Global Information Assurance Certification Paper

Wireless Attacks from an

Intrusion Detection Perspective

GCIA Gold Certification

Author: Gary Deckerd, gdeckerd@secureworks.com

Adviser: Dominicus Adriyanto Hindarto

Accepted: November 23rd 2006

Abstract

Security professionals commonly implement wired intrusion detection systems, but wireless intrusion detection systems (WIDS) are not as prevalent. Many security professionals simply do not understand the nature of wireless networks or the attacks they are prone to. Intrusion detection is available for wireless networks, but just how does wireless intrusion detection work and why is it different from wired IDS. In this paper I will discuss wireless intrusion detection systems and explain how to detect common wireless attacks.

Table of Contents

1. Why Wireless Intrusion Detection Is Needed

Wireless networks are prevalent everywhere from corporate offices, coffee shops and city parks. These networks are commonly implemented because of the ease of deployment and their ability to provide network access to areas where running cable is not an option. Wireless networks allow employees to roam offices and buildings and provide guests with internet access. However, this same ease of access and mobility can also be leveraged by malicious individuals to attack from the most unlikely of locations. Wireless networks do not have defined borders and air waves can penetrate into unintended areas allowing attackers to bypass perimeter firewalls, sniff sensitive information, access the internal network or attack wireless hosts without direct access to the network.

Proper design of a wireless network can help minimize wireless threats, but like wired networks, defense in depth should be implemented to minimize risk. Security professionals implementing defense in depth on a wireless network need wireless IDS in order to have proper vision to view wireless attacks.

2. What is the Difference between Wireless and Wired IDS?

Many security professionals do not realize that wireless and wired intrusion detection systems are very different. Many are under the impression that traditional intrusion detection systems, like snort, are sufficient whether the data is transmitted through the air or over a wire.

A wireless IDS is unique in that it detects attacks against the 802.11 frame at layer two of the wireless network. There are three different types of 802.11 MAC frames; data, control, and management (Geier, 2002). The majority of wireless attacks target management frames, because they are responsible for authentication, association, disassociation, beacons, and probe request/response (IEEE, 2003). Wireless threats like man-in-the-middle attacks, rogue access points, war drivers and denial of service attacks function within the 802.11 frames and cannot be detected on layer three past the access point. Wired IDS will not receive these frames, because management frames are not forwarded to upper layers of the OSI model.

3. Effective Deployment of Wireless IDS (WIDS)

Like traditional wired intrusion detection systems that are deployed to monitor a network, wireless intrusion detection systems need a dedicated interface. This wireless interface should run in monitor mode, also known as RFMON mode; this mode is similar to promiscuous mode for wired devices and allows the device to accept all incoming traffic (Wikipedia contributors, 2006).

Another important aspect of a wireless IDS is that the monitoring interface should hop between the 12 channels available to wireless networks. Several wireless attacks work by utilizing a rogue AP on a different channel. For instance, man-in-the-middle attacks utilize a rogue AP that is at least 5 channels away from the target AP. Without channel hopping the wireless IDS would be blind to attacks that function on other channels.

WIDS can be deployed using a network of dedicated wireless devices running in monitor mode. Since the wireless IDS is separate from the access points it is important for the monitoring devices to match the coverage of the wireless network. Wireless site surveys should be performed to ensure that the WIDS covers the entire wireless network. The case study contains an example of a WIDS deployed in this fashion.

Ideally, manufactures would include two wireless interfaces on access points, one to transmit and receive traffic and one monitor interface. With the monitor interface built into the AP there will be fewer devices to manage and the IDS will provide adequate coverage of the wireless network.

4. Detection Methodology

In order to detect the broad range of wireless attacks, wireless IDS systems pair signature and knowledge-based detection methodologies (Vladimirov, Gavrilenko, and Mikhailovsky, 2004).

Signature-based detection utilizes static signatures to match bad traffic. This type of matching works well for known attacks that match a predefined pattern. For example, in order to detect rogue access points, the IDS utilize a list of authorized access points then alerts when a detected AP does not match the list(Vladimirov et al., 2004).

Knowledge-based detection employs a historical baseline and alerts when network traffic varies from the historical baseline. Many wireless attacks do not match a signature, but instead cause network traffic anomalies that a knowledge-based IDS can detect. For instance, to generate enough packets to crack a WEP

key an attacker can replay captured traffic onto the wireless network. This attack causes the amount of network traffic to increase drastically in comparison to the historical baseline (Vladimirov et al., 2004).

5. Wireless IDS and False Positives

Like traditional intrusion detection systems, wireless systems will not provide valuable data without proper tuning. Knowledge-based detection engines are particularly prone to false positives, because they rely upon a historical baseline. If the historical baseline has been tainted by attacks occurring when the baseline was developed then false negatives or positives will be more likely. To mitigate this factor, a long historical baseline is needed and should be updated periodically to account for new network patterns (Vladimirov et al., 2004).

6. WEP Cracking

WEP keys have been known to be vulnerable since August 2001 and in 2005 the FBI demonstrated cracking a 64 bit WEP key in 3 minutes using publicly available tools (Wikipedia contributors, 2006). WEP keys are still in use by thousands of home access points and corporate locations to protect against individuals casually accessing the wireless network. However, a more secure wireless network will simply avoid WEP and employ radius-based WPA, or an open network that requires VPN.

An attacker needs about 200,000 – 700,000 encrypted data frames to crack 128 bit encryption, and only 50,000-200,000 frames to crack 64 bit encryption (Cheung, 2005). The speed and accuracy of this attack depends on the number of packets an attacker can gather. There are no preventative measures to block

this type of attack; however the rate at which the attacker gathers packets to crack the key will increase the chances of detection. An attacker will need between 10 to 15 minutes to gather the number of packets needed to crack 128 bit WEP. Within this time frame he/she will generate thousands of duplicate packets.

WEP Cracking Technical Details

WEP Keys use a 24 bit initialization vector(IV) concatenated by a static 104 bit or 40 bit key. The IV is sent in the clear, within the packet and can be reused on the wireless network. If an attacker can gather enough unique IV's then he/she can crack the WEP key.

128 bit WEP = 24 bit IV + 104 bit Key

64 bit WEP = 24 bit IV + 40 bit Key

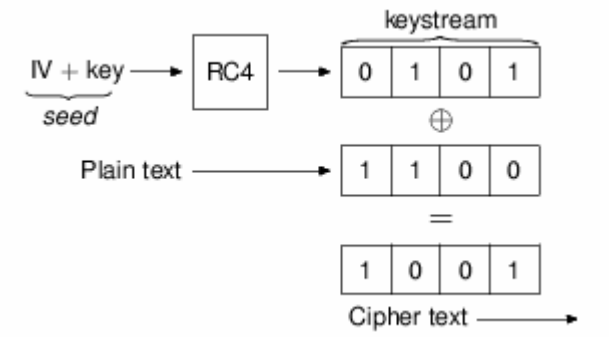

Figure 1: Basic WEP Encryption: RC4 Keystream XORed with Plaintext (Wikipedia contributors, 2006)

6.1 Malicious Reasons to Crack WEP

1. Decrypt Sniffed Traffic

2. Connect to WEP protected access point

3. Use in man-in-the-middle attack to clone AP.

6.2 Passive Cracking:

Passive cracking is done by simply listening and recording packets sent by the AP and its clients. Even on a busy network, this method is slow, it could take up to a few hours to capture enough packets to crack the WEP key. On slow networks or a SOHO wireless router this could take days or even weeks (Vladimirov et al., 2004).

Passive Cracking Detection:

An intrusion detection system cannot detect passive WEP cracking, because the attacker does not generate any traffic. Physically spotting an attacker is the only option available for detecting a passive attacker. The attacker could capture packets using a PDA or a laptop, therefore physically spotting an attacker could be difficult.

6.3 Active Cracking: (Selective Packet Injection)

Active Cracking can be detected because the attacker generates traffic on the network. Two common forms of active cracking are to de-authenticate hosts from an AP or reinject sniffed traffic into the network (Cheung, 2005).

6.3.1 De-authentication Attack:

When a host authenticates to a WEP protected AP there are six packets involved in the authentication. Two of these packets can be used to crack the WEP key. Below is a capture of a six packet authentication between the client, 00:14:6C:6C:AA:77, and the AP, 00:0F:66:2B:8A:CF.

1.
2.
3.
4.
5.
6.

```
BSSID:ff:ff:ff:ff:ff:ff DA:ff:ff:ff:ff:ff:ff SA:00:14:6c:6c:aa:77 Probe Request (gmd393) [1.0* 2.0* 5.5* 11.0* M
 4000 0000 ffff ffff ffff 0014 6c6c aa77  @...........ll.w
 ffff ffff ffff 408b 0006 676d 6433 3933  ......@...gmd393
 0104 8284 8b96 3208 8c12 9824 b048 606c  ......2....$.H`l
BSSID:00:0f:66:2b:8a:cf DA:00:14:6c:6c:aa:77 SA:00:0f:66:2b:8a:cf Probe Response (gmd393)  [1.0* 2.0* 5.5* 11.0*
 Mbit] CH: 1, PRIVACY
 5000 3a01 0014 6c6c aa77 000f 662b 8acf  P.:...ll.w..f+..
 000f 662b 8acf 9038 3525 472a 6500 0000  ..f+...85%G*e...
 6400 1104 0006 676d 6433 3933 0108 8284  d.....gmd393....
 8b96 2430 486c 0301 012a 0104 2f01 0432  ..$0Hl...*../..2
 040c 1218 60dd 0600 1018 0201 04         ....`........
BSSID:00:0f:66:2b:8a:cf DA:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 Authentication (Shared Key)-1: Succesful
 b000 3a01 000f 662b 8acf 0014 6c6c aa77  ..:...f+....ll.w
 000f 662b 8acf c08b 0100 0100 0000       ..f+..........
BSSID:00:0f:66:2b:8a:cf DA:00:14:6c:6c:aa:77 SA:00:0f:66:2b:8a:cf Authentication (Shared Key)-2 [Challenge Text]
 b000 3a01 0014 6c6c aa77 000f 662b 8acf  ..:...ll.w..f+..
 000f 662b 8acf e038 0100 0200 0000 1080  ..f+...8........
 00fc e2ee 707c e211 7553 65d5 5189 b552  ....p|..uSe.Q..R
 94a2 ec67 39c9 49b0 87c7 3bda 2ba7 3da9  ...g9.I...;.+.=.
 4841 0844 273f 0007 39ca 5741 f740 fa2c  HA.D'?..9.WA.@.,
 9b24 d8c0 0000 01f1 7189 b26e 8ba3 e3c3  .$......q..n....
 e2eb 5ad6 4a52 6c9c 1ce1 f079 cf7d eff9  ..Z.JRl....y.}..
 cb5f fce5 d082 ee75 526c 67c1 0e74 a3e5  ._.....uRlg..t..
 2e74 5b22 e8be 0d97 41f6 b290 86c9 4b65  .t["....A.....Ke
 d26f 79c9 4c9e 0f7d e9b7 bde9 b367 3f09  .oy.L..}.....g?.
 dd06 0010 1802 0004                      ........
BSSID:00:0f:66:2b:8a:cf DA:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 Authentication (Reserved)-de:
 b040 3a01 000f 662b 8acf 0014 6c6c aa77  .@:...f+....ll.w
 000f 662b 8acf d08b 0017 de00 6fb7 7eb4  ..f+........o.~.
 efea 42d0 f4d5 9e8c 6c7f ce77 3bf8 1828  ..B.....l..w;..(
 fece 3999 5f88 34ab a7cc bc70 7fe7 9c0f  ..9._.4....p....
 ae94 be65 2d55 7270 3d3b 975f c242 6f28  ...e-Urp=;._.Bo(
 7ed1 78e7 a21f 5ee1 bd07 3d84 c273 c8a6  ~.x...^...=..s..
 6892 8001 55a9 2fb1 fee7 7a13 f46d f58c  h...U./...z..m..
 2780 dc5c 3e86 a362 05ba a1ec 249e dc48  '..\>..b....$..H
 ddbd 1095 5108 7666 aaa4 dc29 7fa9 c3ba  ....Q.vf...)....
 6f23 d600 ee78 5aa6 f550 76dd e5b1 08c8  o#...xZ..Pv.....
 06da 8bf9 11f7 ff46                      .......F
BSSID:00:0f:66:2b:8a:cf DA:00:14:6c:6c:aa:77 SA:00:0f:66:2b:8a:cf Authentication (Shared Key)-4:
 b000 3a01 0014 6c6c aa77 000f 662b 8acf  ..:...ll.w..f+..
 000f 662b 8acf f038 0100 0400 0000 dd06  ..f+...8........
 0010 1802 0004                           ......
```

1. Client sends Probe Request with ESSID to the broadcast address

2. AP with matching ESSID responds indicating the AP's MAC address and other available options

3. Client acknowledges probe response

4. AP sends encrypted challenge text to client

5. Client deciphers challenge text and responds with the challenge text encrypted using the shared key

6. The AP verifies that the challenge text is correct and responds indicating that authentication was successful.

Attackers are interested in capturing packet number four and five; the challenge text exchange between the AP and client. Both of these packets are encrypted using the shared WEP key and therefore can be used to crack the WEP key.

Attack Details:

An attacker can use aireplay-ng to de-authenticate a host using the –-deauth option. This attack will send a spoofed de-authentication request as the AP to the client. To perform this attack he/she will need the target's MAC address, option –c below and the target AP BSSID, option –a below. Both of these can be gathered using Kismet.

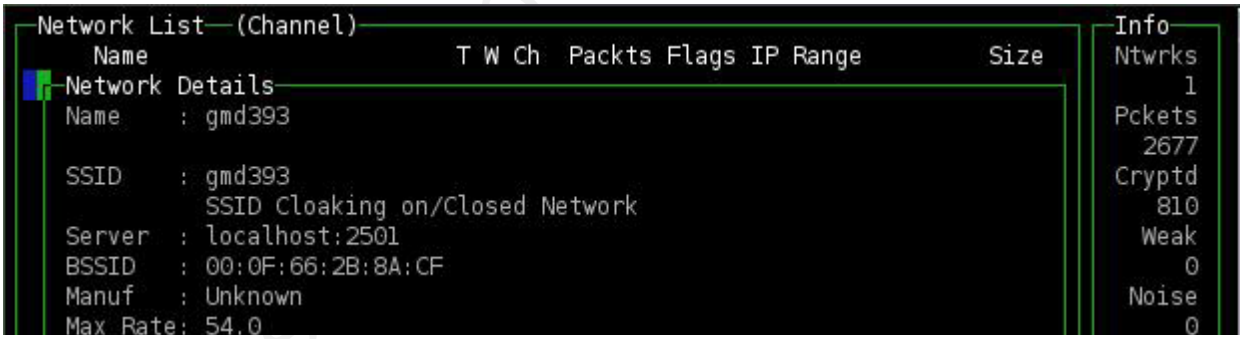

Figure 2: Kismet Network Details: Target AP BSSID

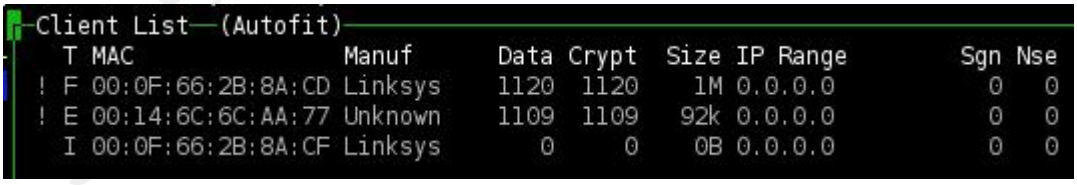

Figure 3: Kismet Client List

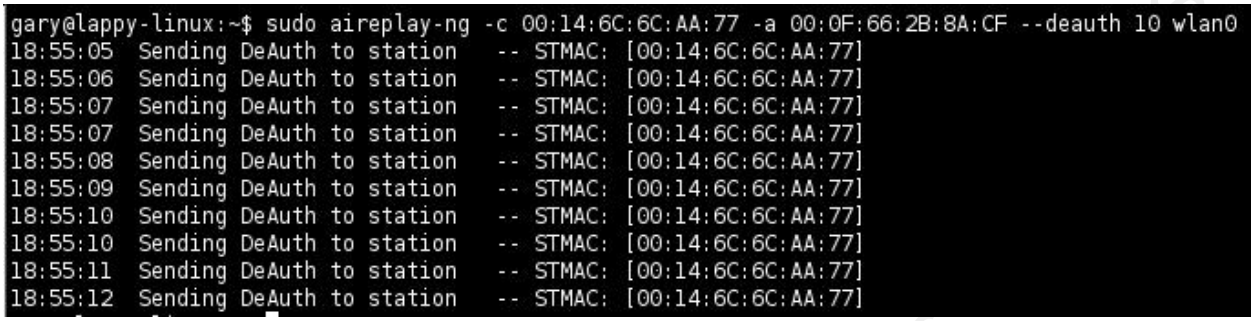

Figure 4: Deauthentication Attack using Aireplay-ng

De-authentication Detection:

De-authenticating a host is quite noisy because it causes the targeted client to disconnect from the access point and re-authenticate thousands of times. During this attack a client will lose network access and likely cause the user to go running to their IT Department. The one scenario where network disruption may go unnoticed is when a laptop is connected to the network on a wired port and the wireless card is still active.

This attack is easy to detect because large amounts of disassociation packets are not normal for a wireless network. A WIDS should raise the following alerts during this attack.

Alerts:

- De-Authentication Flood send to broadcast address
- De-Authentication Flood
- Repeated Authentication Attempts from one or several hosts

6.3.2 Injection Attack:

Another common attack used to generate WEP encrypted packets is to passively listen for an ARP packet, replay the ARP packet, and capture the access point's encrypted response. Packet injection is common because this attack does not create a denial of service condition for clients associated to the access point. This attack works well on slow or small wireless networks because only one associated host is needed to perform the attack and the host doesn't need to be very active.

Attack Details:

1. Aireplay-ng is used to sniff for broadcast ARP packets sent by associated clients.

2. In order to expedite an ARP request a disassociation attack may be used against the target host to prod it to create an ARP request while associate to the AP. Most operating systems will clear their ARP cache when they are disconnected, then once connected the host will need to rebuild the ARP table (Aircrack-ng Contributors, 2006).

3. Once captured, the ARP request is replayed from the attacking host onto the network thousands of times.

4. Each replayed packet generates a response from the AP with a new WEP encrypted packet.

5. Within 10-15 minutes an attacker will have plenty of packets to crack the key.

This attack works by replaying one wireless frame thousands of times. The replayed frames are indicated below by the duplicate data IV: bc7307. The replayed frames solicit a new encrypted response from the AP that uses a different IV.

```
BSSID:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 DA:ff:ff:ff:ff:ff:ff Data IV:bd7307 Pad 0 KeyID 0
DA:00:14:6c:6c:aa:77 BSSID:00:0f:66:2b:8a:cf SA:00:14:38:b1:b4:be Data IV:b143a6 Pad 0 KeyID 0
BSSID:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 DA:ff:ff:ff:ff:ff:ff Data IV:bd7307 Pad 0 KeyID 0
DA:00:14:6c:6c:aa:77 BSSID:00:0f:66:2b:8a:cf SA:00:14:38:b1:b4:be Data IV:b143a8 Pad 0 KeyID 0
BSSID:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 DA:ff:ff:ff:ff:ff:ff Data IV:bd7307 Pad 0 KeyID 0
DA:00:14:6c:6c:aa:77 BSSID:00:0f:66:2b:8a:cf SA:00:14:38:b1:b4:be Data IV:b143aa Pad 0 KeyID 0
BSSID:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 DA:ff:ff:ff:ff:ff:ff Data IV:bd7307 Pad 0 KeyID 0
DA:00:14:6c:6c:aa:77 BSSID:00:0f:66:2b:8a:cf SA:00:14:38:b1:b4:be Data IV:b143ac Pad 0 KeyID 0
BSSID:00:0f:66:2b:8a:cf SA:00:14:6c:6c:aa:77 DA:ff:ff:ff:ff:ff:ff Data IV:bd7307 Pad 0 KeyID 0
DA:00:14:6c:6c:aa:77 BSSID:00:0f:66:2b:8a:cf SA:00:14:38:b1:b4:be Data IV:b143ae Pad 0 KeyID 0
```

Figure 5: Duplicate Frames with Link Layer Displayed

Injection Detection:

A WIDS should alert when there are a large amount of duplicate frames seen on the network. A WIDS should raise the following alerts during this attack:

- Increase in Duplicate IVs
- Large amount of Duplicate Frames Received
- Short De-Authentication Flood

Injection Attack Speed Bump:

An access point could slow down this attack by applying a threshold to the amount of responses sent to duplicate frames.

A WIDS can detect active WEP cracking, but the source will be spoofed as an associated host and there are no wires to trace

back to the culprit. Remember to think of the wireless network as a large hub, there will not even be MAC address collisions.

7. Man-in-the-Middle Attacks (MIM)

Attackers use man-in-the-middle attacks on wired networks to intercept or sniff traffic. However, wireless networks function like a large hub and an attacker only needs to listen in order to collect network traffic. So what purpose do MIM attacks server on a wireless network? Attackers will use these attacks on wireless networks to proxy ssl connections and webpage logins, conduct phishing attacks or other attacks that involve modifying the packet stream.

An attacker can successfully implement a man-in-the-middle attack by first, configuring a rogue access point to imitate a legitimate AP. Then coerce wireless clients to connect to the rogue AP by performing a denial of service attack against the legitimate AP or by providing a stronger signal than the targeted AP. Wireless clients will normally associate to the AP with the strongest signal or lowest signal to noise ratio(SNR). To make the intercepted connection appear seamless to victims, the rogue AP could then bridge connections to another network connection. If successfully executed an attacker will have complete control of the wireless client's network connection and may perform any inline attack they wish (Vladimirov et al., 2004).

7.1 Scary Things Malicious Person could do with MIM:

1. Forge Wireless Authentication Webpage to collect IDs and passwords.

2. Proxy web logins and gather websites, usernames and passwords used.

3. Attempt to compromise associated hosts by injecting exploit code into the network stream.

7.2 How Wireless Man-in-the-Middle Attacks are Performed:

1. Target AP and associated clients are located
    a. If WEP is used, then crack the key.
2. Configure wireless card as rogue AP
    a. Mode: Master
    b. WEP: <cracked key>
    c. ESSID: <target ESSID>
    d. Channel: at least 5 channels away from target AP
3. Create noise on the target AP channel using Void11 http://www.wirelessdefence.org/Contents/Void11Main.htm and Fake AP http://www.blackalchemy.to/project/fakeap/. Void11 can be used to flood an AP with authentication or association packets. Fake AP can be used to flood a channel with thousands of fake ESSIDs.
4. Use Aireplay-ng to send de-authentication packets to the target host. The targeted host will disconnect from the legitimate AP.

5. The disconnected client will rescan wireless channels and associate with the malicious AP.

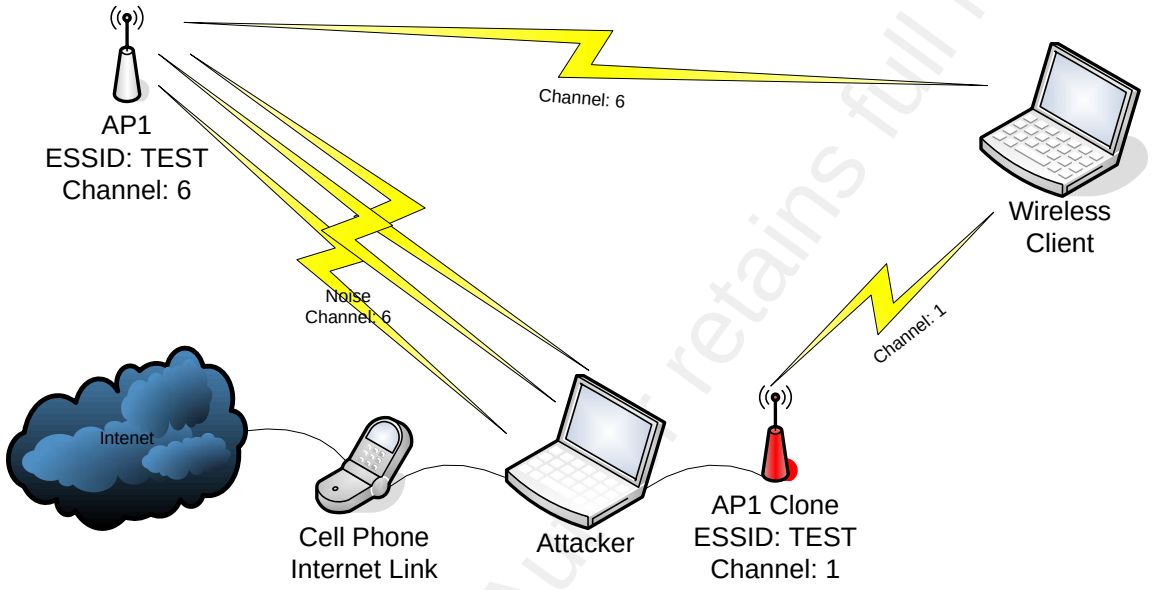

Figure 6:Man-in-the-Middle Attack

7.3 Detecting MIM Attacks

In order for an attacker to be successful, the MIM AP has to be at least 5 channels away from the target AP's channel to avoid interference from the denial of service attack (Vladimirov et al., 2004). Therefore, detecting the ESSID on an undocumented channel should raise an alert. This type of detection should be sufficient for a wireless network with only one AP, but will not suffice for a large wireless network. Large networks contain multiple access points configured on different channels to avoid RF interference with neighboring access points.

7.3.1 Static List Detection of MIM

The IDS can compare detected access points against a list of authorized ESSID, BSSID and channel combinations. The IDS can alert if an AP is detected that does not match any combination on the authorized list. It is important for the authorized list to have BSSIDs paired with the channel it uses. The current rogue AP preprocessor for snort-wireless uses separate lists of BSSIDs and channels. The IDS will not be able to determine when a BSSID is used on an unauthorized channel. This is very important because man-in-the-middle attacks normally utilize a BSSID on a channel that is at least 5 channels from the legitimate AP.

BSSID != Authorized BSSID => Alert Unauthorized BSSID

BSSID & !Authorized Channel => Alert BSSID on Unauthorized Channel

This type of detection is rather rudimentary and could be fooled by a careful attacker who accurately clones an access point with the same BSSID and channel combination.

7.3.2 Knowledge Based Detection of MIM

If an attacker configures their rogue access point to use a valid AP's BSSID and channel the static list detection mechanism described above will fail. However, MIM attacks can be detected by utilizing the signal strength of the detected APs. An attacker will not be able to place the cloned rogue AP exactly where the targeted AP is located, because the RF interference would disrupt the attack. The BSSID and channel are now in use

in two locations, so the signal strength detected by IDS sensors will change. Increasing the amount of IDS sensors should increase the reliability of this detection, by creating more points to monitor signal strength.

The following table illustrates how the database should store BSSID/Channel combinations with the signal strength per IDS sensor.

IDS Sensor	ESSID	BSSID	Channel	Signal Strength
0	Test	11:11:11:11:11:11	1	60
0	Test	22:22:22:22:22:22	6	70
1	Test	11:11:11:11:11:11	1	40
1	Test	22:22:22:22:22:22	6	50

The IDS should alert on increases in signal strength or if an IDS sensor detects a new BSSID/channel combination.

Note: The IDS will not be able to detect MIM attacks that work at a lower signal strength than that of the legitimate AP.

7.3.3 Radio Triangulation Detection:

If the IDS could triangulate radio signals, then any change in the triangulated location of an AP should raise an alert. Radio triangulation could also provide location based wireless network authentication (Morrison, 2002).

8. Case Study: WIDS using Linksys WRT54G Wireless Router

A basic WIDS can be deployed using a Linksys WRT54G wireless router running OpenWRT linux-based firmware and a Linux server. Kismet-Drone can be used on the WRT54G router to stream wireless data collected by the router to a stationary Kismet

server. The stationary Kismet server then correlates traffic received from different Kismet-Drones and analyzes the traffic for attack patterns. Snort-Wireless is integrated with Kismet using a FIFO data pipe from Kismet. Snort-Wireless is used to compliment Kismet and perform further analysis of the wireless network.

For information on installing and configuring Kismet-Drone on a WRT54G router please visit http://www.personalwireless.org/tools/wrt54g/.

The diagram below outlines the IDS configuration and the connections that are made between the components.

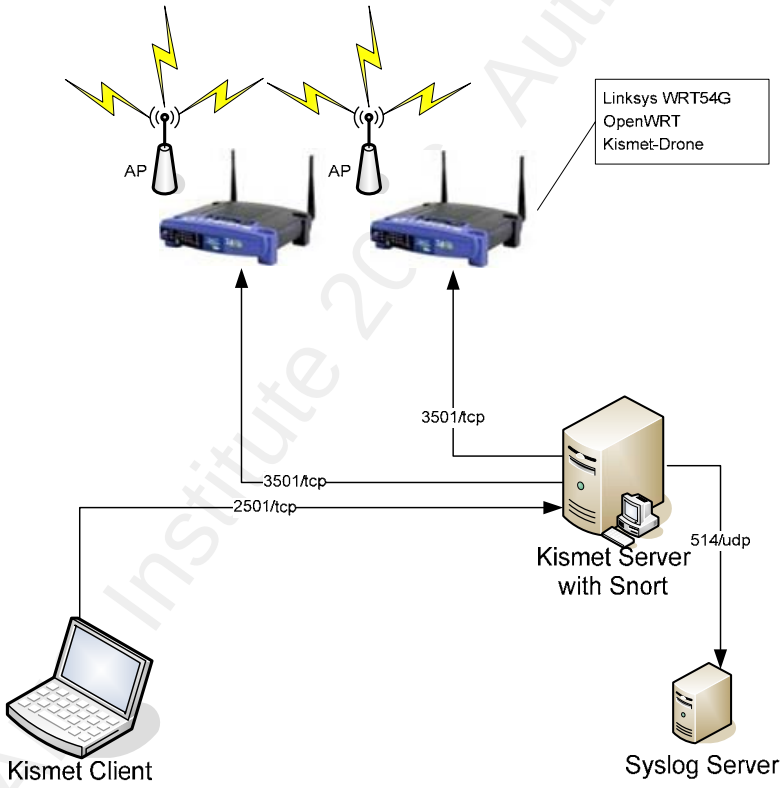

Figure 7: WRT54G Kismet-Drone Infrastructure

The Linux server requires a network connection that is capable of connecting to the IDS sensors. The wireless routers

are running Kismet-Drone which listens on port 3501/tcp for the Kismet-server. Once the Kismet-server connects to a drone the drone will start streaming 802.11 frames back to the server. The Kismet-server combines the frames into one stream for analysis and provides Snort-Wireless with a FIFO data pipe. Snort-Wireless reads the FIFO pipe as a file using Snort's –r option.

8.1 Detection Capabilities

The WIDS did detect rogue APs and MAC address spoofing. The system would also provide data indicating denial of service and WEP key cracking attacks.

Kismet provides excellent information about detected access points, including the ESSID, BSSID, channel and packet statistics. This information can be logged into a CSV or flat text file.

Snort-Wireless can detect MAC address spoofing using sequence number analysis. A common security mechanism for wireless networks is to utilize a white list of authorized MAC addresses. Attackers can set their client to use a white listed MAC address and connect to the network. Sequence number detection will detect jumps in sequence numbers when a MAC address is in used by two different hosts (Wright, 2003).

Kismet and Snort-wireless will both alert on de-authentication and disassociation floods. These attacks could indicate a denial of service, WEP key cracking, or MIM attack.

Kismet could detect WEP key cracking, but currently Kismet does not contain an IDS rule to alert on increases in duplicate

packets. A signature should be added to the current Kismet rule set that will alert on a trend increase in duplicate packets.

8.2 Strengths

Rogue AP detection

Ability to Deploy Multiple Sensors

Centralized Packet Collection:

Kismet combines all network traffic into one pcap file

Kismet and Snort-Wireless are ran on the same host

8.3 Areas for Improvement

This WIDS performed rather poorly as a wireless intrusion detection system. It could detect rogue APs, WEP key cracking, some MIM attacks and MAC address spoofing, but alerting on these attacks is very difficult.

The logging and detection capability of the WIDS is limited. Kismet does not write its IDS alerts to a log file, but rather displays these alerts in a rolling log within the Kismet-client. This effectively negates Kismet’s IDS functionality because it is not possible to monitor these alerts, without an individual sitting at the Kismet client, reading the stream of alerts. The lack of logging also prevents the possibility of correlating Kismet alerts with other logs, like Snort-Wireless.

Snort-Wireless will alert on a BSSID and channel combination that is not on the authorized BSSID or Channel list. However, this detection is flawed because it utilizes separate

lists for authorized BSSIDs and channels. Below is an example of how these lists are declared in the snort.conf file.

```
# Authorized AP BSSIDs
var ACCESS_POINTS [XX:XX:XX:XX:XX:XX, YY:YY:YY:YY:YY:YY,…]
# Authorized Channels
var CHANNELS [X, Y, ...]
```

The authorized list should pair BSSID with the channel it is used on. For instance,

```
var AUTHORIZED_APS [<BSSID>,<Channel>,…]
```

The rogue AP preprocessor should then be modified to check BSSID, Channel combinations against this list and alert when a BSSID is not on its authorized channel or when an AP does not match any on the list. Currently, alerts generated by this preprocessor only display the BSSID of the unauthorized AP. This alert should include the BSSID, Channel and ESSID of the detected AP. For instance, a rogue AP with the ESSID of "linksys" is likely just an unauthorized AP that needs to be removed, but if the ESSID of your network is in use by an unauthorized BSSID and channel combination then there could be a potential MIM attack occurring.

For MIM attacks, the WRT54G router driver does not support signal strength statistics for Kismet. Signal strength statistics are vital to MIM detection and could allow the IDS to provide location information about access points and clients. The IDS should keep track of signal strengths per IDS sensor. This would allow for the MIM attack detection outlined previously in this paper.

9. Future Research (Commercial Wireless IDS)

The following commercial wireless IDS systems claim to have wireless IDS or even IPS functionality. Further research is needed to determine the effectiveness of these technologies against wireless attacks like MIM and Rouge APs.

- Aruba Networks, Wireless Intrusion Protection Module and Aruba Access Points.
    - http://www.arubanetworks.com/products/arubaos/wip/
- AdventNet, RF Sensors and Management Console, deployed similar to case study IDS.
    - http://manageengine.adventnet.com/products/wifi-manager/intrusion-protection-system.html
- AirDefense Enterprise
    - http://www.airdefense.net/products/enterprise.php

10. References

Aircrack-ng Contributors, (2006,09 05). Aircrack-ng Newbie Guide. Retrieved October 30, 2006, from Aircrack-ng Web site: http://www.aircrack-ng.org/doku.php?id=newbie_guide

Cheung, Humphrey (2005, May 18). How to crack WEP - part 2: performing the crack. Retrieved October 26, 2006, from Tom's Networking Web site: (1) http://www.tomsnetworking.com/2005/05/18/how_to_crack_wep_/page3.html

Geier, Jim (2002, Aug 15). Understanding 802.11 Frame Types. Retrieved October 27, 2006, from Wi-Fi Planet Web site: http://www.wi-fiplanet.com/tutorials/article.php/1447501

IEEE, (2003, June). Part 11: Wireless LAN Medium Access. *ANSI/ IEEE Std 802.11, 1999 Edition (R2003)*, Retrieved 09, 2006, from http://standards.ieee.org/getieee802/download/802.11-1999.pdf

Morrison, J. D. (2002, 09). IEEE 802.11 WIRELESS LOCAL AREA NETWORK. Retrieved 10,2006, from http://cisr.nps.edu/downloads/theses/02thesis_morrison.pdf

Vladimirov, A, Gavrilenko, K, & Mikhailovsky, A (2004). *WI-FOO The secrets of wireless hacking*. Boston: Addison-Wesley.

Wright, J (2003, 01 21). Detecting Wireless LAN MAC Address Spoofing. Retrieved 10,2006, from http://www.rootsecure.net/content/downloads/pdf/wlan_macspooof_detection.pdf

Monitor mode. (2006, June 9). In *Wikipedia, The Free Encyclopedia*. Retrieved October 28, 2006, from http://en.wikipedia.org/w/index.php?title=Monitor_mode&oldid=57740803

Wired Equivalent Privacy. (2006, October 01). In *Wikipedia, The Free Encyclopedia*. Retrieved October 01, 2006, from http://en.wikipedia.org/w/index.php?title=Wired_Equivalent_Privacy&oldid=83952916