Global Information Assurance Certification Paper

Denial of Service Attack Against an 802.11b Network Using Wide-Band Frequency Interference

Morgan Bailey
GCIH Certification Practical Version 3
Submitted 7/12/04

Table of Contents

Statement of Purpose ***4***

The Exploit ***5***

Name **5**

What is a Denial of Service Attack? 5

Operating System **5**

Protocols/Services/Applications **5**

Variants **9**

Description **9**

CSMA/CA 9

Basic Radio Theory 11

Basic Antenna Theory 12

Equipment 14

2.4 GHz ATV Transmitter 14

14 dB gain directional grid array antenna. 15

Signatures of the attack ***17***

Victim's Platform **18**

Source Network **19**

Target Network **19**

Network Diagram **19**

Network Components **19**

Stages of the attack ***21***

Reconnaissance 21

Scanning 25

Exploiting the System 25

Keeping Access 28

Covering Tracks 28

The Incident Handling Process ***29***

Preparation 29

Identification 30

Containment and Eradication 31

Recovery 33

Lessons Learned 33

Additional Notes ***35***
Works Cited ***37***
References ***38***
AusCert Advisories: 38
CERT Vulnerability Notes: 38
Applications: 38
Appendix ***39***

Table of Figures

FIGURE 1. SIMPLIFIED CSMA/CA METHOD OF OPERATION. 11
FIGURE 2. 13CM (2400MHZ) FM ATV TRANSMITTER (WWW.TVHAM.COM) 15
FIGURE 3. ANTENNA RADIATION PATTERN 15
FIGURE 4. REPRESENTATION OF A HEALTHY SNR 17
FIGURE 5. REPRESENTATION OF AN UNHEALTHY SNR 18
FIGURE 7. RECONNAISSANCE PHOTO OF ANTENNA TYPE, AND PLACEMENT 24
FIGURE 8. NETSTUMBLER RESULTS FROM SCANNING. 25
FIGURE 9. TRANSMITTER FREQUENCY SETTINGS. 26
FIGURE 10. RESULTS OF 802.11 SIGNAL JAMMING. 27

Tables

TABLE 1. THE 802.11B FREQUENCY SPECTRUM 8
TABLE 2. COMMON POWER CONVERSIONS 12
TABLE 3. FIREWALL RULE SET. 20

Statement of Purpose

The exploit that this paper will cover is a Denial of Service (DoS) attack against an 802.11b network. In this writing, we will not attack the network using traditional methods, but by "thinking outside the box" and exploiting an obvious, but often overlooked vulnerability that resides at the core of the wireless communication medium itself.

This exploit is extremely effective due to its simplicity and ease of implementation, and is nearly impossible to defend against. Because this exploit targets the core of all radio based, wireless communications all commercially available 802.11 equipment on the market today is vulnerable, and currently there is no way to close this hole short of removing wireless all together.

This paper will cover the theory of the vulnerability, and how the actual exploit works. All protocols, services, and applications and theory used or affected by this attack will also be explained with enough detail to fully understand the footprint of the attack and why the vulnerability exists. We will then perform an actual attack on an existing wireless network in a lab environment. The attack will be presented in a step-by-step format, and every procedure necessary for the successful exploitation of the network will be covered in detail.

Once the attack has been successfully executed, we will change to the defensive point of view. We will use the six steps of the Incident Handling process developed by the SANS Institute in attempt to identify the source of the attack and close the holes in our network. We will also use the knowledge gained by this incident to protect our network from this type of attack in the future, if possible.

This paper will cover all aspects of this incident, from the initial stages of the attack to the Incident Handling process using a scenario based on what could be a real world situation. The purpose of this is to attempt to make it easier to realize the impact this exploit could have on a real networked environment that heavily depends on 802.11 wireless communications.

The Exploit

Name

Denial of Service Attack on a wireless network using Wide Band Interference.

At the start of this writing, April 23, 2004, a published advisory on this vulnerability did not exist. As of March 15th, 2004, AusCERT published an advisory, vulnerability number AA-2004.02. In this advisory, 802.11 equipment was used to exploit this vulnerability by modifying the drivers used to operate the device. Although the same results are obtained, the vulnerability in this writing is exploited using different methodology, which may be more effective in our DoS attack. The reason for this being that the jamming equipment used in this writing was not designed for an 802.11 network, and therefore, does not inherit many of the limitations of existing commercial 802.11 equipment, such as limited power output, and bandwidth restrictions. This will allow us greater flexibility in the execution of our attack.

What is a Denial of Service Attack?

A Denial of Service (DoS) attack is an attack on a system, or a portion of a system, rendering a service or a system unavailable for at least a temporary amount of time. DoS attacks do not usually destroy data or invoke physical damage, but they often results in monetary loss.

Operating System

This vulnerability does not directly affect any operating systems. Although this writing concentrates on the 802.11b extension of the wireless protocol, All 802.11 devices are vulnerable to this attack.

Protocols/Services/Applications

The 802.11b Wireless Standard

A wireless LAN (WLAN) is a data transmission medium used to facilitate communications between computers and other computing devices via radio communications rather than physical cable. In 1997 The Institute of Electrical and Electronics Engineers (IEEE) developed the 802.11 protocol as the standard for wireless LANS. The initial version of 802.11 allowed for speeds of up to 2 Mbps in perfect conditions. The IEEE quickly recognized that the data transmission rates were too limited for most commercial and industrial operating environments to justify a WLAN deployment as a practical investment. To overcome this roadblock, the 802.11 standards were amended, and in September of 1999 the 802.11b standard was born. The new standard supported speeds of up to 11 Mbps, which made it more comparable to the

current operating speeds of its wired counterpart, and because 802.11b is based on the current Ethernet standard, it allows the administrators and network engineers to seamlessly integrate wireless technology into their existing infrastructures. The industry immediately grasped the potential of 802.11b and products and hardware were rapidly developed and deployed.

Like all IEEE 802 standards, the 802.11 standards operate on the bottom two levels of the Open Systems Interconnection (OSI) model, the physical layer, and the data link layer. The core operation of the 802.11b standard is the same as the original 802.11 standard. The 802.11b specification changes occur only at the physical layer of the OSI model, adding the ability to support a higher data rate.

There are three different physical layer specifications defined for 802.11, two of which are spread spectrum techniques, which use radio transmission as the communication medium, and the third uses an infrared specification, which is beyond the scope of this paper. It is important to note that although these three schemes are all part of the 802.11 standards, they are not compatible with each other, as their methods of operation greatly differ.

Spread spectrum is a communications technique that was developed by the United States Military and was patented in 1942. Spread spectrum signals are hard to detect, hard to intercept and decode, and are interpreted as noise by another receiver not designed for this type of transmission. It is more resistant to jamming and other forms of interference. It is for these reasons that spread spectrum communications are preferred by the military. By using a wide bandwidth and low power, it is able to overcome certain disadvantages of its counterpart: Narrow Band Transmission. Narrowband transmission is a communications technique that only uses enough frequency spectrum to transmit the desired information, and nothing more. An example of this would be your car radio. This is directly opposite of spread spectrum since it uses a much wider bandwidth than is required to transmit information.

The 802.11b WLAN standard operates within the Industrial Scientific and Medical (ISM) band of 2.4 GHz reserved by the Federal Communications Commission (FCC) for unlicensed radio communications. This means that as long as regulations are observed for power output, and antenna gain, anyone may operate a transmitter in this band without a license or special training. There are many other devices that share this band. A common example of this is a household microwave oven. Microwave ovens also occupy the ISM-2.4 GHz band because the electromagnetic radiation emitted at 2.4 GHz is particularly suited for boiling water and heating food. Some other examples of devices that use this band are baby monitors, cordless phones, garage door openers, and several more. The reason for this band being unlicensed is self-evident. Can you imagine having to apply for a FCC license to microwave a pizza, or open your garage door?

With all of these devices using the same band as our wireless hardware, certain methods of transmission need to be implemented to ensure avoid signal degradation. The 802.11 standard uses two different spread spectrum techniques to overcome this problem, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum, (DSSS).

FHSS uses a simple algorithm to quickly switch frequencies to avoid interference from other devices operating in the same bandwidth. The FHSS scheme divides the entire 2.4 GHz band into 75 non-overlapping sub-channels (for use in the United States and Europe) with each channel having a bandwidth of 1 MHz. The hopping sequence must hop at a minimum of every 2.5 times per second and over a minimum range of 6 channels. The sending and receiving end negotiate on a channel-hopping pattern, and data is sent on the agreed sequence of sub-channels. Each conversation takes place with a different hopping pattern that is designed to avoid the chance of two senders using the same channel simultaneously.

Although FHSS allows for very simple and efficient radio design, data transmission rates when using this technique are limited to no more than 2 Mbps. This is primarily due to restrictions set forth by the FCC. These restrictions limit the bandwidth of each channel to 1 Megahertz (MHz), and force FHSS systems to utilize the entire 2.4 GHz frequency spectrum. This leads to a high amount of overhead used just for hopping, and the side effect is low data throughput.

DSSS, on the other hand, divides the band into 11 channels for use in the United States. These channels center on frequencies in a portion of the Industrial, Scientific and Medical (ISM) band from 2.412-2.462 Gigahertz (GHz) in steps of 5 MHz. (See Table 1 for list) Each channel has a bandwidth of 22 MHz, and since the channels are actually smaller than their available bandwidth, only channels 1, 6, and 11 can be used without a threat of interference from existing channel overlap.

DSSS encodes all data transmitted over the air using an encoding method referred to as “chipping”. In this method, each data bit is translated to a redundant data sequence called “chips”. These chips are then sent over the air, and decoded by the receiver. Using this technique, data can be exchanged more reliably with an unfavorable signal-to-noise ratio (SNR) due to low transmitting power, or third party interference, because the information is being spread into many different redundant data bits across the bandwidth of the assigned channel.

Table 1. The 802.11b Frequency Spectrum

Channel	Bottom (GHz)	Center (GHz)	Top (GHz)
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

Here is an extremely simplified example of this technique:

If you were to send the sequence 01010 to a peer over a very noisy or weak radio connection, you could agree beforehand to send every bit in the sequence 11 times. The sequence of 01010 would be translated to:

00000000000
11111111111
00000000000
11111111111
00000000000

The peer would receive the new sequence and break it down to the original. This ensures that if several bits of that sequence were corrupted, or fail to be received correctly, there is still a decent chance that the message could be reassembled.

The main goal that drove the development of the new 802.11b standard was to increase maximum data transmission rates to 11 Mbps. This was accomplished by standardizing the usage of the DSSS physical layer technique, rendering the use of FHSS obsolete. They then revamped the DSSS encoding methodology using much more complex coding mechanisms and algorithms to modulate data more efficiently, and to overcome some of the fundamental problems with the transmission of data in a noisy environment. Thus, 802.11b emerged.

The 802.11b standard has rapidly gained popularity due to its low investment and implementation costs, and relatively high performance. The flexibility of having a mobile network connection quickly overshadowed the benefits of a faster wired network.

Variants

At the time of this writing a published variant of this exploit was not found. The vulnerability that is being exploited in this paper is one that is commonly known and exists in virtually all types of radio-based communications. There several DoS exploits for the 802.11 protocols, but most if not all concentrate on the network and transport layers of the TCP/IP protocol, and are not similar except in the resulting effects. The most similar, publicly disclosed, variation of this attack was published by AusCERT, vulnerability number AA-2004.02, on March 15th 2004.

Description

What is the Vulnerability?
The vulnerability described here is one that plagues all forms of radio communications: Radio Frequency Interference (RFI) or also known as *harmful interference*. According to part 15.3 of the FCC Rules and Regulations harmful interference is defined as:

"Any emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter."

For an in-depth description and explanation of Radio Frequency Interference, refer to the ARRL RFI Book, published by the American Radio Relay League.

RFI can be more easily understood if compared to static on an AM radio or a cordless phone. As we have read in previous sections of this paper, 802.11 is also a radio based protocol meaning that it is just as susceptible to interference as other forms of radio based communications. While we can usually deal with a small amount of static or noise reception on a voice communications platform, RFI is much more detrimental to the transmission of data. Wireless Access Points (WAP) and other 802.11 communications devices are not selective in what they receive. They cannot chose to only receive valid 802.11 data. They must receive any communications that are being transmitted at their same frequency. According to Federal Communication Commission rules Part 15 ,these devices must not cause harmful interference and must accept any interference causing undesired operations. Considering this fact, it is very simple to generate malicious interference in order to intentionally disrupt 802.11-based communications. This is commonly referred to as jamming, or jabbering.

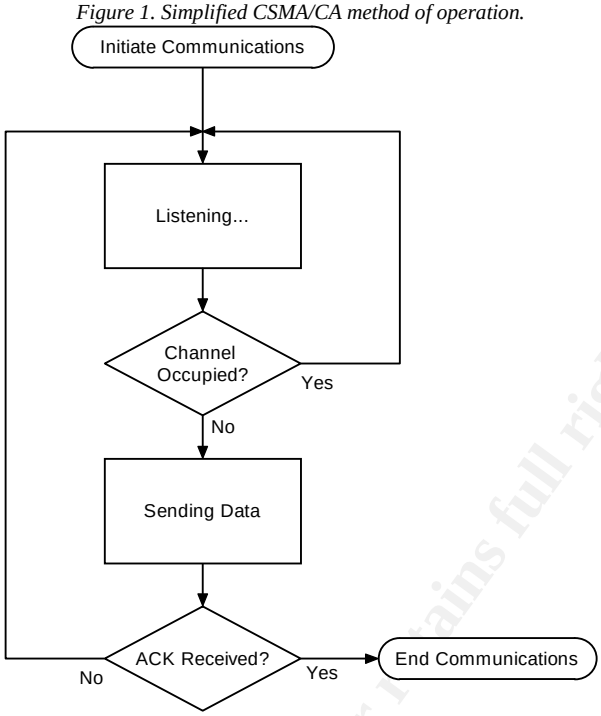
CSMA/CA
Jamming 802.11 communications is simple and extremely effective. This is primarily due to the nature of the way radio communication works, as well as the methods that 802.11 uses in attempt to avoid traffic collisions. 802.11 makes

use of a protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA attempts to avoid collisions over the wireless medium using packet acknowledgements (ACK) on the receiving end. This means that in order to confirm a successful data communications, the receiving station transmits an ACK packet to the sending station after each packet is received.

CSMA/CA functions as follows. Before transmitting, the sending station "listens" to the frequency of its assigned channel by way of the Clear Channel Assessment (CCA) procedure integrated within the CSMA/CA protocol. If there is activity detected that frequency, then the sender waits a randomly selected amount of time and attempts to send again. If the frequency is vacant on the next try, the data is transmitted to the receiver, and if the reception is successful, the receiver sends an ACK packet back to the sender for confirmation. If the ACK frame is not detected after the sender transmits, then a collision is assumed to have occurred and the data is retransmitted again after waiting another randomly selected time period (See Figure 1). This will be the very heart of our exploit. By exploiting the CCA procedure, we can generate interference that will case the CCA algorithm to determine that all frequencies for the current channel are busy, and all communications will be halted.

If there is a constant wide-band transmitting source within the reception range of any transmitting or receiving station, it is possible to trick the sending and receiving units into thinking that the band is constantly busy. Our transmitter will transmit what the sending and receiving units will perceive as noise over most of the bandwidth available to the 802.11 channel, preventing both the transmission of data, and the reception of acknowledgement packets from the sender. The transmitting and receiving units will not be able to communicate because they won't have an open frequency to use. This is proves effective in denial of service to all 802.11 clients, and it is difficult to defend against.

Figure 1. Simplified CSMA/CA method of operation.



In order to completely understand how our exploit functions, and why this vulnerability exists, it is necessary to understand some basic theories and concepts that apply to radio communications. Once these basic concepts are understood, it will be much easier to understand the rest of this paper, and the impact that this exploit has on 802.11 communications.

Basic Radio Theory

A *radio* is a device that transmits information through space using oscillating alternating current (AC) current. The most commonly known example of a radio is the receivers that we use to listen to music and news in our homes and automobiles. These are examples of one-way radios. They have a transmission source, commonly referred to as a radio station, and we use our receivers to listen to the information broadcast from the station. Two-way radios, also known as transceivers, allow the transmission and reception of information from all parties. They can be used for point-to-point applications, where two sites only talk to themselves, for example, walkie-talkies, or point-to-multipoint applications, commonly used for various telecommunications mediums such as cellular phone networks and wireless LANs where multiple sites talk to a single central, or core site. All equipment designed for 802.11 communications, for example, wireless network interface cards (NIC) and wireless access points (WAP) are two-way radios and can be use for point-to-point as well as point-to-multipoint communications.

The single most important aspect of all radio-based communications is power. The output power of a radio that is transmitted to an antenna is measured in watts (W) or milliwatts (mW). Power can also be expressed using a logarithmic

scale to compare the number of watts or milliwatts to decibels (dB). The reasons for this being that decibels are a relative measurement unit, while watts and milliwatts are an absolute measurement. Radio manufacturers provide the transmitting power of a radio in dBm, which is decibels per 1 milliwatt, or dBW, decibels per 1 watt. Table 2 provides conversion information between power in watts and decibels.

The following table and mathematical formulas were taken from 802.11 Wireless LAN Fundamentals written by Pejman Roshan and Jonathan Leary, published by Cisco Press. http://www.ciscopress.com

Table 2. Common power conversions

Milliwatts (mW)	Watts (W)	Decibels per 1 mW (dBm)	Decibels per 1 W (dBW)
1	.001	0	-30
2	.002	3	-27
5	.005	7	-23
10	.01	10	-20
20	.02	13	-17
50	.05	17	-13
100	.1	20	-10
1000	1.0	30	0

The values in Table 2 were obtained using the following conversion formulas:

dBm to mW: $P_{mW} = \log^{-1}\left(\frac{P_{dBm}}{10}\right)$

mW to dBm: $P_{dBm} = 10 \log_{PmW}$

mW to W: $P_W = P_{mW} * .001$

If we use the fact that a 0 dBm signal is equal to –30dBw, we can find the dBm figure, and subtract 30 to get its value in dBW.

dBm to dBW: $P_{dBW} = P_{dBm} - 30$

Basic Antenna Theory

An *antenna* is a device used to transmit or receive radio frequency (RF). The radio produces an RF signal and the antenna is the transport medium used to direct that signal into free space for its eventual reception by another antenna attached to a receiver. Some very important aspects of an antenna are its radiation pattern, directivity, bandwidth, antenna gain, and loss.

The radiation pattern of an antenna is defined as the “angular variation of radiation at a fixed distance from an antenna.” It is often referred to in units of directivity or gain. Directivity and gain are very similar, and are probably the most important part of antenna theory and design. Directivity is simply the ability of an antenna to transmit or receive RF strongly in one direction over another direction. Antenna gain is the measure of strength of the amplification effect of an antennas directed signal with respect to signal loss. An antenna can create an amplification effect depending on its construction. The amplification effect is the result of focusing the transmission signal into a tight beam. A similar effect would be to focus the light beam that is emitted from a flashlight through a paper cone. The light emitted from the small end of the cone will seem brighter and more concentrated. Antenna gain works by the same principle. Signal loss simply describes a decrease in signal strength. Gain and loss are very important to antenna and radio performance because they directly affect signal quality and the signal transmission and reception capabilities. Being able to measure loss and gain are important because all radios have a sensitivity threshold. A sensitivity threshold is the point in which a receiver can clearly distinguish legitimate signal from background noise. Because the sensitivity of a receiver is limited, the transmitting station must send information with enough power to be recognized by the receiver. If losses occur at some point between the transmitting and receiving unit, the problem must be resolved by removing the source of the signal loss, or by increasing the transmitting power, or increasing antenna gain of the transmitter or the receiver or both.

The estimated value of gain and loss can be determined by using the reference commonly known as the 3’s of radio frequency math. This is the way this works.

+3dB = doubles the power in mW
-3dB = halves the power in mW

Example:

100mW + 6dB = 400 mW

*100mW + 3dB = 100mW * 2 = 200mW*
*200mW + 3dB = 200mW * 2 =* ***400mW***

100mW – 3dB = 50 mW

100mW – 3dB = 100mW / 2 = ***50mW***

These values make it quick and easy to estimate the value of gain or loss in an RF system without having to perform long math calculations with a calculator. In the case where a more exact value is necessary, the formulas shown under figure 2 should be used.

The units that describe the measurement of antenna gain are dBi, decibels relative to an isotropic antenna. Antenna gain has a direct effect on the total power radiated from an antenna. The value of the power transmitted into an antenna will not leave the antenna at the same value. It will be increased by the amount of gain of the antenna. This is referred to as the effective radiated power. An isotropic antenna is one that radiates equally well in all directions. Antennas are compared to this ideal radiator. Antenna efficiency expressed in relation to this antenna model and are referred to gain in decibels over an isotropic antenna or effective isotropic radiated power (EIRP). For the purpose of this paper, we will discuss in terms of EIRP.

The formula to calculate EIRP is:
EIRP(dBm)=**TxPower(dBm)+AntennaGain(dBi)-Loss(dB)**

Example:
If we have an 802.11b WAP with a 10dBm TX output power connected to a 13dBi gain antenna via coaxial cable with a loss of 3.0 dB, the EIRP would be:

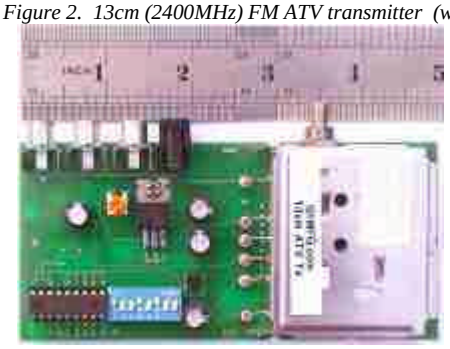
EIRP(dBm)=**10dBm+13dBi-3.0dB=20dbm or 100mW**

For a more in-depth explanation of dB, dBi, and the differences between EIRP and ERP refer to the ARRL Antenna Book, published by the American Radio Relay League.

Equipment
Having covered some of the basic concepts that are essential to understand before performing the exploit, the equipment that is used in this scenario, will now be examined. Note that this is just an example of the type of equipment that can be used to exploit this vulnerability.

2.4 GHz ATV Transmitter
The transmitter used in this writing can be obtained from www.tvham.com for approximately $89.00. (See Figure 2.) It can operate within the same bandwidth that is allocated for 802.11b, and transmits the equivalent of what an access point interprets as noise, or RFI. The legitimate use for this transmitter is for Amateur Radio hobbyists to transmit video and sound via the 13 cm Amateur Radio band. This is referred to as “Amateur Television” or “ATV”, by licensed Amateur Radio Operators. This device works because it transmits an RF signal that has an 18 MHz bandwidth. If we refer to the transmitter specifications listed in Figure 2, it is seen that this particular transmitter is tunable from 2.320 GHz to 2.559 GHz in 1 MHz steps. This covers the entire 2.4 GHz wireless band.

Figure 2. 13cm (2400MHz) FM ATV transmitter (www.tvham.com)

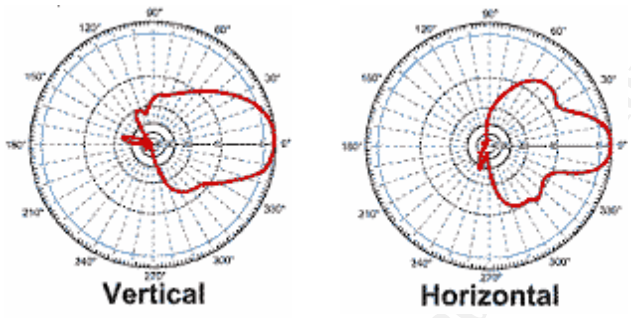


- Tunes 2320 to 2559 MHz in 1 MHz steps
- Sound sub-carriers at 6 MHz & 6.5 MHz
- RCA sockets for video and audio
- SMA RF output socket
- 20mW (typical) 50mW (max) output power
- Runs from 13.8V DC

14 dB gain directional grid array antenna.

This antenna was purchased for approximately $40.00 from www.hdcom.com. It gives us the gain needed to perform this exploit. It also has the directivity needed to focus the signal in a specific direction, while being wide enough to cover a general area. (See Figure 3)

Figure 3. Antenna Radiation Pattern



Referring to the description of the 802.11b wireless standard, it is known that 802.11b uses DSSS. The wireless spectrum is divided up into 11 different channels in 5 MHz steps with a bandwidth of 22 MHz per channel. The frequency of each channel is roughly at the center of its 22 MHz of allocated bandwidth. This means that each channel operates within approximately +- 11 MHz of its center frequency (depending on equipment design). For example, channel 1 has a center frequency of 2.412 GHz but its range of operation varies between 2.401 and 2.423 GHz. Our ATV transmitter, on the other hand has an operating bandwidth of 18 MHz. If the network that is to be exploited is on channel 1, the transmitter is tuned to 2.412 GHz and it will occupy +/- 9 MHz of the channel 1 center frequency. The transmitter will transmit from 2.403 GHz to 2.421 GHz. This leaves only +-2 MHz of open spectrum for channel 1 to operate. In most cases, this is more than enough interference to render this channel useless for reliable communications.

It is important to note that in order to successfully jam an 802.11 network, the jammer must have an EIRP rating of approximately the same value as the targets EIRP rating, or greater. If we refer to Figure 1 we see that our transmitter puts out a minimum of 20 mW. If we use an antenna with a 14 dBi

gain rating, and use a small length of low loss coaxial cable for our connection between the transmitter and the antenna, our EIRP can be calculated using the formula present in section 2.5.

Jammer EIRP:
EIRP (dBm)=13dBm + 14dBi – 1.0dBm (cable loss)=26dBm or approx 400 mW.

We know that our WAP has an EIRP of 17 dBm or 50mW. This was the value provided to us by the manufacturer. If we use the chart provided in Table 2, we know that 17 dBm is the equivalent of 50 mW. The power emitted from our transmitter is 8 times this value, so we should be able to easily obtain our goal of jamming wireless communications. A general rule of thumb to follow when attempting to jam 802.11 communications is to always attempt to achieve an EIRP rating of 4 Watts or more for the jamming device. The reason for this is that according to Part 15 of the FCC Rules and Regulations, the maximum EIRP allowed for 802.11 LAN communications in the United States is 4 Watts. It is a fairly safe assumption that any business or organization that is using wireless heavily will be abiding by these rules. If we come close to or even exceed this power level, it is safe to assume that we will always be able to successfully deny 802.11 services.

Signatures of the attack

This exploit is particularly malicious because of its effectiveness. The only way this attack can be tracked is to track it real time, as the attack is happening. To exploit this vulnerability the attacker doesn't even need to be connected to the network. The only evidence that can be gathered from the attack is a historical log of the throughput, and the Signal-to-Noise ratio (SNR) values as the attack is occurring. SNR is simply the ratio of useful information in a signal as compared to the noise it carries. A high SNR is desirable. There are several tools such as, Netstumbler (www.netstumbler.com) and Airopeek (www.wildpackets.com) that are capable of measuring a particular connections' SNR over time, as well as many other statistics pertaining to a wireless network. Although these tools can be very effective in identifying the cause of the problem, **if this attack is carried out properly and efficiently, these tools are rendered useless.** The reason for this is that these tools are dependent upon a wireless LAN adapter to function. If the attacker successfully jams most of the bandwidth for the operating channel, the access points will not be able to send beacon information over the air and the wireless LAN adapter that is being used to determine the SNR level will not be able to receive any data. Thus, an SNR rating that allows legitimate traffic transmission will not be obtained using 802.11 network equipment. All sending and receiving traffic will be blocked, and all connections will be broken. Typically, this DoS attack will cause an extreme spike in the amount of noise present in the signal. This will cause a major slowdown in the transmission and reception of all wireless traffic. If the signal strength of the noise is high enough, it will cause all clients to lose their connection to the access point, as there is not enough legitimate traffic getting through to maintain a reliable wireless session.

Figure 4. Representation of a healthy SNR

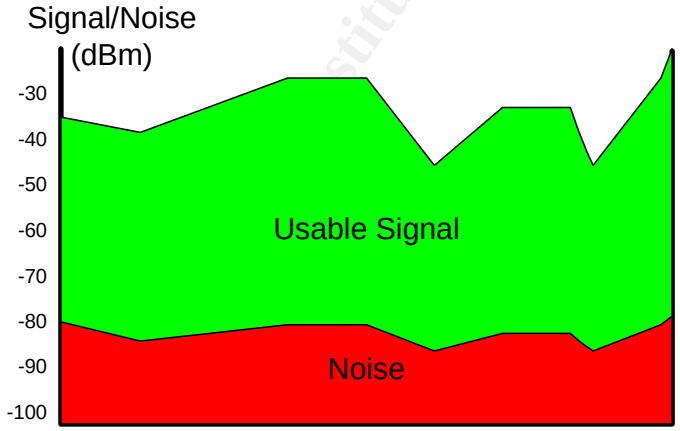


Figure 4 represents a healthy SNR ratio. As you can see, there is a small amount of noise present in our connection. This will apply for most 802.11 connections. The noise is inherently present due to electromagnetic radiation from the atmosphere, outer space, and household devices sharing the same frequency spectrum.

Figure 5. Representation of an unhealthy SNR

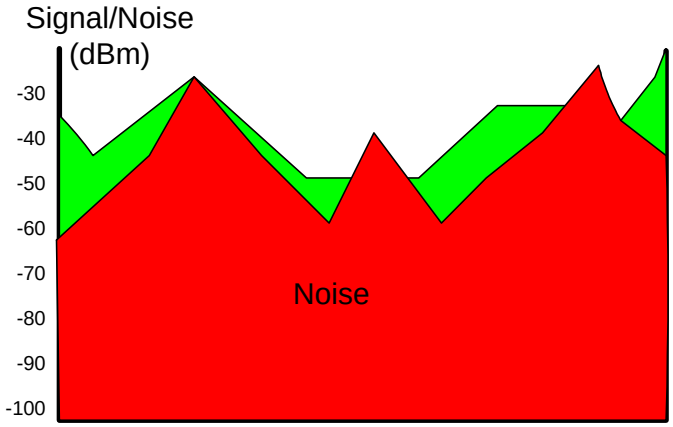


Figure 5 represents an unhealthy SNR. If the history of the SNR has always been different or more similar to the SNR depicted in Figure 4, and is now more represented by the SNR as depicted above, this is a fairly reasonable indicator that jamming of some sort is taking place. You'll also notice that there does seem to be a small amount of legitimate signal getting through. This is most-likely not enough to maintain any session information for any pre-existing connections. As a result of lab testing, it was determined that if the jammer can produce a constant signal that comes within 4-8 dB of, or is greater than the EIRP of the target, then all connections will be broken and Denial of Service can be achieved. A noise value as high as what is depicted in Figure 5 would be more than enough to successfully implement this attack.

Active monitoring of the attack in progress is the only way to track this exploit. If there is a small amount of usable signal able to pass through, the types of tools mentioned above can be used to find the root of the problem**. If the noise level is so high as to over power the legitimate signal, then obtaining an SNR measurement with 802.11 equipment may prove to be impossible.** Also, if the administrator manages to identify the root of the problem as interference, the fact that this is purposeful and malicious interference may not be evident.

Tracking down the source of the interference may prove even more difficult without some very specialized equipment and training, as the jamming device and other devices of its kind require a very small footprint, and do not necessarily need to be in the immediate vicinity to be effective.

Victim's Platform

There is no particular platform in this scenario, although there could be multiple victims. The primary victim would be the users in this scenario. Since this scenario takes place in an environment intended to mimic a public hotspot, there could be multiple operating systems affected, the most probable being a Microsoft Windows version or some form of Linux or Mac variant.

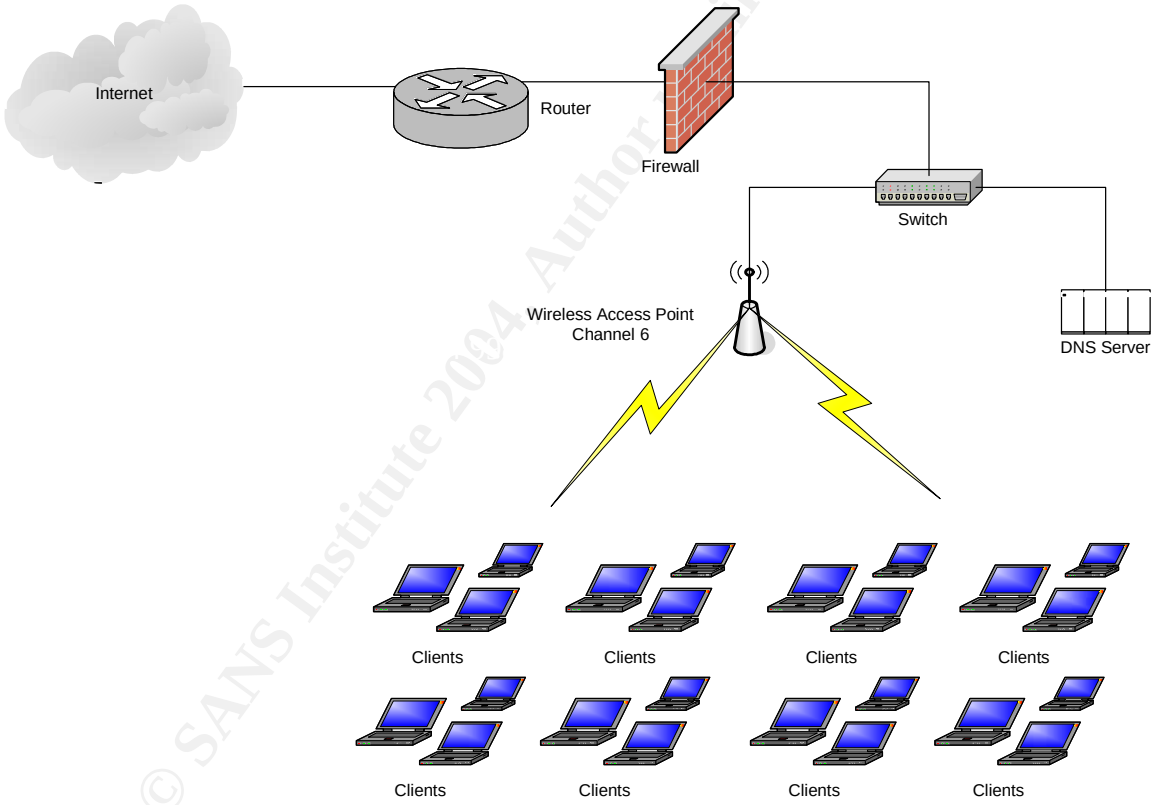
Source Network

The attacker is not connected to a network, as it is not necessary for this exploit. The attacker is located in the immediate vicinity with a laptop running Windows XP Service Pack 1. The attacker is using this machine to monitor the SNR ratio between the clients and the access points.

Target Network

The target network in this scenario has been implemented in a lab environment. The configuration of this network is designed to represent a typical wireless hotspot implementation, or a small business.

Network Diagram



Network Components

Wireless Access Point (WAP): The WAP used in this scenario was a Linksys BEFW11S4. This device was chosen for its ability to attach different antennas and for its relatively low cost. The WAP is using the latest Firmware version 1.50.10 dated 1/16/04.

DNS Server: The DNS server in this scenario provides local DNS resolution and is configured to forward all outside queries to the public DNS server provided by the ISP for the hotspot facility. It is running Microsoft DNS services with Windows 2000 SP4 and all of the latest hotfixes and critical updates.

Firewall: The firewall is a Nokia IP 350 network appliance running IPSO 3.71, and Checkpoint NG FP3 HFA-325

Router: The router is a Cisco 2600 and is managed by the Internet Service Provider of the facility.

Table 3. Firewall Rule Set.

Firewall Rule Set			
Source	**Service**	**Destination**	**Action**
Internal	FTP (TCP21)	ANY	Accept
Internal	Telnet (TCP23)	ANY	Accept
Internal	HTTP (TCP80)	ANY	Accept
Internal	HTTPS (TCP443)	ANY	Accept
Internal	SSH (TCP22)	ANY	Accept
ANY	ANY	ANY	Drop

Stages of the attack

Reconnaissance

Traditional methods of network-based reconnaissance would for the most part, not apply for this type of attack. However, these methods of reconnaissance will be covered in this section in order to fully understand how to use them.

Since the target network in our scenario does not operate any servers that are accessible from outside it's internal network, we will use GIAC.org as an example.

There are many different tools that can be used to perform network reconnaissance on a target host. The object of reconnaissance is to gain as much information on the target while leaving as little evidence behind as possible. This is a trivial task with the correct tools. For this stage of the attack, a web based service, or other third party service is best used to avoid leaving any evidence on the target host that could be linked back to you.

In this example we will use the services that www.kloth.net has made available to us.

The following utilities were used to gather information about our target:

- Whois
- Traceroute
- NSlookup

WHOIS

A WHOIS lookup can yield valuable information that can be put to excellent use for social engineering purposes. Typically, the results consist of information for administrative, technical, and business contacts from within the domain, or from within the entity responsible for the domain, as well as facility postal addresses as seen below

Input Parameters: giac.org

Results:

```
NOTICE: Access to .ORG WHOIS information is provided to assist persons in determining the
contents of a domain name registration record in the PIR registry database. The data in
this record is provided by Public Interest Registry for informational purposes only, and
PIR does not guarantee its accuracy.  This service is intended only for query-based
access.  You agree that you will use this data only for lawful purposes and that, under
no circumstances will you use this data to: (a) allow, enable, or otherwise support the
transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial
advertising or solicitations to entities other than the data recipient's own existing
customers; or (b) enable high volume, automated, electronic processes that send queries
or data to the systems of Registry Operator or any ICANN-Accredited Registrar, except as
reasonably necessary to register domain names or modify existing registrations.  All
rights reserved. PIR reserves the right to modify these terms at anytime. By submitting
this query, you agree to abide by this policy.

Domain ID:D16237909-LROR
Domain Name:GIAC.ORG
Created On:29-Dec-1999 18:55:24 UTC
Last Updated On:18-Oct-2003 23:06:57 UTC
Expiration Date:29-Dec-2011 18:55:24 UTC
Sponsoring Registrar:R71-LROR
Status:OK
Registrant ID:C35725469-RCOM
Registrant Name:SANS SANS
Registrant Organization:SANS
Registrant Street1:4610 Tournay Road
Registrant City:Bethesda
Registrant State/Province:MD
Registrant Postal Code:20816
Registrant Country:US
Registrant Phone:+1.3019510102
Registrant FAX:+1.3019510104
Registrant Email:hostmaster at sans.org
Admin ID:C35725520-RCOM
Admin Name:SANS SANS
Admin Organization:SANS
Admin Street1:4610 Tournay Road
Admin City:Bethesda
Admin State/Province:MD
Admin Postal Code:20816
Admin Country:US
Admin Phone:+1.3019510102
Admin Email:hostmaster at sans.org
Tech ID:C35725521-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575 8th Avenue
Tech City:New York
Tech State/Province:NY
Tech Postal Code:10018
Tech Country:US
Tech Phone:+1.9027492701
Tech Email:domain-registrar at register.com
Name Server:NS1.HOMEPC.ORG
```

```
Name Server:NS2.HOMEPC.ORG
Name Server:NS1.GIAC.NET
Name Server:NS2.GIAC.NET
```

Traceroute

Traceroute is a tool used to trace the path that packets take to a network host. The tool is uses ICMP to track the number of routers that data travels through before arriving it's final destination. In this example giac.org is blocking ICMP at their routers. Nevertheless, the information retrieved here is still useful in determining the last route before arriving at the destination network.

Input Parameters:

Domain: giac.org

Results:

```
traceroute to giac.org (65.173.218.144), 30 hops max, 40 byte packets
 1  213.133.98.129  0.253 ms   0.344 ms   0.432 ms
 2  et-2-2.RS86001.RZ3.hetzner.de (213.133.96.193)  1.534 ms   2.772 ms   3.844 ms
 3  gi-2-2.RS8K1.RZ2.hetzner.de (213.133.96.57)  3.871 ms   3.960 ms   4.030 ms
 4  nbg.de.lambdanet.net (213.133.96.234)  4.421 ms   4.511 ms   4.581 ms
 5  F-4-eth220-0.de.lambdanet.net (217.71.105.149)  6.228 ms   6.179 ms   6.452 ms
 6  F-8-eth200.de.lambdanet.net (217.71.105.54)  7.237 ms   7.343 ms   7.377 ms
 7  pos6-1.pr1.fra1.de.mfnx.net (216.200.116.65)  7.964 ms   8.526 ms   8.589 ms
 8  so-3-1-0.cr1.fra1.de.above.net (216.200.116.130)  5.137 ms   5.224 ms   5.043 ms
 9  216.200.115.254.reverse.not.updated.above.net (216.200.115.254) 5.668 ms 5.583 ms
10  so-4-2-0.cr1.lhr3.uk.above.net (64.125.29.77)  22.818 ms   23.050 ms   23.123 ms
11  so-7-0-0.cr1.dca2.us.above.net (64.125.31.186)  93.477 ms   93.381 ms   93.559 ms
12  sl-gw19-rly-3-0.sprintlink.net (144.232.247.85)  95.788 ms   95.761 ms   95.871 ms
13  sl-escal-1-0-0.sprintlink.net (160.81.98.26)  98.356 ms   98.448 ms   98.561 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

DNSLookups

There are two main utilities that can be used to resolve information about a domain's DNS records: NSlookup and Dig. These utilities are used to enumerate the IP addresses and names of the authoritative DNS servers for a particular domain. They both enumerate the same information, and have the same input parameters on kloth.net. Using the tools that kloth.net makes available to us we are able to perform an Nslookup on giac.org:

Input Parameters:

Domain: Giac.org
Nameserver: ns1.kloth.net

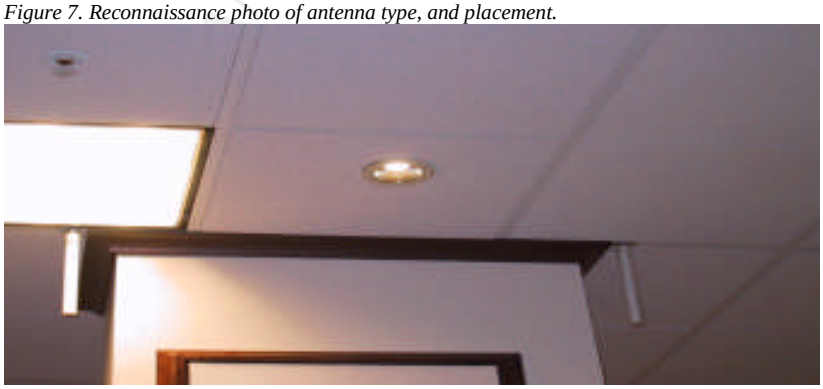
Results:

```
Server:         ns1.kloth.net
Address:        213.133.98.149#53

Non-authoritative answer:
Name:   giac.org
Address: 65.173.218.144
giac.org        nameserver = ns2.giac.net.
giac.org        nameserver = ns2.homepc.org.
giac.org        nameserver = ns1.giac.net.
giac.org        nameserver = ns1.homepc.org.

Authoritative answers can be found from:
giac.org        nameserver = ns1.giac.net.
giac.org        nameserver = ns1.homepc.org.
giac.org        nameserver = ns2.giac.net.
giac.org        nameserver = ns2.homepc.org.
```

Physical Reconnaissance

For this scenario, physical reconnaissance could also be performed. Because this is a public network, the environment can be evaluated beforehand in order to determine what kind of equipment is in use by the facility, but more importantly, the number of access points and the types of antennas being used. In this scenario, we were only able to determine they types of antennas being used by the access points. A snapshot was discreetly taken for future reference.

Figure 7. Reconnaissance photo of antenna type, and placement.

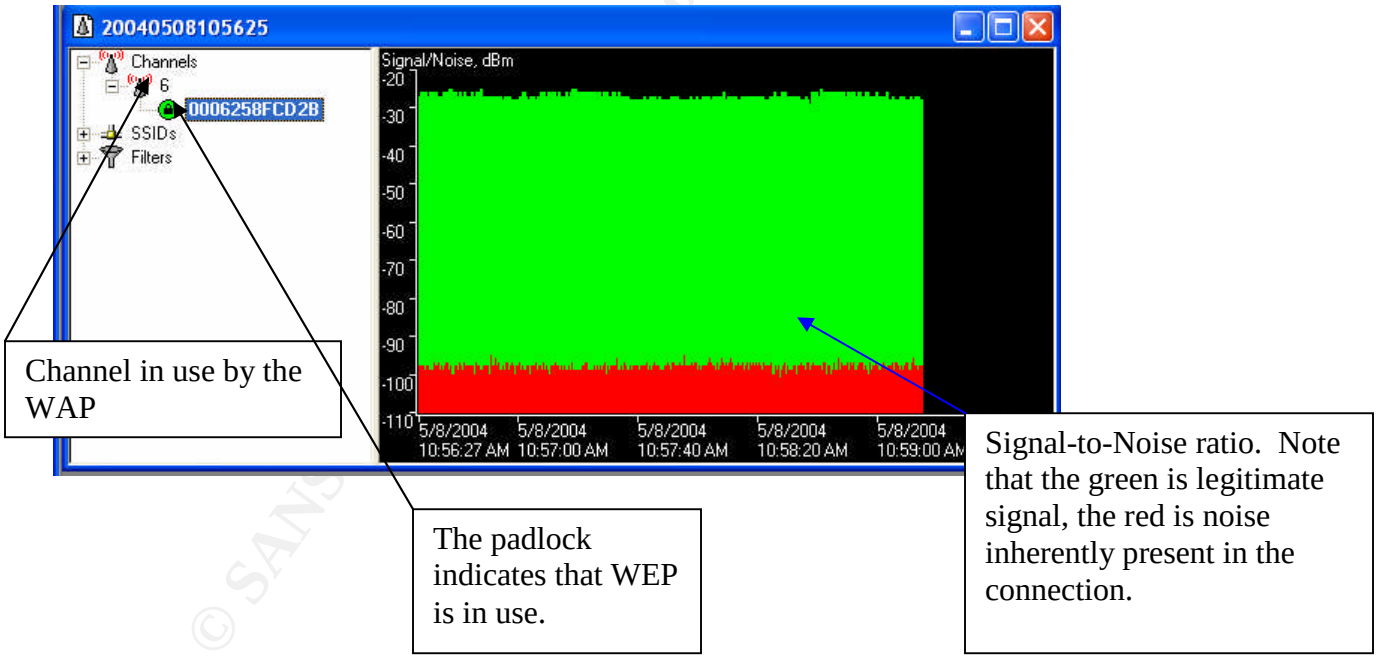


We can see from Figure 7 that from the looks of the antennas in use and the way they have been mounted, they are most likely omni-directional, and from their size and length, they probably have around a 5-8 dBi gain to them. This information is important to our attack in estimating what kind of output power we will need to overpower or mask the legitimate signal (Refer to the figures on page 12).

Scanning

Netstumbler (www.netstumbler.com) written by Marius Milner was used to determine the channel frequency in use by the WLAN. Netstumbler is a free piece of software, but the source code has not been released to the public. It is a tool used primarily to detect 802.11 wireless networks in the local vicinity. Using Netstumbler it is possible to detect the operating channel of a wireless network, whether Wired Equivalent Privacy (WEP) is in use, the Service Set Identifier (SSID), signal strength data, and much more. It was primarily written as troubleshooting utility for WLAN administrators, but like many other utilities used for this purpose, it can also prove to be useful by attackers as well. According to Netstumbler, our LAN is using WEP and is operating on channel 6 of the wireless spectrum (Figure 8).

Figure 8. Netstumbler results from scanning.



Exploiting the System

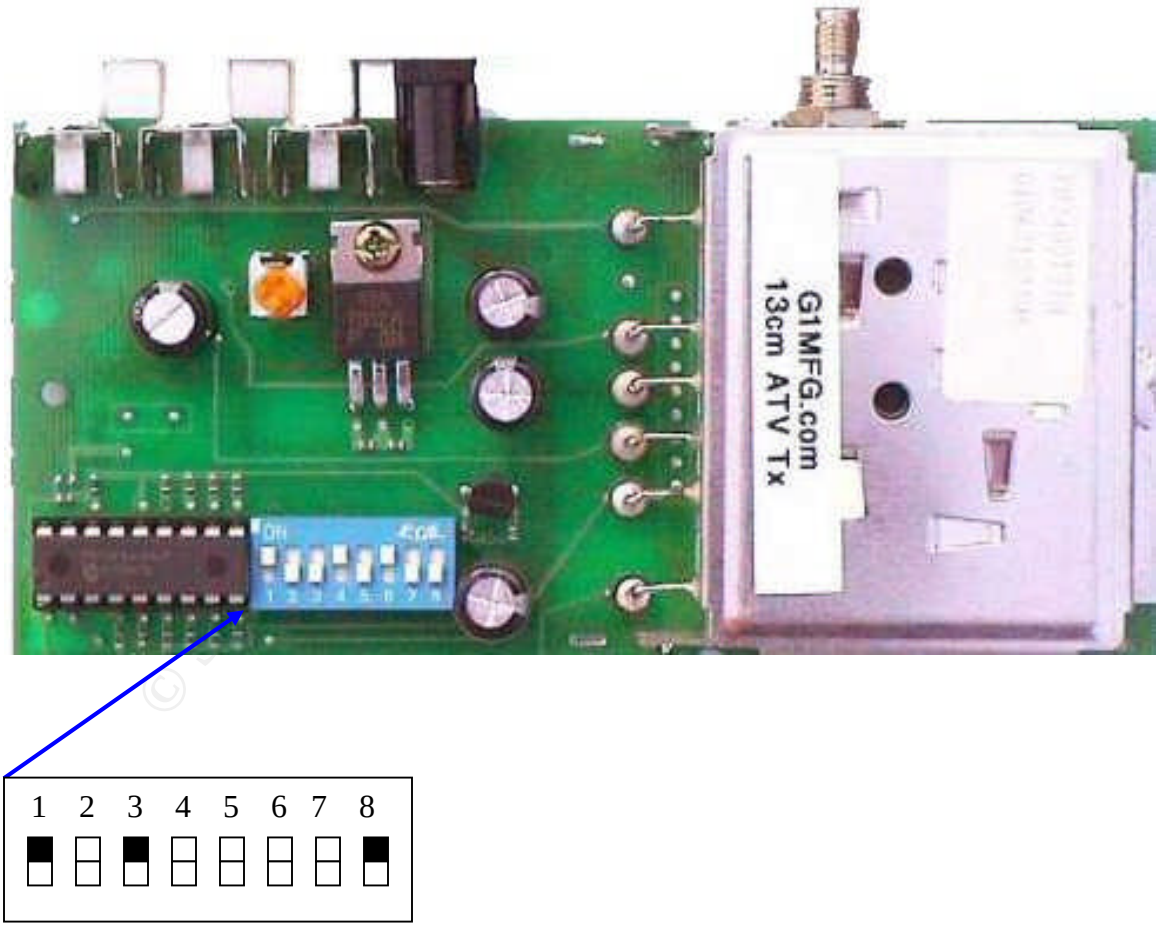
In order to execute the DoS attack, the following steps will need to be followed:

1. Determine the operating channel of the WLAN.
    a. This can be done using a wireless discovery utility. Netstumbler was used in this scenario.

2. Set the transmitter to operate at the same frequency of the WLAN channel.
    a. This is done by setting the DIP switches on the transmitter in the correct on/off sequence. Please refer to the chart in the appendix to determine the correct sequence.
3. Connect the transmitter to the antenna and direct the antenna towards the target network.
4. Apply power to the jamming transmitter.
5. Monitor the signal strength and the SNR using Netstumbler to determine whether the attack is successful.

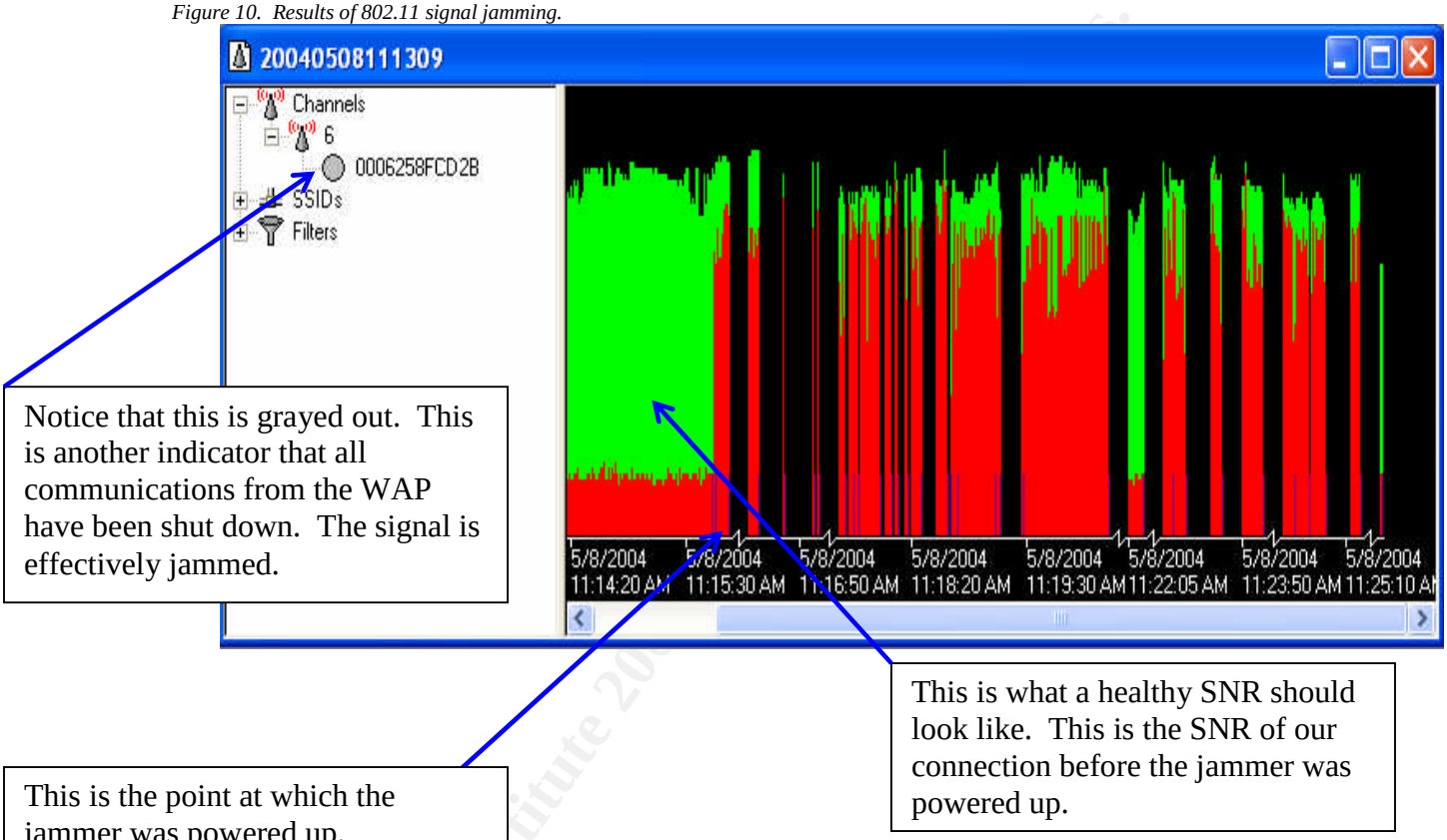
Using Netstumbler to determine what channel our target is using, and referring to the information presented in Table 1 and noting that the center frequency for channel 6 is 2.437 GHz, the jamming transmitter is set to the same frequency as the channel in use for the WLAN. This is accomplished by referring to the frequency settings that accompany our particular transmitter (Appendix), and changing the DIP-switch settings to match the appropriate configuration.

Figure 9. Transmitter frequency settings.



The transmitter has an 18 MHz bandwidth and its center frequency is set at channel 6. The next step is to attach an antenna to the device, and power it on using a 12-volt AC adapter. Before this is done, Netstumbler is running to monitor the SNR to determine the effectiveness of the jamming. Continued monitoring of the WLAN under attack for changes in channel frequency allows the ability to act accordingly and change the operating frequency of the jammer to match the WLAN channel changes.

Figure 10. Results of 802.11 signal jamming.



Once power is applied to the transmitter, the effects are on the WLAN are obvious. It is seen that the noise level spikes severely and the connection is severed as the noise overpowers the signal. You'll notice that occasionally some signal gets through, but it does not carry enough useable information to re-establish the session. This can go on all indefinitely, and the network is at the whim of the attacker.

Detecting the jamming can be quite difficult if not impossible. An experienced administrator may immediately notice the characteristics of jamming and use an application like Netstumbler to monitor the SNR levels. As seen above in Figure 10, it is obvious that there is some major interference to the signal. The problem is that it might not be apparent to the administrator that this is a malicious act. This problem is compounded by the fact that depending on the transmitting power output of the jammer, the attacker could be literally anywhere within an 800-1000 foot radius of the target. Or, the attacker wouldn't have to be present at all. The transmitter could simply be hidden in a tree or on the top of a building attached to a high gain directional antenna pointed towards the target, or I could be hidden in a car in the parking lot. The possibilities are numerous.

Keeping Access

In this scenario, keeping access to the target network is not a problem. As long as the target network can be detected with Netstumbler or another similar application, jamming is possible. In this scenario we only have one jamming device to work with. In order to ensure that our attack is always effective, we must monitor the network with Netstumbler as the attack is occurring. By doing this, we can ensure that we know if the administrator has changed channels on the LAN in attempt to defeat our attack, and adapt as necessary by changing the transmitter to match the corresponding channel of the WLAN. Or, if possible we could use three different jamming devices operating on channels 1, 6, and 11 to jam the entire available spectrum at once.

Covering Tracks

Covering your tracks while exploiting this vulnerability is very simple because it is a relatively anonymous exploit by nature. It is not necessary for the attacker to be located at the target site, and the attack does not leave any evidence that could be traced to the attacker.

The Incident Handling Process

This section will cover the 6 Incident Handling steps developed by the SANS Institute. Throughout this section we will walk through the necessary steps to effectively handle this incident. In some cases, a few of these steps will not apply to our attack scenario. In these situations we will speak of the step theoretically for informational purposes.

Preparation

Countermeasures

The target network in this scenario consists of a router, firewall, DNS server and a wireless access point. All of these devices are running with the latest firmware, service packs, and security patches. The DNS server is backed up incrementally from Saturday to Thursday, and a full backup is performed on Friday.

Incident Handling Team

The following excerpt was taken directly from the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide. It describes what the components of an ideal Incident Handling team should consist of. It has been modified slightly to better adapt to the context of this paper.

- **Management.** Management invariably plays a pivotal role in incident response. In the most fundamental sense, management establishes incident response policy, budget, and staffing. Without management support, an incident response team is unlikely to be successful.

- **Information Security.** Members of the information security team are often the first to recognize that an incident has occurred or is occurring and may perform the initial analysis of incidents. In addition, information security staff members may be needed during other stages of incident handling—for example, altering network security controls (e.g., firewall rule sets) to contain an incident.

- **Telecommunications.** Some incidents involve unauthorized access to telephone lines, such as dialing into unsecured modems. Private Branch Exchange (PBX) compromises often are intertwined with break-ins into other systems. The telecommunications staff is aware of the current capabilities and the policies and procedures for working with telecommunications carriers.

- **IT Support.** IT technical experts (e.g., system administrators, network administrators, and software developers) not only have the needed technical skills to assist during an incident but also usually have the best understanding of the technology with which they deal on a daily basis. This understanding can facilitate decisions such as whether to disconnect an attacked system from the network.

- **Legal Department.** Legal experts should review incident response policies and procedures to ensure their compliance with local and federal law, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit.

- **Public Affairs and Media Relations.** Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public (within the constraints imposed by security and law enforcement interests).

- **Human Resources.** When an employee is the apparent target of an incident or is suspected of causing an incident, the human resources department often becomes involved—for example, in assisting with disciplinary proceedings or employee counseling.

- **Business Continuity Planning.** Computer security incidents undermine the business resilience of an organization and act as a barometer of its level of vulnerabilities and the inherent risks. Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to certain types of incidents, such as a denial of service (DoS). Organizations should also ensure that incident response policies and procedures and business continuity processes are in sync.

- **Physical Security and Facilities Management.** Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. Threats made against the organization may not indicate whether logical or physical resources are being targeted. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office. Thus, close coordination between physical security and facilities management and the incident response team is important.

There was no Incident Handling process, or support staff in place for the target network in this scenario. The SANS Incident Handling procedure was used to handle the incident as if this was an actual production environment.

Because our target is small and has no dedicated support staff, an Incident Handling process, as well as an Incident Handling team, does not exist. It is ideal to have an Incident Handling process in place to avoid having to make split second decisions that may, or may not be the best for the situation. Having a preconceived plan established is a great asset to the Incident Handler(s) when an incident occurs.

Identification

Timeline

May 8th 2004 11:15am: Attack begins, wireless connectivity is severed.
Within 2 seconds of the attack being executed, the results were apparent. All wireless communications were severed as demonstrated in Figure 10.

May 8th 2004 11:22am: User notifies the network administrator of connection problems.
The event proceeded with the administrator receiving an angry phone call from an end user alerting him of the network conditions.

May 8th 2004 11:29am: Administrator begins troubleshooting process.
The administrator immediately fired up Netstumbler, and was unable to detect any access points in the area.

The particular access point used in this scenario also has an integrated 4-port switch. A laptop was connected to an empty port on the switch, and it was discovered that the wired portion of the network was still functioning normally.

After this test, the administrator replaced the access point with a unit configured identical to the first and the same results were recorded.

By following the normal troubleshooting process that one familiar with wireless networks would follow, the administrator changed the operating channel of the access point from channel 6 to channel 11. The network was restored. Ten minutes later the network went down again with the same characteristics as the first attack.

Just to be absolutely sure that the equipment he had was functioning properly, the administrator took the access point off site and was successfully able to setup up a quick and dirty connection between it, and his laptop. Upon returning to the site, he changed the channel on the access point to channel 1, and connectivity was restored. After waiting a few minutes, channel 1 went down. He then repeated these steps using channels 2 through 5 and 7 through 10 and received the same results.

May 8th 2004 11:52am: Administrator determines that the interference is malicious.
Now our administrator knew that something was up. What he had just seen gave him some major insight into what could be going on here. He had never seen interference adapt like this before, and he was now thinking that this was a malicious attack.

Containment and Eradication

May 8th 2004 11:57am: Administrator continues with the Incident Handling Process.

Instead of panicking, our administrator remained calm and examined the two most important facts that he had so far:

- The attacker seemed to be able to cover the entire 2.4 GHz spectrum, but not multiple channels at the same time.
- After inspecting the relatively small area of the target network and finding nothing out of the ordinary as well as no strange looking devices, he reasoned that the attack was originating from outside the office perimeter.
- Our administrator new that the attacker had to have some way of monitoring the access point channel settings to determine how to adapt to the tests he had performed.

Acting on gut instinct, the administrator went to a local electronics store in the area, and purchased an 802.11a access point and WLAN adapter. He knew that that 802.11a operates in the 5 GHz band. He had a hunch that the attacker did not have the capability to cover 5 GHz as well as 2.4 GHz. After reading through the instruction manual, he powered up the access point, installed the drivers for

the 802.11a network adapter, and successfully established a connection with the access point. Thirty minutes passed, and he still had connectivity. He fired up Netstumbler, and all of his SNR levels were normal. He had the solution! He was correct in assuming that the malicious interference was directed towards the 2.4 GHz spectrum alone.

Because all of the other client adapters were conveniently multimode 802.11a and 802.11b compatible, the client cards being auto-sensing, were able to reestablish their network connectivity and resume business as usual.

After further consideration, he decided not to take down the old access point just yet. He reasoned that if the attacker weren't able to detect the access point for a long period of time, he would get suspicious and investigate.

Containment of this attack is very difficult if not impossible. If the source of the attack is determined to be outside the physical location of the target network, there are a few things one can do to avoid this attack, but most likely not totally prevent it.

First things first, it is necessary to take a look at the physical structure of the building. Take note of the type of building and its construction material. For example, is the building a multilevel commercial building constructed of concrete? If so, there is very likely to be steel reinforcements, and metal conduit within the building walls and ceilings, and may already be somewhat resistant to interference. Also, take note of the number and size of windows on the building. Most of the time, glass will pass radio frequency with no problems.

The fact is that there is not much that the victim can do to totally block directed and malicious interference to their wireless LANs. However, there are a few precautions one can take to avoid these situations:

- Use a metallic based paint on all walls inside and out.
- Line the insides of the building with commonly available copper mesh.
- Use an RF resistant tint on the building windows.
- Use a metallic based insulation within the building walls and ceilings.
- Take the appropriate steps to minimize RF escaping the building. This will reduce the possibility of the network being detected from outside the building and making it a target to all sorts of attacks. This can be most easily done by:

    a. Adjusting the RF output power of the on the access point(s) to the minimum required amount for adequate coverage and throughput.

b. Using directional antennas with the lowest gain and the most narrow radiation pattern possible for adequate coverage and client throughput.

The steps outlined above can help avoid interference originating from outside of the physical location, but will do nothing to avoid interference originating from the inside. Unfortunately there are even fewer options available to Incident Handlers combating this type of attack originating from the inside. The only ultimate solution to stopping an attack of this nature from the inside is to locate the source of the malicious interference. This has proved to be a very difficult task, but it is possible. What is needed is costly spectrum analysis and direction finding equipment, the ability to troubleshoot using trial and error, and luck.

Recovery

The recovery stage in this scenario was partly explained in the Containment/Eradication section. Several changes were made to the network and the physical environment. These are outlined below.

Recovery Steps:

1. The access point was removed and replaced with Nortel 802.11a solution operating at 5 GHz.

2. The access points transmitting power was reduced to lower the potential of RF escaping the building, to avoid detection from the outside the building and thus being targeted for future attacks.

3. All of the outside windows were treated with an RF resistant covering, and the copper mesh was inserted behind the wallboard, and up in the ceiling in the area that wireless was used.

May 11th 2004 9:30am: Administrator closes the incident.

After three days of continuous monitoring and no sign of any further interference, the administrator considered the incident to be successfully mitigated. He recorded his results in the handwritten logbook that he had kept throughout the Incident Handling process, and wrote up the necessary briefings to report to management.

Lessons Learned

Incident Analysis and Recap

In this scenario a DoS attack was performed on the target network by introducing wide band interference into the frequency spectrum of the operating channel of the WLAN. The administrator in this scenario was successfully able to eliminate

the effects of this attack on his network by implementing equipment that uses a different wireless band all together. As you know, this is not a solution or a patch to the existing vulnerability. This is simply a work around. The same results would have occurred had the attacker used a transmitter that was designed for the 5 GHz band as well. The fact is, and will remain, that all wireless and radio communications are vulnerable to RF interference in some form. Because of the cost involved to make a physical structure immune to wireless attack, it may be cheaper to pull wire and abandon the use of a wireless network in this facility.

In conclusion, the lessons learned in this scenario are very simple. **Wireless communications should not be deployed in any situation where maximum uptime, and high availability are required.** It is very important for administrators to take ample time to evaluate the risks and benefits of deploying 802.11 technologies into their environment. 802.11 technologies can be beneficial to an organization if they are deployed in a secure and intelligent manner.

Additional Notes

There is a common theory that 802.11 technologies that operate using Orthogonal Frequency Division Multiplexing (OFDM) techniques instead of DSSS or FHSS are not vulnerable to this attack. I do not believe this to be true. It should be noted that while their spectrum encoding solutions differ, they still share the same physical layer (PHY), and thus they both use CSMA/CA and the CCA procedure to "listen" before transmitting on a given channel. Others may argue that while they share the same PHY, 802.11a/g has much more bandwidth available for operation, and with the multi-carrier nature of OFDM, they may not be **as** vulnerable to this attack. This is true…somewhat… The available bandwidth is greater; therefore there is more frequency available for the CSMA/CA protocol to work with, therefore increasing the probability of finding a clear channel. However, all this means for the attackers is that they must either use more transmitters operating in series and set to different channels spread throughout the band, or one could use a single transmitter that occupies a wider bandwidth. For example, if we were attacking an 802.11a network and we wanted to be absolutely sure our attack was effective, we could use a transmitter much the same as we did in this scenario, with coverage from 5.1-5.9 GHz.

Furthermore, because of the brute force nature of this attack, all 802.11 receivers are subject to a condition known as *near field interference.* This condition occurs in an 802.11 network when there are multiple clients that are operating very close to the access points and have higher power settings, while there other client nodes located farther away and therefore have a much weaker signal getting to the access point. The result of this situation is that the clients that are located near the access point drown out the signal of the clients further away, and the access point does not "hear" them. The concept is similar to a speaker standing in front of a noisy conference room. If there are 20 people yelling at him standing five feet away, and there are a few other people standing 30 feet away and speaking at a normal volume, the speaker will not hear the people in the back because the people in front are too loud.

It is possible to create this condition using a high power transmitter. If the malicious signal directed at the access point is so strong as to drown out the client communications, a DoS condition occurs. By barraging the access point with high power interference, it doesn't matter how much bandwidth is available, the access point won't be able to hear enough clear signal to process anything legitimate. A very common transmitter of this nature is the common household microwave oven. These devices can be modified using a popsicle stick and some electrical tape to defeat the safety switch that prevents the appliance from operating with the door open. If this is accomplished, all one would need to do is direct the opening in the general direction and set the timer to the maximum possible cook time. This would effectively eliminate communications for all wireless devices in the general area. This could also possibly affect, or even damage other electronic equipment in the area including switches, hubs, routers,

etc. **A microwave oven has a transmitting power of anywhere from 400 to 1200 Watts, approximately 20,000 to 60,000 times more power than the jamming device used in the paper.** This practice is not safe, and has some serious health related dangers, but if one wanted to be particularly malicious and thorough in their attack, this would be of no real concern.

Works Cited

Stahlberg, Mika. "Radio Jamming Attacks Against Two Popular Mobile Networks." 11 Nov 2000.
http://www.hut.fi/~mstahlbe/papers/jamming_paper.html

Sutherland, Ed. "Is Wi-Fi Heading Down the Wrong Track?" 9 May 2002.
http://www.internetnews.com/wireless/article.php/1107451

Pozar, Tim. "Regulations Affecting 802.11 Deployment." 10 Feb 2004.
http://www.lns.com/papers/part15/Regulations_Affecting_802_11.pdf

Moran, Joseph. "Wireless Home Networking, Part V – Interference and Range Extension." 8 Nov 2002.
http://www.wi-fiplanet.com/tutorials/article.php/1497111

Intersil Corporation. "Effects of Microwave Interference on IEEE 802.11 WLAN Reliability." May 1998.
http://www.wlana.org/learn/microreliab.pdf

Geier, Jim. "Minimizing 802.11 Interference Issues." 11 Jan 2002.
http://www.wi-fiplanet.com/tutorials/article.php/953511

Bardwell, Joe. "Converting Signal Strength Percentage to dBm Values." Nov 2002.
http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf

Ratzel, Greg. "Broadband FH Wireless Radios Solve Last-Mile Gap. " 24 Oct 2002.
http://www.commsdesign.com/showArticle.jhtml?articleID=16505876

Huotari, Allen. "A Comparison of 802.11a and 802.11b WIRELESS LAN STANDARDS." 1 May 2002.
http://www.linksys.com/products/images/wp_802.asp

Grance, Tim, Karen Kent, Brian Kim. Computer Security Incident Handling Guide. Maryland: National Institute of Standards and Technology. Jan. 2004 http:// http://csrc.nist.gov

Roshan, Pejman, Jonathan Leary. 802.11 Wireless LAN Fundamentals. Indiana: Cisco Press. Dec 2003

References

IEEE-SA Standards Board, "IEEE Std IEEE 802.11-1999 Information Technology – Telecommunications and Information Exchange Between Systems-local and metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, " IEEE 1999.
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

Flickenger, Rob. Building Wireless Community Networks. California: O'Reilly and Associates, 2002

Gast, Matthew, S. 802.11 Wireless Networks: The Definitive Guide. California: O'Reilly and Associates, 2002.

Hare, Ed. The ARRL RFI Book: Practical Cures for Radio Frequency Interference. American Radio Relay League, 1999.

Straw, Dean R. The ARRL Antenna Book: The Ultimate Reference for Amateur Radio Antennas, Transmission Lines, and Propagation. (ARRL Antenna Book 20th Edition.) American Radio Relay League, 2003.

AusCert Advisories:

AusCERT: AA-2004.02 – Denial of Service Vulnerability in IEEE 802.11 Wireless Devices.
http://www.auscert.org.au/render.html?it=4091

CERT Vulnerability Notes:

VU#106678: IEEE 802.11 wireless network protocol DSSS CCA algorithm vulnerable to denial of Service.
http://kb.cert.org/vuls/id/106678

Applications:

NetSumbler: http://www.netstumbler.com

Equipment:

Transmitter (Jammer): http://www.tvham.com
Antenna: http://www.hyperlinktech.com

Appendix

Transmitter settings for frequency calibration.

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2304	0	0	0	0	0	0	0	0
2305	1	0	0	0	0	0	0	0
2306	0	1	0	0	0	0	0	0
2307	1	1	0	0	0	0	0	0
2308	0	0	1	0	0	0	0	0
2309	1	0	1	0	0	0	0	0
2310	0	1	1	0	0	0	0	0
2311	1	1	1	0	0	0	0	0
2312	0	0	0	1	0	0	0	0
2313	1	0	0	1	0	0	0	0
2314	0	1	0	1	0	0	0	0
2315	1	1	0	1	0	0	0	0
2316	0	0	1	1	0	0	0	0
2317	1	0	1	1	0	0	0	0
2318	0	1	1	1	0	0	0	0
2319	1	1	1	1	0	0	0	0
2320	0	0	0	0	1	0	0	0
2321	1	0	0	0	1	0	0	0
2322	0	1	0	0	1	0	0	0
2323	1	1	0	0	1	0	0	0
2324	0	0	1	0	1	0	0	0
2325	1	0	1	0	1	0	0	0
2326	0	1	1	0	1	0	0	0
2327	1	1	1	0	1	0	0	0
2328	0	0	0	1	1	0	0	0
2329	1	0	0	1	1	0	0	0
2330	0	1	0	1	1	0	0	0
2331	1	1	0	1	1	0	0	0
2332	0	0	1	1	1	0	0	0
2333	1	0	1	1	1	0	0	0
2334	0	1	1	1	1	0	0	0
2335	1	1	1	1	1	0	0	0
2336	0	0	0	0	0	1	0	0
2337	1	0	0	0	0	1	0	0
2338	0	1	0	0	0	1	0	0
2339	1	1	0	0	0	1	0	0
2340	0	1	0	0	1	0	0	0
2341	1	0	1	0	0	1	0	0
2342	0	1	1	0	0	1	0	0
2343	1	1	1	0	0	1	0	0
2344	0	0	0	1	0	1	0	0
2345	1	0	0	1	0	1	0	0
2346	0	1	0	1	0	1	0	0
2347	1	1	0	1	0	1	0	0

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2348	0	0	1	1	0	1	0	0
2349	1	0	1	1	0	1	0	0
2350	0	1	1	1	0	1	0	0
2351	1	1	1	1	0	1	0	0
2352	0	0	0	0	1	1	0	0
2353	1	0	0	0	1	1	0	0
2354	0	1	0	0	1	1	0	0
2355	1	1	0	0	1	1	0	0
2356	0	0	1	0	1	1	0	0
2357	1	0	1	0	1	1	0	0
2358	0	1	1	0	1	1	0	0
2359	1	1	1	0	1	1	0	0
2360	0	0	0	1	1	1	0	0
2361	1	0	0	1	1	1	0	0
2362	0	1	0	1	1	1	0	0
2363	1	1	0	1	1	1	0	0
2364	0	0	1	1	1	1	0	0
2365	1	0	1	1	1	1	0	0
2366	0	1	1	1	1	1	0	0
2367	1	1	1	1	1	1	0	0
2368	0	0	0	0	0	0	1	0
2369	1	0	0	0	0	0	1	0
2370	0	1	0	0	0	0	1	0
2371	1	1	0	0	0	0	1	0
2372	0	0	1	0	0	0	1	0
2373	1	0	1	0	0	0	1	0
2374	0	1	1	0	0	0	1	0
2375	1	1	1	0	0	0	1	0
2376	0	0	0	1	0	0	1	0
2377	1	0	0	1	0	0	1	0
2378	0	1	0	1	0	0	1	0
2379	1	1	0	1	0	0	1	0
2380	0	0	1	1	0	0	1	0
2381	1	0	1	1	0	0	1	0
2382	0	1	1	1	0	0	1	0
2383	1	1	1	1	0	0	1	0
2384	0	0	0	0	1	0	1	0
2385	1	0	0	0	1	0	1	0
2386	0	1	0	0	1	0	1	0
2387	1	1	0	0	1	0	1	0
2388	0	0	1	0	1	0	1	0
2389	1	0	1	0	1	0	1	0
2390	0	1	1	0	1	0	1	0
2391	1	1	1	0	1	0	1	0

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2392	0	0	0	1	1	0	1	0
2393	1	0	0	1	1	0	1	0
2394	0	1	0	1	1	0	1	0
2395	1	1	0	1	1	0	1	0
2396	0	0	1	1	1	0	1	0
2397	1	0	1	1	1	0	1	0
2398	0	1	1	1	1	0	1	0
2399	1	1	1	1	1	0	1	0
2400	0	0	0	0	0	1	1	0
2401	1	0	0	0	0	1	1	0
2402	0	1	0	0	0	1	1	0
2403	1	1	0	0	0	1	1	0
2404	0	0	1	0	0	1	1	0
2405	1	0	1	0	0	1	1	0
2406	0	1	1	0	0	1	1	0
2407	1	1	1	0	0	1	1	0
2408	0	0	0	1	0	1	1	0
2409	1	0	0	1	0	1	1	0
2410	0	1	0	1	0	1	1	0
2411	1	1	0	1	0	1	1	0
2412	0	0	1	1	0	1	1	0
2413	1	0	1	1	0	1	1	0
2414	0	1	1	1	0	1	1	0
2415	1	1	1	1	0	1	1	0
2416	0	0	0	0	1	1	1	0
2417	1	0	0	0	1	1	1	0
2418	0	1	0	0	1	1	1	0
2419	1	1	0	0	1	1	1	0
2420	0	0	1	0	1	1	1	0
2421	1	0	1	0	1	1	1	0
2422	0	1	1	0	1	1	1	0
2423	1	1	1	0	1	1	1	0
2424	0	0	0	1	1	1	1	0
2425	1	0	0	1	1	1	1	0
2426	0	1	0	1	1	1	1	0
2427	1	1	0	1	1	1	1	0
2428	0	0	1	1	1	1	1	0
2429	1	0	1	1	1	1	1	0
2430	0	1	1	1	1	1	1	0
2431	1	1	1	1	1	1	1	0
2432	0	0	0	0	0	0	0	1
2433	1	0	0	0	0	0	0	1
2434	0	1	0	0	0	0	0	1
2435	1	1	0	0	0	0	0	1

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2436	0	0	1	0	0	0	0	1
2437	1	0	1	0	0	0	0	1
2438	0	1	1	0	0	0	0	1
2439	1	1	1	0	0	0	0	1
2440	0	0	0	1	0	0	0	1
2441	1	0	0	1	0	0	0	1
2442	0	1	0	1	0	0	0	1
2443	1	1	0	1	0	0	0	1
2444	0	0	1	1	0	0	0	1
2445	1	0	1	1	0	0	0	1
2446	0	1	1	1	0	0	0	1
2447	1	1	1	1	0	0	0	1
2448	0	0	0	0	1	0	0	1
2449	1	0	0	0	1	0	0	1
2450	0	1	0	0	1	0	0	1
2451	1	1	0	0	1	0	0	1
2452	0	0	1	0	1	0	0	1
2453	1	0	1	0	1	0	0	1
2454	0	1	1	0	1	0	0	1
2455	1	1	1	0	1	0	0	1
2456	0	0	0	1	1	0	0	1
2457	1	0	0	1	1	0	0	1
2458	0	1	0	1	1	0	0	1
2459	1	1	0	1	1	0	0	1
2460	0	0	1	1	1	0	0	1
2461	1	0	1	1	1	0	0	1
2462	0	1	1	1	1	0	0	1
2463	1	1	1	1	1	0	0	1
2464	0	0	0	0	0	1	0	1
2465	1	0	0	0	0	1	0	1
2466	0	1	0	0	0	1	0	1
2467	1	1	0	0	0	1	0	1
2468	0	0	1	0	0	1	0	1
2469	1	0	1	0	0	1	0	1
2470	0	1	1	0	0	1	0	1
2471	1	1	1	0	0	1	0	1
2472	0	0	0	1	0	1	0	1
2473	1	0	0	1	0	1	0	1
2474	0	1	0	1	0	1	0	1
2475	1	1	0	1	0	1	0	1
2476	0	0	1	1	0	1	0	1
2477	1	0	1	1	0	1	0	1
2478	0	1	1	1	0	1	0	1
2479	1	1	1	1	0	1	0	1

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2480	0	0	0	0	1	1	0	1
2481	1	0	0	0	1	1	0	1
2482	0	1	0	0	1	1	0	1
2483	1	1	0	0	1	1	0	1
2484	0	0	1	0	1	1	0	1
2485	1	0	1	0	1	1	0	1
2486	0	1	1	0	1	1	0	1
2487	1	1	1	0	1	1	0	1
2488	0	0	0	1	1	1	0	1
2489	1	0	0	1	1	1	0	1
2490	0	1	0	1	1	1	0	1
2491	1	1	0	1	1	1	0	1
2492	0	0	1	1	1	1	0	1
2493	1	0	1	1	1	1	0	1
2494	0	1	1	1	1	1	0	1
2495	1	1	1	1	1	1	0	1
2496	0	0	0	0	0	0	1	1
2497	1	0	0	0	0	0	1	1
2498	0	1	0	0	0	0	1	1
2499	1	1	0	0	0	0	1	1
2500	0	0	1	0	0	0	1	1
2501	1	0	1	0	0	0	1	1
2502	0	1	1	0	0	0	1	1
2503	1	1	1	0	0	0	1	1
2504	0	0	0	1	0	0	1	1
2505	1	0	0	1	0	0	1	1
2506	0	1	0	1	0	0	1	1
2507	1	1	0	1	0	0	1	1
2508	0	0	1	1	0	0	1	1
2509	1	0	1	1	0	0	1	1
2510	0	1	1	1	0	0	1	1
2511	1	1	1	1	0	0	1	1
2512	0	0	0	0	1	0	1	1
2513	1	0	0	0	1	0	1	1
2514	0	1	0	0	1	0	1	1
2515	1	1	0	0	1	0	1	1
2516	0	0	1	0	1	0	1	1
2517	1	0	1	0	1	0	1	1
2518	0	1	1	0	1	0	1	1
2519	1	1	1	0	1	0	1	1
2520	0	0	0	1	1	0	1	1

Frequency (MHz)	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
2521	1	0	0	1	1	0	1	1
2522	0	1	0	1	1	0	1	1
2523	1	1	0	1	1	0	1	1
2524	0	0	1	1	1	0	1	1
2525	1	0	1	1	1	0	1	1
2526	0	1	1	1	1	0	1	1
2527	1	1	1	1	1	0	1	1
2528	0	0	0	0	0	1	1	1
2529	1	0	0	0	0	1	1	1
2530	0	1	0	0	0	1	1	1
2531	1	1	0	0	0	1	1	1
2532	0	0	1	0	0	1	1	1
2533	1	0	1	0	0	1	1	1
2534	0	1	1	0	0	1	1	1
2535	1	1	1	0	0	1	1	1
2536	0	0	0	1	0	1	1	1
2537	1	0	0	1	0	1	1	1
2538	0	1	0	1	0	1	1	1
2539	1	1	0	1	0	1	1	1
2540	0	0	1	1	0	1	1	1
2541	1	0	1	1	0	1	1	1
2542	0	1	1	1	0	1	1	1
2543	1	1	1	1	0	1	1	1
2544	0	0	0	0	1	1	1	1
2545	1	0	0	0	1	1	1	1
2546	0	1	0	0	1	1	1	1
2547	1	1	0	0	1	1	1	1
2548	0	0	1	0	1	1	1	1
2549	1	0	1	0	1	1	1	1
2550	0	1	1	0	1	1	1	1
2551	1	1	1	0	1	1	1	1
2552	0	0	0	1	1	1	1	1
2553	1	0	0	1	1	1	1	1
2554	0	1	0	1	1	1	1	1
2555	1	1	0	1	1	1	1	1
2556	0	0	1	1	1	1	1	1
2557	1	0	1	1	1	1	1	1
2558	0	1	1	1	1	1	1	1
2559	1	1	1	1	1	1	1	1