GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Wireless Penetration Testing and Ethical Hacking (Security 617)"
at http://www.giac.org/registration/gawn

802.11 Denial of Service Attacks and Mitigation

GAWN Gold Certification

Author: Stuart Compton, stuartcompton@hotmail.com

Adviser: Charles Hornat

Accepted: May 17th 2007

© SANS Institute 2008, Author retains full rights.

Table of Contents

1. Introduction 4

2. Background 6

3. Application Layer 7 attacks 8

4. Transport Layer 4 attacks 9

5. Network Layer 3 attacks 12

6. Media Access Control (MAC) Layer 2 attacks 13

7. Client attacks 22

8. Defensive measures 24

9. 802.11w to the rescue? 27

10. Summary 28

11. References 29

12. Appendix A 31

© SANS Institute 2008, Author retains full rights.

13. Appendix B 32

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

1. Introduction

Wireless solutions are in great demand as organisations seek to become more flexible and productive. Employees are increasingly accessing their organisation's network from home wireless networks or public wireless "hotspots".

Organisations today are increasing their dependence on wireless networks in order to operate and maintain a cost effective and competitive advantage. Wireless networks offer organisations mobility, allowing their users to physically move about whilst maintaining a connection to the organisation's wireless network. There is also a cost saving when compared with the traditional installation of a wired network. However, organisations need to control and prevent their network and systems from being exposed to wireless attacks.

Many organisations overlook the potential impact of a Denial of Service (DoS) attack against their wireless networks. Wireless networks can be very vulnerable to DoS attacks and the results can be anything from degradation of the wireless network to a complete loss of availability of the wireless network within the organisation.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

It does not require much expertise and expensive equipment to launch a DoS attack against an organisation. These attacks could be launched by competitors, for political reasons, as part of a combined attack or just frustration on an attacker's part of not being able to break into an organisation's network.

DoS attacks can be launched from inside an organisation or from the outside at great distance using readily available standard wireless equipment. It is also much harder to physically secure wireless networks in the same way that wired networks can be.

This GIAC Gold Certification paper explores DoS attacks against wireless networks, introducing some examples of DoS attacks and some of the tools and techniques available that attackers can make use of. We will also discuss some of the available defensive measures that can be adopted by an organisation to protect their business and what the Institute of Electrical and Electronics Engineers (IEEE)[6] are doing to help mitigate DoS attacks.

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

2. Background

Since the ratification of the IEEE 802.11i[7] in 2004, organisations have been able to improve security on their wireless networks by making use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code protocol). CCMP uses AES (Advanced Encryption Standard) as opposed to the RC4 streaming cipher found in implementations of WEP (Wired Equivalent Privacy) and TKIP (Temporal Key Integrity Protocol). However, the protection offered by 802.11i applies only to data frames and does not provide any protection over the management frames. It is these management frames that are insecure and can lead to DoS attacks against an organisation's wireless network.

Unencrypted management frames can disclose important pieces of information to an attacker, including details about the type of wireless equipment in use on the wireless network and configuration settings.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

It is important to classify the types of wireless DoS attacks that an attacker can carry out against an organisation's wireless network. DoS attacks can target many different layers of the Open Systems Integration (OSI) model[8].

These include the Application Layer 7, Transport Layer 4, Network Layer 3, Media Access Control (MAC) Layer 2 and lastly the Physical Layer 1. The wireless clients themselves can also be a target for a wireless attack.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

3. Application Layer 7 attacks

An Application layer DoS attack can be carried out on a wired or wireless network. It is achieved by an attacker sending large amounts of legitimate requests to an application. For example, an HTTP flood attack can make hundreds of thousands of page requests to a web server which can exhaust all of the server's processing capability. With an HTTP flood attack, an attacker sends a SYN packet, and the target system responds with a SYN ACK. The attacker will complete the three way handshake with an ACK packet and then issues an HTTP GET request for a common page on the target system. This process amplified on a wireless network can cause a very high computational load on the target system and may result in degradation of the wireless network to a complete loss of availability of the application. One of the best examples of an HTTP flood attack was the MyDoom[9] worm, which targeted many thousands of sites. In the case of MyDoom, 64 requests were sent every second from every infected system. With thousands of infected systems, the attack can prove to be overwhelming.

© SANS Institute 2008, Author retains full rights.

4. Transport Layer 4 attacks

A Transport layer DoS attack can be carried out on a wired or wireless network. A transport layer DoS attack involves sending many connection requests to a target host. This attack is targeted against the operating system of the victim. It is very effective and extremely difficult to trace back to the attacker because of IP spoofing techniques used.

An example transport layer attack is the TCP SYN flood[10]. When a normal TCP connection starts, the client sends a SYN packet from a specific port to a server where the port is in a listening state. The server will then send back a SYN ACK. The server will wait for an ACK acknowledge of the SYN ACK before the connection can be established. This is known as the TCP three-way handshake (See Figure 1.0).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

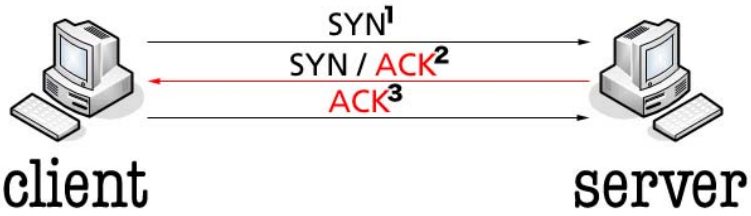


Figure 1.0: The standard TCP three-way handshake

However, the problem with the TCP three-way handshake process is that systems allocate resources to connections that have not been fully established - these are also known as half-open connections. Too many of these potential connection requests can exhaust all resources allocated to setting up a connection. When the SYN flood attack starts, attackers will send large amounts of SYN packets to the target system. These SYN packets can be from spoofed source addresses of unreachable systems. If the attacker is spoofing source addresses from systems that are unreachable, the target system will attempt to complete the session by sending back SYN ACK packets which will never be acknowledged or reset (ACK or RST packets).

© SANS Institute 2008, Author retains full rights.

The target system is now committed to setting up a connection, and this attempted connection will only be removed from the queue after the connection establishment timer expires. The three-way handshake is therefore never completed and the system under attack will not be able to clear the queue before receiving new SYN requests. If the attacker generates SYN packets at a very rapid rate from spoofed source addresses of unreachable systems, it is possible to fill up the connection queue and deny TCP services for legitimate users on the wireless network and may result in degradation of the wireless network.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

5. Network Layer 3 attacks

A Network layer DoS attack can be carried out on a wired or wireless network. If a wireless network allows any client to associate to it, the wireless network could be vulnerable to a network layer attack. A network layer DoS attack is achieved by sending a large amount of data to a wireless network. This type of attack targets the wireless network infrastructure of the victim. A good example of a network layer attack is the ICMP flood[11].

The ICMP flood attack works by an attacker sending so many ICMP ECHO REQUEST packets to the target wireless system that it cannot respond fast enough to ease the amount of traffic. If the attacker spoofs the source IP address, then the attacker can use all of its resources to just send packets, while the target wireless system has to use all of its resources to process the packets. If the attacker makes use of thousands of systems to perform this attack, the target wireless system may be brought down.

The attack will quickly consume all available bandwidth, resulting in legitimate users being unable to access wireless services.

© SANS Institute 2008, Author retains full rights.

6. Media Access Control (MAC) Layer 2 attacks

On an 802.11 network, an attacker can transmit packets using a spoofed source MAC address of an access point. The recipient of these spoofed frames has no way of telling if they are legitimate or illegitimate requests and will process them. The ability to transmit spoofed management frames allows MAC layer DoS attacks to take place.

Two such MAC layer attacks are the authentication/association flood attack and the deauthentication/disassociation flood attacks.

Authentication/Association flood attack

During the authentication/association flood attack, an attacker uses spoofed source MAC addresses that attempt to authenticate and associate to a target access point. The attacker repeatedly makes authentication/association requests, eventually exhausting the memory and processing capacity of the access point leaving clients with little or no connection to the wireless network.

© SANS Institute 2008, Author retains full rights.

The void11[12] tool will execute an authentication/association flood attack against a target. When the attacker is equipped with a high-gain antenna, void11 could be used to target many access points in a specific area.

The command line options for void11 are detailed as follows:

```
void11_penetration wlan0 -D -t <type of attack> -s <station MAC address> -S <SSID> -B <BSSID>
```

The void11 command line options are detailed in Appendix A.

Deauthentication/Disassociation flood attack

In a deauthentication/disassociation flood attack, an attacker transmits spoofed frames with the source address of the access point. When the recipient receives the frames, they will disconnect from the network and attempt to reconnect. If the attack is sustained, the clients will be unable to maintain a connection to the wireless network.

The deauthentication/disassociation flood attack targets one or all users on a specific BSSID (MAC address of the access point).

© SANS Institute 2008, Author retains full rights.

The file2air[13] tool written by Joshua Wright will execute a deauthentication flood attack against a target by the repeated transmission of a deauthenticate frame to a specified target. The victim is then unable to reconnect to the wireless network.

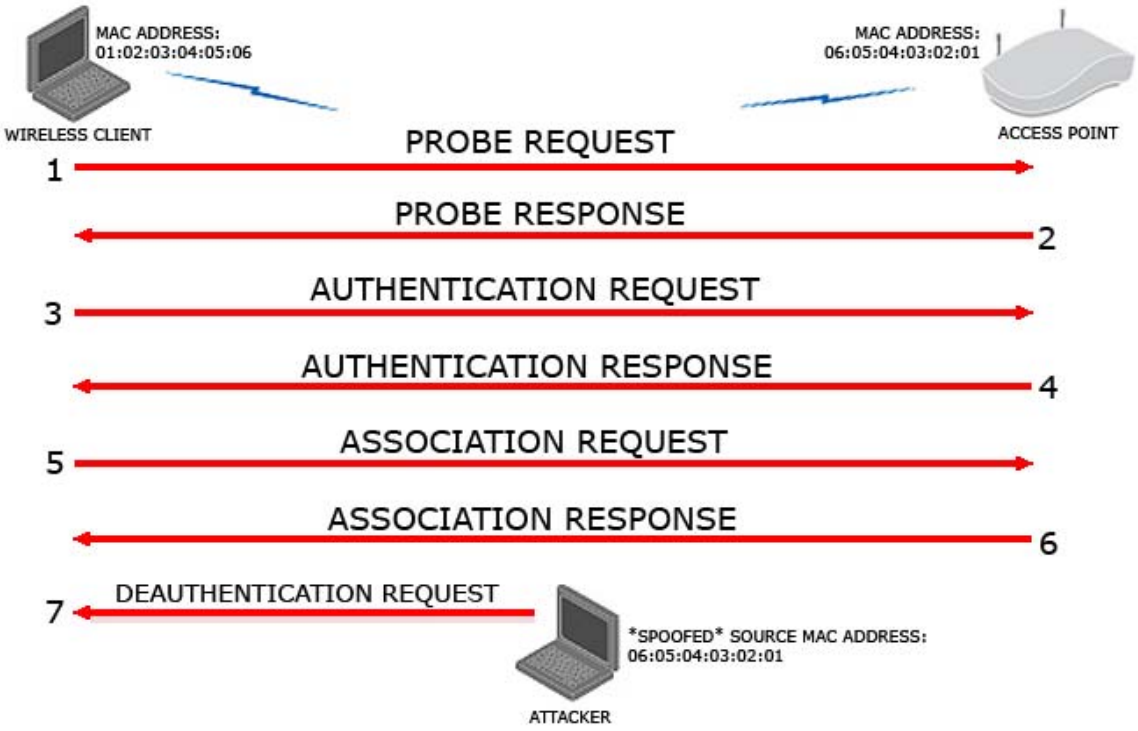


Figure 2.0: A deauthentication attack on an open wireless network

© SANS Institute 2008, Author retains full rights.

Using the file2air tool to perform a deauthentication flood DoS attack against a victim, the attacker needs to locate the network BSSID (MAC address of access point) that they want to attack. This information can be gained through sniffing the network using protocol analyser tools such as tcpdump[14] or wireshark[15] (formerly ethereal).

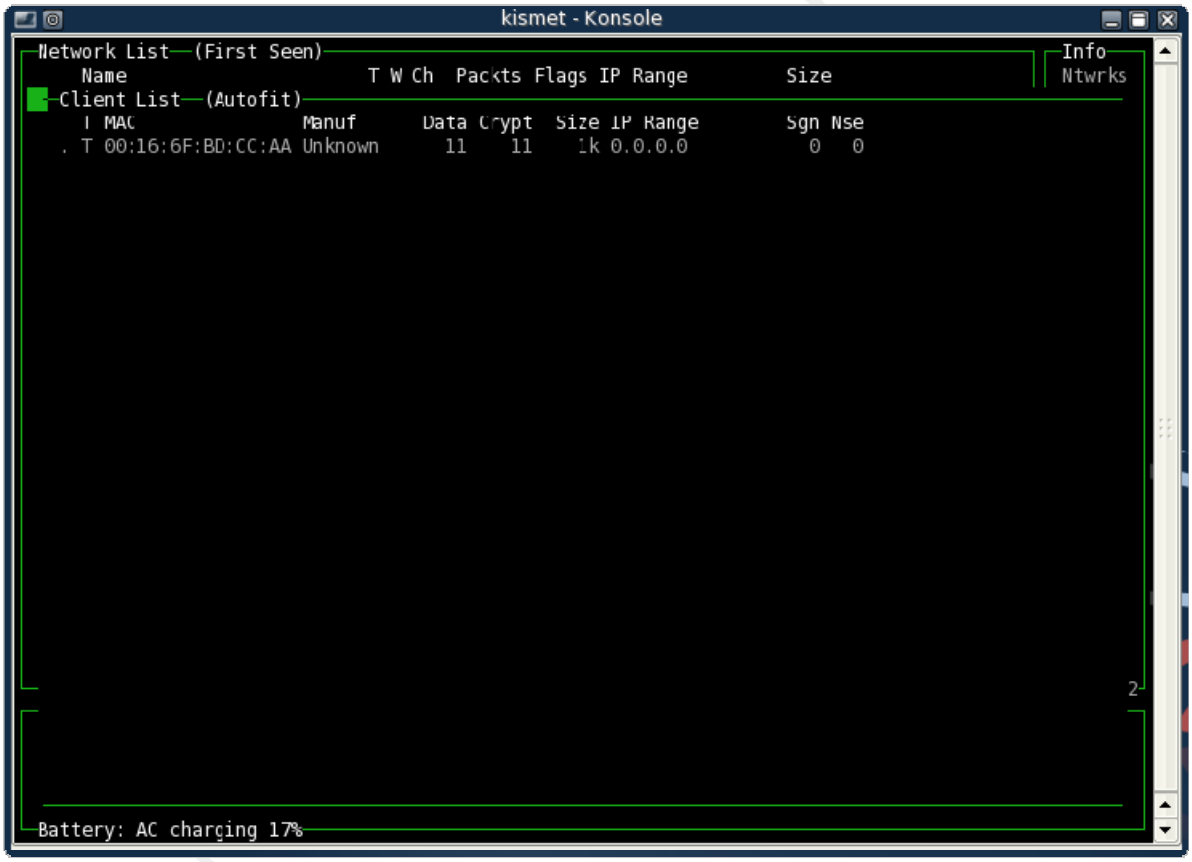
Implementing the deauthenticate flood attack is straightforward. An attacker runs the file2air command specifying an interface name to transmit the packet on, the driver the interface is using, the supplied deauth.bin file, channel number, number of packets to transmit, timing between packets, victim's destination address, spoofed source address and finally the BSSID. File2air will then inject the traffic until the packet count is exceeded. The command line options are detailed as follows:

```
File2air –i wlan0 –r wlan-ng –f deauth.bin –c <channel> -n 100000 –t –d <victim MAC address> -s <access point MAC address> -b <BSSID>
```

The file2air command line options are detailed in Appendix B.

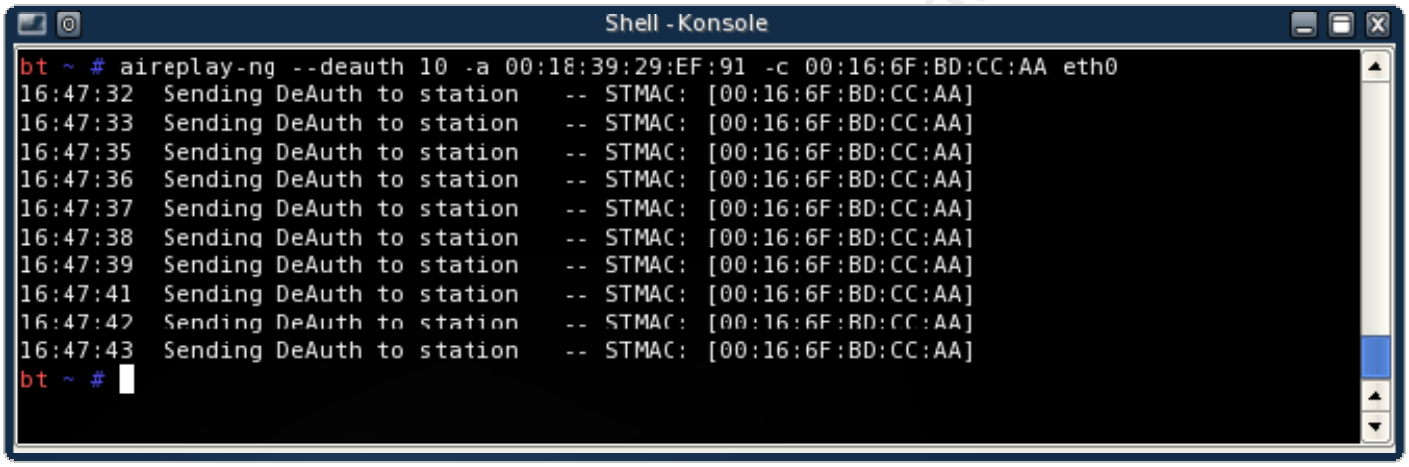
© SANS Institute 2008, Author retains full rights.

The aircrack-ng[16] suite also includes aireplay-ng which can be used to send deauthentication packets to one or more clients which are currently associated with a particular access point. To find out what clients are currently associated with an access point, wireless auditing tools such as Kismet[17] can be used. In the screenshot below, Kismet as been used to identify an access point that has wireless clients associated with it.



© SANS Institute 2008, Author retains full rights.

The aireplay-ng tool can then used to send deauthentication packets to the targeted wireless client. The following screenshot shows ten deauthentication packets sent to the targeted wireless client.



This will cause the wireless client to become deauthenticated creating a denial of service if the attack is sustained.

© SANS Institute 2008, Author retains full rights.

The command line options for the aireplay-ng tool are detailed as follows:

```
aireplay-ng --deauth 10 -a 00:18:39:29:EF:91 -c 00:16:6F:BD:CC:AA eth0
```

- --deauth means deauthentication
- 10 is the number of deauthentication packets to send. To send continuous deauthentication packets a 0 can be used
- -a 00:18:39:29:EF:91 is the MAC address of the access point
- -c 00:16:6F:BD:CC:AA is the MAC address of the client to deauthenticate. If this is omitted then all clients are deauthenticated
- eth0 is the wireless interface name

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Physical Layer 1 attacks

A physical layer attack on a wired network ideally requires the attacker to be inside or very close to the target wireless network. Any network that relies on a shared medium is subject to DoS attacks from other devices sharing the same medium. When one device saturates the medium, other clients will find it difficult to communicate. An attacker using a laptop equipped with a high output wireless client card and a high gain antenna can launch a physical medium attack on an organisation's wireless network by generating enough RF noise to reduce the signal-to-noise ratio to an unusable level by saturating the 802.11 frequency bands. The jamming device could also be a custom built transmitter.

For example, a Power Signal Generator (PSG) that is used to test antennas, cables and connectors for wireless devices can be turned into a wireless jamming device, when connected to a high gain antenna.

© SANS Institute 2008, Author retains full rights.

It is not possible to stop someone from transmitting using the same frequency used by wireless networks. Disruptions to organisations can also be caused by noise from everyday household items such as microwave ovens, cordless phones, or any other appliance that operate on the 2.4 GHz or 5 GHz radio frequency that 802.11 networks make use of.

There are also problems with Bluetooth networks which make use of the same ISM band as 802.11b and 802.11g wireless networks. For example, Direct Spread Sequence Spectrum (DSSS) [18] modulation in 802.11b is susceptible to the interference from the Frequency Hopping Spread Spectrum (FHSS)[19] modulation used in Bluetooth networks.

As a last resort, if the access point of an organisation can be physically located by an attacker, this or the antenna can also be the target of a physical attack leaving the clients with little or no connectivity.

© SANS Institute 2008, Author retains full rights.

7. Client attacks

Client attacks are attacks against the wireless stations themselves. For example, an attacker can set their Service Set Identifier (SSID) to be the same as an access point located at a wireless hotspot or a corporate wireless network. Then by directing a DoS attack against the access point, for example by creating RF interference around it, legitimate users will lose their connections to the wireless hotspot or an organisation's wireless network and re-connect to the attacker's access point. This is known as the "evil twin[20]" attack. A feature of Microsoft Windows XP SP1 clients is that they will automatically roam, authenticate and associate to an access point with a stronger signal. The outcome of an "evil twin" attack can vary. As the attacker's access point is not connected to the organisation's network, the victims will lose their connections to the legitimate access point when it re-connects to the attacker's access point. Additionally, an "evil twin" can present users with fake login pages, allowing the attacker to collect user credentials and intercept all the traffic to that device, potentially stealing sensitive data belonging to an organisation.

© SANS Institute 2008, Author retains full rights.

It is also relatively easy for an attacker to have a software based access point running on their laptop. This will allow a wireless card to perform all the functions of a hardware based access point. Coupled with an antenna, this can produce a stronger signal level than the victim's access point even when the attack is mounted from a significant distance. For example, Airsnarf[21] is a simple rogue wireless access point utility that is designed to demonstrate how a rogue access point can steal usernames and passwords by simulating popular public wireless hotspots.

While client attacks tend to target individual stations on a wireless network, it is possible to extend an attack to a larger number of victims by using broadcast destination addresses.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

8. Defensive measures

The protection offered by 802.11i does not defend against the attacks that we have discussed so far in this paper. By deploying Wireless LAN Intrusion Detection Systems (WLAN IDS) this will go some way towards helping to identify DoS attacks but not actually stop the attack that is taking place. A WLAN IDS will monitor the wireless environment with the help of sensors placed at strategic points. They can generate detailed reports about signal quality, signal-to-noise ratio and channel usage. The presence of an attacker can be identified and hopefully administrators within the organisation alerted. Having three or more appropriately placed sensors can help to apply triangulation[22] methods to approximately locate the source of a transmission.

To defend against physical attacks, strategic placement of access points is crucial. Mounting access points at heights will at least prevent attackers from easily reaching and destroying the access point. Aiming directional access point antennas towards the inside of the building will help to contain the Radio Frequency (RF) signal.

© SANS Institute 2008, Author retains full rights.

Organisations can help to protect a wireless network against DoS attacks by making the buildings as resistive as possible to incoming radio signals. Installation of metallic window tint instead of blinds or curtains can help prevent RF leakage and incoming radio signals.

Also the use of metallic based "Wi-Fi proof wallpaper"[23] and "Wi-Fi paint"[24] on the interior parts or the exterior walls will reduce RF leakage and incoming radio signals. Wi-Fi proof wallpaper has been designed to control the transmission of RF signals. It can be incorporated into properly screened rooms and acts as an RF window which can be turned on and off. This allows control over the way systems using WiFi or indeed mobile phones may be accessed. Wi-Fi paint is available that is water based and approved as a TEMPEST[25] (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions) countermeasure by the National Security Agency (NSA).

It is always good security practice for an organisation to carry out wireless audit testing on their wireless network. This will determine how far the RF signal actually extends outside of the organisation and the RF signal power levels can be adjusted accordingly until the leakage is eliminated or reduced to the point that it would be hard for an attacker to carry out attacks on the wireless network.

© SANS Institute 2008, Author retains full rights.

Improving the security of wireless networks by protecting the vulnerable management frames is essential to preventing many of the wireless DoS attacks that we have discussed in this paper so far. With this in mind, the IEEE formed the 802.11w[26] working group in February 2005 to address these issues.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

9. 802.11w to the rescue?

The IEEE goal with 802.11w is to protect management frames in 802.11 networks. This therefore provides wireless networks within organisations the protection against numerous DoS attacks targeted at the Media Access Control (MAC) layer 2. The 802.11w standard will look to provide protection in the following ways:

- Protecting unicast management frames from forgery and disclosure attacks by encrypting the unicast management frames between an access point and the client.
- Protecting broadcast management frames from forgery attacks.
- Protecting broadcast deauthentication and disassociation frames from forgery attacks.

© SANS Institute 2008, Author retains full rights.

10. Summary

In this paper we have looked at some of the issues with wireless DoS attacks and some of the measures to help mitigate these attacks. We have seen that the 802.11i specification does not address DoS attacks against wireless networks. New security standards can introduce new security flaws. However, it is hoped that the 802.11w standard will address many of the DoS attacks and wireless users and organisations are encouraged to research and look into upgrading to the new security standard as and when it becomes available.

The 802.11w standard is not due to be ratified until April 2008. We should not expect that the 802.11w specification completely mitigates DoS issues on wireless networks as it can never mitigate the effectiveness of jamming attacks or physical attacks at layer 1. Strategic placement of access points and RF containment are really the key here.

However, 802.11w will certainly be a step in the right direction in reducing the DoS attacks which are not addressed by the current 802.11i standard.

© SANS Institute 2008, Author retains full rights.

11. References

1) 802.11 Security - Bruce Potter & Bob Fleck (O'Reilly)

2) Wifoo - Andrew A. Vladimirov, Konstantin V. Gavrilenko & Andrei A. Mikhailovsky (Addison-Wesley)

3) 802.11 Wireless Networks – Matthew S. Gast (O'Reilly)

4) Wireless Hacks – 100 Industrial-Strength Tips & Tools – Rob Flickenger (O'Reilly)

5) Network Security Assessment – Chris McNab (O'Reilly)

6) Institute of Electrical and Electronics Engineers (IEEE) - http://www.ieee.org/portal/site

7) IEEE 802.11i standard - http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

8) OSI Model - http://en.wikipedia.org/wiki/OSI_model

9) Mydoom (computer worm) - http://en.wikipedia.org/wiki/Mydoom

10) TCP SYN Flood Attacks - http://www.cert.org/advisories/CA-1996-21.html

11) ICMP Flood Attacks - http://www.securityfocus.com/infocus/1853

12) Void11 - http://www.wlsec.net/void11

13) File2air – Joshua Wright

14) Tcpdump - http://www.tcpdump.org/

15) Wireshark - http://www.wireshark.org/

16) Aircrack-ng - http://www.aircrack-ng.org/doku.php

17) Kismet - http://www.kismetwireless.net/

18) Direct Spread Sequence Spectrum (DSSS) - http://www.ieee802.org/11/Tutorial/ds.pdf

© SANS Institute 2008, Author retains full rights.

19) Frequency Hopping Spread Spectrum - http://www.ieee802.org/11/Tutorial/FH.pdf

20) Evil Twin attack - http://www.wi-fiplanet.com/columns/article.php/3482021

21) Airsnarf - http://airsnarf.shmoo.com/

22) Triangulation - http://en.wikipedia.org/wiki/Triangulation

23) Wi-Fi wallpaper - http://www.baesystems.com/ProductsServices/ss_tes_atc_adv_mat_stealthy.html

24) Wi-Fi paint - http://www.wi-fiplanet.com/news/article.php/3667871

25) TEMPEST - http://www.tech-faq.com/tempest.shtml

26) 802.11w - http://en.wikipedia.org/wiki/IEEE_802.11w

27) 802.11w update - http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm

28) Artwork – Tom Neaves (tom@tomneaves.co.uk)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

12. Appendix A

The void11 command line options are as follows:

Command	Argument	Description
wlan0	wlan0	Interface name to use
-t	0,1,2 or 3	0: no action 1: deauth stations 2: auth flood 3: assoc flood
-s	<station MAC address>	Station (default: ff:ff:ff:ff:ff:ff / random)
-S	<SSID>	SSID (default: ‘ ‘)
-B	<BSSID>	BSSID (default: scan for BSSID’s)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

13. Appendix B

The file2air command line options are as follows:

Command	Argument	Description
-i	wlan0	Interface name to use for transmitting packets
-r	wlan-ng	Driver name used for wlan0 interface
-f	deauth.bin	Binary file describing the packet to inject
-c	<channel number>	The channel number of the victim
-n	100000	Number of packets to transmit
-t		Inject 10 packets per second
-d	<victim MAC address>	Destination address to send packets to
-s	<AP MAC address>	Spoofed source MAC address of the AP
-b	<BSSID>	BSSID address to spoof

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.