150 ft at 5.5 Mbps and 250-350 ft at 2Mbps". It would appear that the problem is only going to get worse. The insatiable business desire for extended range, greater throughput and more efficient use of the spectrum has led to the use of two or more antenna for a system. Known as "diversity antenna" these systems "provide two separate antennas, for one radio, and signal filtering and decision making software selects the better signal (highest power, best quality . ..)." (Kapp, 2002). This increases the signals available for intercept at any given moment as a malicious user now has two transmissions to pick from.

This may sound somewhat complex, but Kabara (2001) notes that, "most wireless networks rely on the inherent technical complexity as a principle means of security". This is reliance upon the "security by obscurity" principle. However, a simple search on the Internet reveals much information that can be used to help exploit wireless networks. There is plenty of information on the Internet for the determined attacker to build an effective system to exploit wireless weaknesses. The enthusiastic can build an antenna from a Pringles can with instructions from Flickenger, R., with impressive results. The more sophisticated or sinister hacker may prefer the anonymity given with greater distance from the target. Frohne, R., claims that by using two "Primestar dish antenna" he was able to achieve working over "a line of sight path … around 10 miles". This demonstrates the effectiveness of a good directional antenna and the "gains" will be realized in both the transmit and receive legs. Shipley, P., provides useful information on how to construct a war-driving kit and some known access points in San Francisco.

What is being done to further defend wireless?

The IEEE is addressing the known problems associated with wireless security. However, Lowber (2002) notes that "End users will take the path of least resistance" and that "Enterprises that have no wireless email policy . . .risk losing control over security and over their users". This is the start point for any security. The policy must be in place and the wireless network forced to conform to it. Mimoso (2002) refers to a successful security system that has at its foundation, "Defence in Depth", this was initiated by "establishing policies based on principles of minimum access and least privilege". Security practitioners would be wise to do the same. The organisation must identify a clear need for wireless working and having done that, keep access at a bare minimum.

Other writers have already proposed stronger encryption, authentication and VPN's. However, Ruley (2001) cautions, "if you plan to implement a VPN, you'll want to disable guest access and require non-blank passwords". It is obvious that techniques using (strong) encryption and authentication are required for wireless working. Industry consensus leads the security planner to two conclusions:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- At the very least, those intending to protect networks that have wireless connectivity, i.e. an wireless access point, then a firewall and strong authentication are required at the point of entry.

- If you wish to protect the data being transmitted then strong encryption is required between the access point and the client, and this should be mandatory.

The ideas in this paper do not seek to relieve the need for the aforementioned defences. What this paper proposes is some techniques that can add more layers to the security onion. In some cases the proposals here may be untenable from a business point of view. It is up to the organisation to decide how it manages it's risk. In some cases the concepts have not been incorporated in any product that I have been able to find on the market. However, security professionals may create the demand!!

How wireless transmissions work

The measures I propose in this paper require some knowledge of how radio works. This section serves as an introduction to how radio propagates. The two figures below are taken from ZoomAir's web site. The radiating lines represent the radio signal and may be likened to the ripples on a pond when a stone has been thrown in. The diagrams demonstrate the difference between directional and non-directional antenna. With the directional antenna the signal is focussed and, with the same power output, will have greater range. The signal distribution in the horizontal plane is the primary concern, but wireless workers in multi-storey buildings should be aware of radiation patterns in the vertical plane as well. Figure 1 shows the omni-directional nature of the "monopole" antenna used by most wireless clients. Because the clients position, relative to the access point changes, an omni directional antenna is more practical. Figure 2 shows the radiation pattern of a directional antenna. Whilst there is still radio signal going in all directions, it is much stronger in one direction and weaker elsewhere. The signals radiating out of the desired direction are referred to as side and back lobes. Directional antenna is more practical for point-to-point links and when station physical positions do not change often. Through the manipulation of the antenna structure, a variety of radiation patterns can be created. It is possible to widen the beam that the signal covers, in the same way a spotlight can be focused or diffused.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

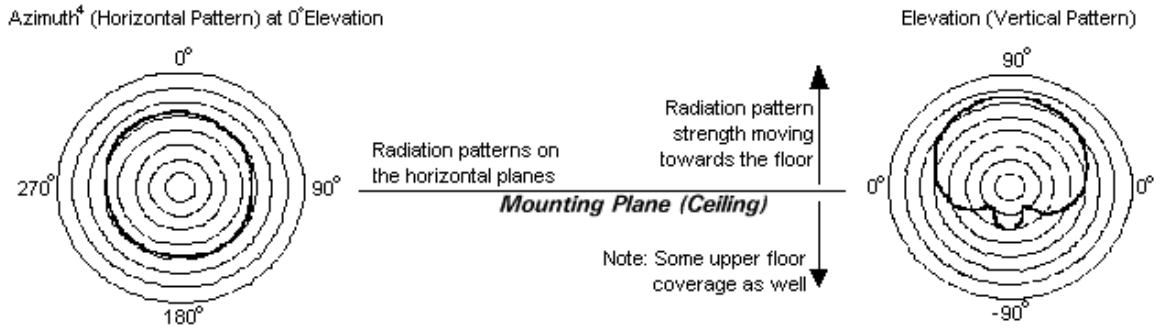

Fig 1. An omni-directional antenna.

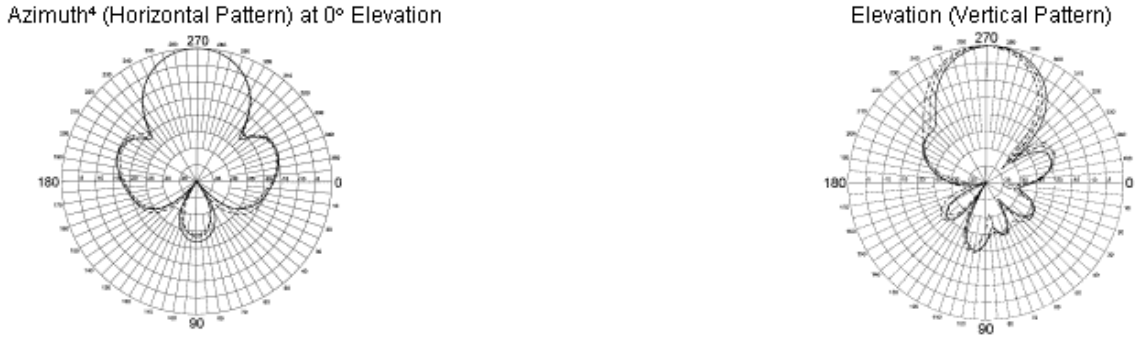

Fig 2. A directional antenna.

A wireless network will use at least one Access Point (AP), which is hard wired in to the network and provides connectivity to the roaming clients. Connection to the network may be client or AP initiated, but is generally AP controlled.

Defensive measures

The best defense against wireless is to not use it. However, this may not always be an option or systems are in place and you must secure them. Many of these techniques are defensive in two ways; they make interception difficult (and hence detection) and they make network penetration more difficult. By making interception more difficult, you are in fact lowering the "radio signature" or disguising in a way, the presence of a wireless network. If malicious users do not know or cannot detect the presence of your wireless network, then chances of it being exploited by that means are significantly reduced. The military refer to such methodologies as "transmission security" or TRANSEC. The US DOD definition is "The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis". Some of these techniques are explained below:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Use low power[1]. Why shout when you can whisper? There is no requirement to boom out at high power settings if the legitimate receiving party is next door. Some systems will allow for the manual adjustment of gain (power). Gain used should be the minimum for satisfactory working.

- Decrease transmission time. The use of "burst" transmissions, where data is sent all at once, will reduce probability of intercept by decreasing the time window during which the signal will be intercepted. This may be done in one of many ways;

  - Compress files. The ubiquitous WinZip application or other file compression utilities can turn a possibly lengthy transmission into a brief communication. Any intercepting party has a far more difficult job trying to reconstitute a compressed file with missing data than a non-compressed file.

  - Be able to disconnect. Where applicable, ensure that the system to be used allows users to disconnect when they don't need to be connected. Wireless is "chatty" as stations tell each other where they are and how they are receiving. This talk betrays the existence of the network and is not necessary until either party needs to connect.

  - Create, store, and transmit. Applications such as email clients allow you to work offline and reconnect as required. A prudent user can connect, download their mail and then disconnect the wireless connection. They may now answer email as necessary, storing replies in the "Outbox" before reconnecting. Upon reconnection the communications path is used more efficiently as mail is sent at the links capacity, once again reducing transmission time. The same technique could be applied if working on a document or other file. Save locally and transmit back to the network later in one hit.

  - Use highest speed available. As technology improves so will the capacity of wireless equipment and software. Keeping abreast of developments and having sophisticated wireless networks makes exploitation more difficult, consider it a form of patching. As time goes on, transmission speeds will be improved through better hardware and software.

- Time of day. If your traffic is not needed urgently, then why not wait for the silent hours before transmitting? This implies some knowledge of malicious users, but if you know your local war drivers are active between 6 pm and 10 pm then consider transmitting outside of those hours. This technique is most applicable when

[1] Ironically, using high power will increase throughput and therefore decrease chance of intercept. However, for "always on" systems this may not be a consideration and low power is preferred from a security perspective.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

organisations are synchronizing data or backing up data en masse, between buildings.

- Direct the transmissions. If you don't want everybody to intercept your signals, don't transmit them in a manner where they are available. A radio signal may be likened to a network in broadcast mode, everyone, if they so wish, may collect the data. The difference being they need not be physically connected.

  - Directional antenna. A directional antenna is one that has been constructed so that the majority of the signal is transmitted in a certain direction. The same can be said for a receiving antenna, it is focussed in a certain direction, the most common type being a TV aerial. This makes the task for a malicious user to penetrate the network via this antenna more difficult, as they have to get in it's "line of sight". Traditionally the wireless client uses an omni-directional antenna (monopole).

  - Reflectors. A reflector is normally a part of a directional antenna. It is used to reflect the radiated signal in the desired direction. Reflectors could also be used to capture (refocus) incoming signals, as satellite dishes do, allowing the transmitting station to use less power. Reflectors could also be used to block or reflect signals coming from undesired directions.

- Utilize physical barriers. Radio and IR, like visible light can be physically blocked. Radio will penetrate walls etc, but the signal is attenuated (weakened) relative to passage through free space. If the physical object is large/dense enough it will at least weaken the signal and at best block the signal. This will create what is known as a "radio shadow". In the radio shadow the signal strength is substantially reduced and interception dubious. By understanding the radiation pattern of the antenna you intend to use, siting can be made to create radio shadows where it is desirable for the signal to be weak/absent.

- Encryption. Clearly data should be encrypted. Encryption of the communication channel creates a transmission overhead and may be inefficient for certain types of traffic. Encryption does not have to be done at the transport level. For applications such as email or for file exchanges, wireless workers can encrypt the data itself. For example, PGP can be used to encrypt files and email with a 2058 bit key, which is far stronger than WEP or WTLS.

- Physical traits. Avoid sticking antenna in clearly visible positions. A malicious user does not necessarily have to "war drive" to find a wireless network. The judicious positioning of antenna on a building is done such that they are not clearly visible from street level, but are still functional. It is possible to buy antenna inside housings, which can be used to further camouflage their presence.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Deployment Examples

This section will describe some practical scenarios where security conscious antenna siting has been employed. With respect to the AP the greatest concern is that they generally have a greater transmitting power. If you know your wireless workers will be within a confined area, say the entire floor of a building, then you can design antenna placement around this knowledge. For example, consider placing more powerful directional antenna for the AP at the physical periphery, but pointing back in to the centre, rather than radiating out form the centre and beyond. The antenna could be structured such that signal is reflected back in towards the centre, further reducing side and back lobe transmissions that could be intercepted. This method would also make unauthorized entry more difficult as the malicious user would need to get inside the area of coverage, i.e. in your physical workspace, to get a good signal. This option would be daunting to the most daring hacker!

Another scenario could be to use directional antenna at the client. If you know that your workers use their wireless to gain access to the network during meetings in the conference room only, then you have a fixed spot from where they are likely to be transmitting. Equipping these users with directional antenna will:

- Reduce their radio signature, as they are no longer using omni directional antenna, and,

- Allow them to use less power, as the signal is focused, thus decreasing the area from which the signal may be intercepted.

Figure 3, below demonstrates poor siting on a rooftop. The grey box represents a lift shaft, which for our purposes attenuates the signal. The transmitting antenna here is omni-directional and can be received by anyone who can obtain a readable signal from it. The wireless network is detectable and becomes a target. If no defenses are present on this network then the malicious user will be able to intercept data, gain entry to the network and possibly insert data into the network. Clearly, none of these activities is desirable!

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

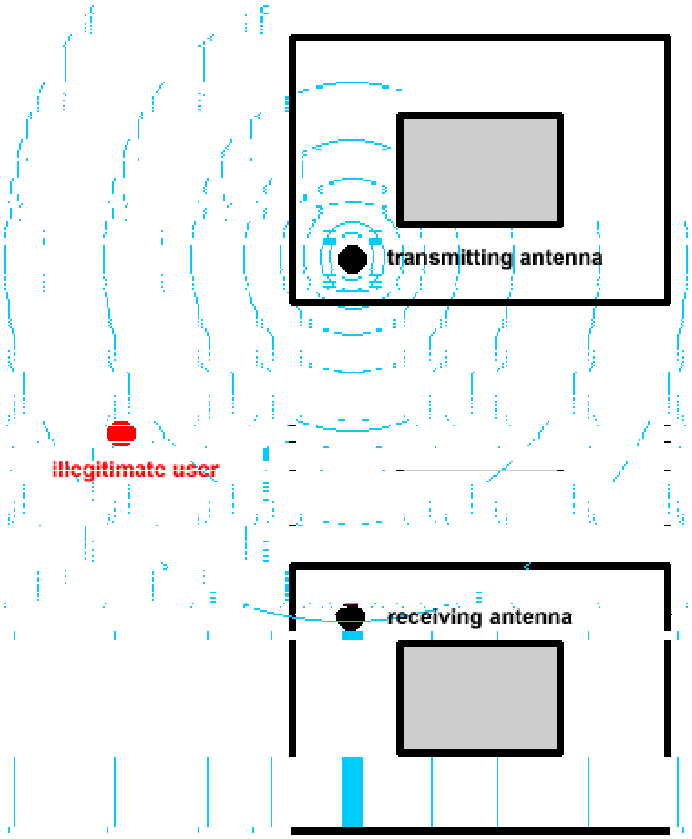

Fig 3. Poor antenna siting.

Whereas, Figure 4, below, show use of several techniques for better security. The antenna being used is directional. This limits the possibility of intercept by the illegitimate user. They would have to get in the line of sight of the transmitting antenna, which is of limited area or attempt to intercept one of the weak side lobes. Furthermore, power output has been decreased on this transmitter, limiting the range of the transmission to what is required. This further reduces the possibility of intercept. As a bonus, the use of the directional antenna also makes it difficult for the illegitimate user to gain access to the network via the wireless antenna, once again, unless he/she can get in its path. This siting has also used physical objects, in this case the lift shaft, to block the transmission from going in directions it is not required in.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

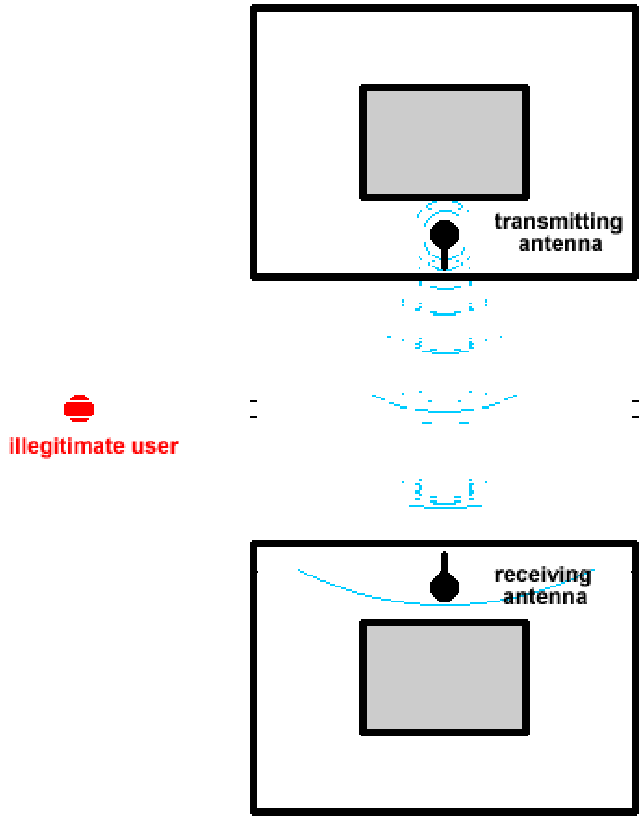

Fig 4. Desirable antenna siting.

Conclusion

Wireless working is here to stay. There are sound business reasons for using wireless and as the technology becomes increasingly popular security professionals will need to be able to defend the wireless network. The security mechanisms inherent in wireless are not yet mature. The vulnerabilities are widely known and can be exploited readily. Therefore, you cannot yet trust the security built in to wireless, but other systems can be employed and there are already security tools that can be used to defend wireless networks. Strong authentication, strong encryption and firewalls are generally what these systems will provide.

But, security solutions are not always technological. They do not have to be out of a box or a change to a check box in an application. Security has many dimensions and some security can be afforded by common sense, practical measures. By understanding your networks and the technology they employ, you can be to use new innovative techniques to defend them. The more you begin to customize your network, the more robust it will be and more difficult to exploit. For wireless, this paper has suggested limiting power

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and using directional antenna to add layers and therefore depth to the security plan. This will make the network more difficult to detect and therefore exploit. Consideration should be given to how workers use the applications associated with the wireless network. Techniques such as file compression/encryption, burst transmissions and changing transmission time can make the hacker/interceptors job more difficult.

© SANS Institute 2002, Author retains full rights.

References

Armstrong, Illena. "Todays telecommuting world". Secure Computing, February 2002. (2002): 27-29

Cisco Systems. "Overveiw Wireless LAN Security". 1 November 2001
URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
(4 March 2002)

Convery, Sean., Miller, Darren. "SAFE: Wireless LAN security in depth." 15 January 2002.
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
(9 April 2002)

Flickenger, Rob. "Antenna on the Cheap (er, Chip)". 5 July 2001
URL: http://www.oreillynet.com/cs/weblog/view/wlg/448 (8 February 2002)

Frohne, Rob. "Use a Surplus Primestar Dish as an IEEE 802.11 Wireless Networking Antenna".
URL: http://www.wwc.edu/~frohro/Airport/Primestar/Primestar.html (2 April 2002)

Haber, Lyn. "Third party solutions". ZDNet Tech Update. 28 March 2002
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2859110-2,00.html
(14 April 2002)

Kabara, Joseph., Krishnamurthy, Prashant. and Tipper, David. "Information Assurance in Wireless Networks". 31 August 2001.
URL: http://www.cert.org/research/isw/isw2001/papers/Kabara-31-08.pdf

Kapp, Steve. "802.11:Leaving the wire behind." IEEE Internet Computing January-February 2002 (2002): 82-85.

Lowber, Peter. "Wireless Email: Strategic Imperative or Headache?" 21 March 2002.
URL: http://www4.gartner.com/DisplayDocument?doc_cd=105314

Mimoso, Michael S., "Olympic network security envy of the enterprise". Security News and Analysis, SearchSecurity. 10 April 2002.
URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci815960,00.html
(11 April 2002)

Ruley, John D. "Use a VPN to secure your wireless network". Windows 2000 Magazine September 15, 2001 (2001). 59-60

Sandberg, Jared. ZDNet News, "Hackers poised to land at wireless AirPort", 4 February 2001
URL: http://zdnet.com.com/2100-11-527906.html?legacy=zdnn 10 April 2002

Schulz, Eugene. "Wireless Network Security Concerns". Computers and Security. (2002). Vol 21, No. 1: 11-12

Shipley, Peter. "Open WLANs, the early results of WarDriving"
URL: http://www.dis.org/filez/openlans.pdf (23 January 2002)

US Department of Defence, "DOD Dictionary of Military Terms", 19 December 2001
URL: http://www.dtic.mil/doctrine/jel/doddict/data/c/01140.html 8 February 2002

Verton, Dan. Computerworld. "Black Hat: Users warned about wireless LAN holes". 12 July 2001

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO62144,00.html
ZoomAir. "ZoomAir Antennas and Options.
URL: http://www.connectronics.com/zoom/zaaops.shtml (23 January 2002)

Biliography / Other sites of interest

http://standards.ieee.org/wireless/
http://grouper.ieee.org/groups/802/11/index.html
http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
http://airsnort.shmoo.com/

© SANS Institute 2002, Author retains full rights.

Last Updated: August 31st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced