Brute force Attacks with WEPAttack against Static WEP Protected Access Points

Bob Davies

18 January 2005

Abstract

The use of Wireless networks has exploded within both residential and commercial networking. Some, if not most people understand the requirement to provide security for their wireless networks using Wired Equivalency Protection (WEP) to encrypt their data. Unfortunately, as with many other user chosen passwords, these people do not always chose appropriate passphrases to use as their WEP keys.

These weak passphrases are susceptible to both dictionary and brute force password guessing attacks using such tools as WEPAttack and John the Ripper. A compromised key an put anyone within range of your access points transmissions on your network as easily as if they had plugged an Ethernet card directly into your network.

Brute force Attacks with WepAttack against Static WEP Protected Access Points

Table of Contents

1 Statement of Purpose 2
2 The Exploit 2
2.1 Kismet 2
2.2 WEPAttack 2
2.3 John the Ripper 2
2.4 Operating System 2
2.4.1 Target 2
2.4.2 Attacker 2
2.5 Protocols/Services/Applications 2
2.5.1 802.11 2
2.5.2 802.11b 2
2.5.3 802.11a 2
2.5.4 802.11g 2
2.5.5 802.11i (also known as WPA2) 2
2.5.6 Wireless Authentication 1
2.6 Description 2
2.7 Signatures of Attack 2
3 Stages of the Attack Process 2
3.1 Reconnaissance 2
3.2 Scanning 4
3.3 Exploiting the System 6
3.3.1 WEPAttack 6
3.3.2 John the Ripper 8
3.3.3 Cracking the Key 9
3.4 Network Diagram 10
3.5 Keeping Access 12
3.6 Covering Tracks 12
4 Incident Handling Process 13
4.1 Preparation 13
4.1.1 Configuring WEP on Access Point and Wireless card. 13
4.2 Identification 14
4.2.1 Audit logs on access point 14
4.2.2 Audit logs on other systems connected to the same network 15
4.2.3 Law Enforcement Investigation of your Networks 15
4.3 Containment 15
4.3.1 Change WEP Key 15
4.3.2 Place firewall between access point and rest of network 16
4.3.3 Disable Access Point 16
4.4 Eradication/Recovery 16
4.4.1 Change the Access Point Administrative Password 16
4.4.2 Validate Firmware Version of the Access Point 16
4.4.3 Validate Access Point Configuration 16

4.4.4 Examine other systems on the network for root kits, etc. 17
4.5 Lessons Learned 17
4.5.1 Change WEP Key regularly 17
4.5.2 Strategic Placement of access point 17
4.5.3 Use of Open System WEP authentication. 19
4.5.4 Use a more complex WEP key 19
4.5.5 Use of Secondary Authentication 19
4.5.6 Use of WPA/802.11i 19
5 Conclusions 19

1

2 Statement of Purpose

The use of 802.11 wireless networks has exploded in both the business and residential sector almost at the speed of the wireless waves themselves. In businesses, wireless networks provide flexibility, allowing staff to move from their office to the boardroom without tethers. In homes, it allows families to have multiple computers throughout the house without the cost of hardwired network infrastructure.

However, the flexibility that wireless networking provides comes at a cost. The radio waves that allow you to stay connected on the patio or in the boardroom, radiate in all directions, and can be received by neighbours looking for some free Internet access, or by malicious individuals attempting to gain access to sensitive information on the network.

One of the few things between your data or services and someone intending on taking advantage of your wireless network is your Wired Equivalency Protection (WEP) key. The WEP key is used as a key for encrypted data transferred over the wireless networks, and for authenticating wireless devices to the access point.

Some newer access points employ newer and more effective security mechanisms such as the 802.11i standard, WIFI Protected Access (WPA) and external wireless user authentication. However, it is not always possible to use these new mechanisms, for a variety of reasons.

The passphrase for the WEP key is like any other password. It provides only as much security as the choice of passphrase allows. An easily guessed or short passphrase, or one based on a dictionary word, is an invitation for an attacker to make use of the access point for whatever purpose he may want. This also applies to a good passphrase that is used for an extended period of time. With the increase in processor speed and the number of tools available to conduct brute force attacks on WEP keys, the passphrases must be changed on a regular basis.

3 The Exploit

Currently, there is no single exploit used to conduct a WEP key cracking attack. The attack discussed in this document is conducted using a set of tools comprised of Kismet, WEPAttack, and John the Ripper. Kismet detects and sniffs the access points, WEPAttack performs the cracking of the WEP key, and John the Ripper generates wordlists for use by WEPAttack.

3.1 Kismet

Wireless packets are captured using a wireless network sniffer such as Kismet. The data is stored in a PCAP format capture file. Kismet captures both 802.11

beacon or data packets. From this data, Kismet is able to identify the name and BSSID of the access point, whether WEP is enabled, and if the data is not encrypted, any IP addresses associate with the access point and it's clients. In order to conduct a key cracking session, a minimum of one encrypted data packet is required for any give access point. Other examples of tools that can perform this function include PrismStumbler[1]

3.2 WEPAttack

WEPAttack is a WLAN open source Linux tool for cracking 802.11 WEP keys. This tool is based on an active dictionary attack that tests millions of words to find the right key. WEPAttack encrypts dictionary words until it finds a match to the key from the captured data. In order to conduct a key cracking session, a minimum of one encrypted data packet is required for any give access point.[2]

3.3

3.4 John the Ripper

John the Ripper is an open source password cracking utility. It is designed for identifying weak passwords on Unix and Windows computer systems.

Like most security tools, Kismet, WEPAttack, and John the Ripper do not have a Common Vulnerabilities and Exposures (CVE) value from Mitre associated directly with them. However IT security organizations have often identified the use of weak passwords as a continuing security risk, and these advisories apply to user created WEP keys as well as to passwords used to access any system.[3]

3.5 Operating System

3.5.1 Target

Most commercial access points used by Small Office/Home Office (SOHO) or home users are appliances based on the Linux operating systems. These tend to be specialized embedded operating systems with the routing and firewall capabilities built in. There are many vendors providing such devices, including Linksys, SMC, Cisco and NetGear.

Some sophisticated users employ computers with wireless network cards running as access points. These computers, running either Windows or Linux operating systems, allow other wireless devices to connect to them and route traffic through them. An example of this could be a Windows XP system using Internet Connection Sharing (ICS).

Brute force Attacks with WepAttack against Static WEP Protected Access Points

Whether the target is a dedicated device or a computer sharing it's network access, if they employ WEP for security of the connection, they are potentially vulnerable to exploitation of weak WEP keys.

3.5.2 Attacker

All of the tools used in this attack are available for the Linux operating system. Only John the Ripper is currently available for Windows systems. Therefore, Linux is best suited as an attack system for WEP key cracking.

3.6 Protocols/Services/Applications

There are a number of sub-versions of the 802.11 protocol. These include 802.11b, 802.11a, 802.11g, and 802.11i. The following sections describe these subversions of the wireless 802.11 protocol

3.6.1 802.11

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard. They called it **802.11** after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum bandwidth of 2 Mbps - too slow for most applications.[4]

3.6.2 802.11b

IEEE expanded on the original 802.11 standard in July 1999, creating the 802.11b specification. 802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet.

802.11b uses the same radio signaling frequency - 2.4 GHz - as the original 802.11 standard. Being an unregulated frequency, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided. Vendors often prefer using unregulated frequencies to lower their production costs.

Pros of 802.11b - lowest cost; signal range is best and is not easily obstructed
Cons of 802.11b - slowest maximum speed; supports fewer simultaneous users; appliances may interfere on the unregulated frequency band

3.6.3 802.11a

When 802.11b was developed, IEEE created a second extension to the original 802.11 standard called **802.11a**. Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a fits predominately in the business market, whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated 5 GHz range. Compared to 802.11b, this higher frequency limits the range of 802.11a. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions. Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid **802.11a/b** network gear, but these products simply implement the two standards side by side.

Pros of 802.11a - fastest maximum speed; supports more simultaneous users; regulated frequencies prevent signal interference from other devices
Cons of 802.11a - highest cost; shorter range signal that is more easily obstructed

3.6.4 802.11g

In 2002 and 2003, WLAN products supporting a new standard called **802.11g** began to appear on the scene. 802.11g attempts to combine the best of both 802.11a and 802.11g. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 Ghz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

Pros of 802.11g - fastest maximum speed; supports more simultaneous users; signal range is best and is not easily obstructed
Cons of 802.11g - costs more than 802.11b; appliances may interfere on the un regulated signal frequency

3.6.5 802.11i (also known as WPA2)

802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on 24 June 2004, and supersedes the previous security WEP specification. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. It implemented a subset of 802.11i; the Wi-Fi Alliance also refers to the new standard as WPA2 which is their approved interoperable implementation of 802.11i. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use only the RC4 stream cipher. [5]

Pros of 802.11i – better security than previous 802.11 implementations using WEP.

Brute force Attacks with WepAttack against Static WEP Protected Access Points

Cons of 802.11i - costs more than 802.11b and g; not backwards compatible (although some vendors are backporting WPA into the drivers for some 802.11g devices.

3.6.6 Wireless Authentication

WEP supports two types of key management, Shared Key and Open Network authentication.

3.6.6.1 Open System

In Open System configuration, the sender and recipient do NOT share a secret key. Each party generates its own key-pair and asks the receiver to accept the (usually randomly) generated key. Once accepted, this key is used for a short time only, then a new key is generated and agreed upon. Even if the secret key is discovered, only a small amount of data may be decrypted.

3.6.6.2 Shared Key:

This is when both the sender and recipient share a secret key. Both units use this key for an extended length of time, sometimes indefinitely. Any eavesdropper that discovers the key may decipher all packets until the key is changed.

Step 1 - The client sends an authentication request to the access point requesting shared key authentication.
Step 2 - The access point uses the WEP algorithm to generate a random number used in the authentication response containing a challenge text.
Step 3 - The client uses its locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request.
Step 4 If the access point can decrypt the authentication request and retrieve the original challenge text, it responds with an authentication response that grants the client access.

Table 1 - WEP Shared Key Authentication Process

WEP is known to have vulnerabilities related to manner in which it generates keys and initialization vectors (IVs). “EP produces what's referred to as a "keyschedule" by concatenating a shared secret key with a randomly-generated 24-bit initialization vector (IV). WEP inputs the resulting keyschedule into a pseudo-random number generator that produces a keystream equal to the length of the 802.11 frame's payload. With a 24 bit IV, though, WEP eventually uses the same IV for different data packets. In fact, the reoccurrence of IVs with WEP can happen within an hour or so in busy networks. This results in the transmission of frames having encrypted frames that are similar enough for a hacker to collect frames based on the same IV and determine their shared values, leading to the decryption of the 802.11 frames.”

3.7 Description

The WEP key brute force cracking attack is independent of IV generation vulnerabilities, relating more to the choice of pass phrase used to generate the keys than generation algorithms. Due to laziness or ignorance, many people do not choose good passphrases for their WEP security. They often use words that are in the dictionary, or names of their children, dogs, or models of their cars. As a results, it’s often easier to attempt to crack the phrase using the brute force method.

This is where WEPAttack enters the picture. It implements the two most common methods of generating WEP keys, either by raw ASCII WEP keys, or using MD5 hashing of the phrase to generate a binary key. The phase phrases are drawn from a dictionary file.

The simplest brute force attack involves trying every possible binary key, a process that is completely impractical for 128 bit keys but may be worth trying for 64 bit keys if you have a few supercomputers lying around. WepLab and dwepcrack provide the ability; you provide the CPU cycles.

Because both of the above tools can use any dictionary in a text file or standard input, powerful password cracking utilities such as John the Ripper may be used to generate the word list. Combined with John's ability to apply rules (various capitalizations, appending numbers, etc.) to a basic dictionary, these tools result in a successful crack surprisingly often. Although both performed dictionary attacks successfully in my tests, WepLab executed faster while WEPAttack provided the convenience of multiple simultaneous attack modes.

If a dictionary attack fails, an optimized brute force attack based on the vendor's passphrase method may be fruitful. For devices that use null terminated ASCII keys, WepLab offers a brute force attack that only tries ASCII bytes, resulting in a somewhat smaller (though still generally too large) key space. For the more common MD5 hashed passphrases, dwepcrack can execute an optimized brute force attack for 64 bit keys. This method, devised and first implemented by Tim Newsham, dramatically reduces the potential key space from 2^40 to 2^21 possible keys, resulting in an extremely fast attack.[6]

3.8 Signatures of Attack

One of the difficulties in detecting a successful WEP cracking attack is that the process is completely passive. Unlike many other wireless sniffers which actively probe for networks, Kismet captures packets as they are transmitted by the access point without any active probing at all. As a result Kismet scans are undetectable in the logs of the access point. and then the dump file is taken to fast machine for cracking using WEPAttack. Until the attacker returns and uses the cracked WEP key, there is no evidence at all that anything has taken place.

Once the attacker attempts to use the cracked key to gain access to the secured network, detection will be dependent upon the amount of logging enabled at the access point and other systems. Most modern access points are able to log the Media Access Control (MAC) addresses of wireless devices connecting to them.

In addition, most access points include some firewall capabilities and are able to log network addresses and port numbers the clients connect to. If these accesses are outside the normal activity of the organization's wireless clients, this may indicate that an external attacker has gained access to the network through the access point

Log entries from other systems on the same subnet as the access point may provide indication of a successful WEP key cracking attack. Some entries which maybe found include failed login attempts, portscans, unauthorized service accesses and other types of attacks originating from IP addresses associated

4 Stages of the Attack Process

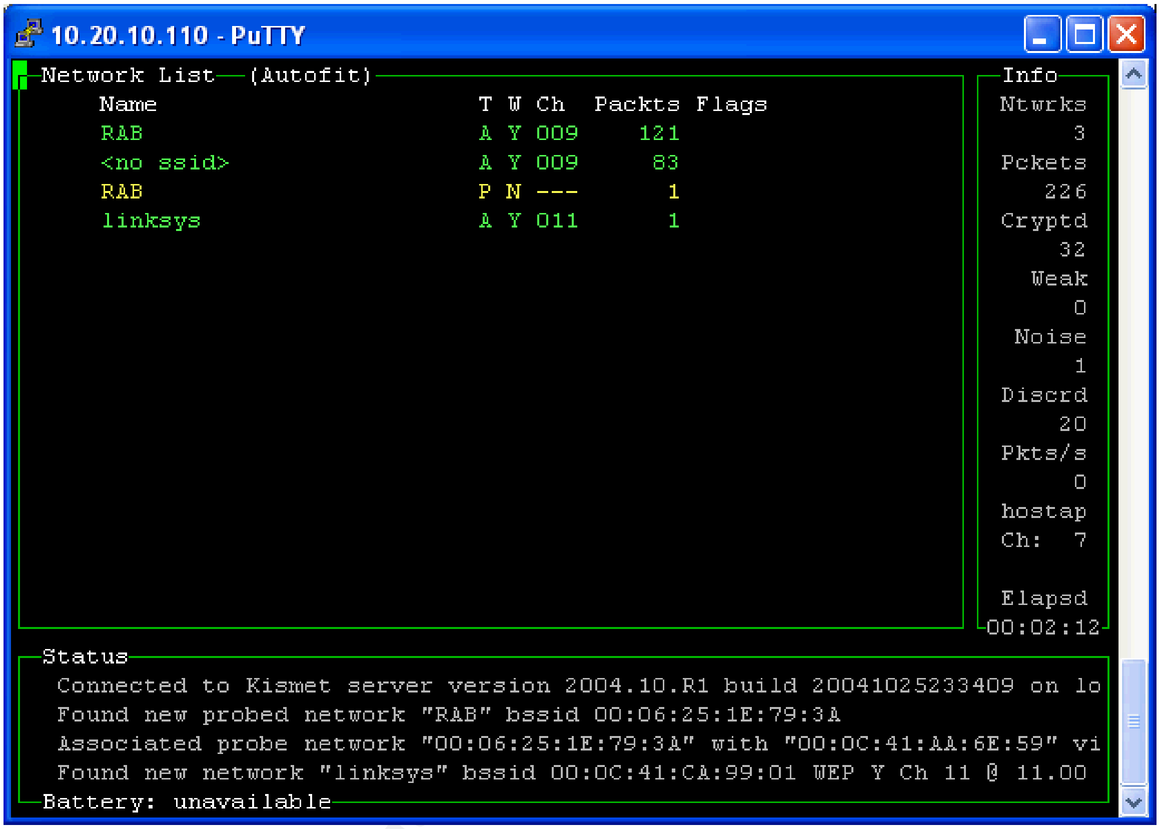
4.1 Reconnaissance

Reconnaissance for a WEP key cracking attack is conducted using a wireless scanning tool which supports Radio Frequency Monitoring (RFMon). Kismet is the best known of these tools. RFMon-based scanners are able to detect all 802.11 access points, including those which do not broadcast their ESSID's. A tool using active scanning could be used to perform some measure of reconnaissance, but will not detect access points not set to broadcast.

To allow different wireless networks to co-exist in the same physical area, access points use a range of radio frequencies mapped to channels. 802.11b and g are able to share a common frequency range if the 802.11g access point in operating with 802.11b compatibility. Otherwise it uses a separate frequency range. 802.11a is separate and cannot interoperate with 802.11b devices.

Each network would use a separate channel and all client devices desiring to connect to that network would be configured to use the channel specified by the access point.

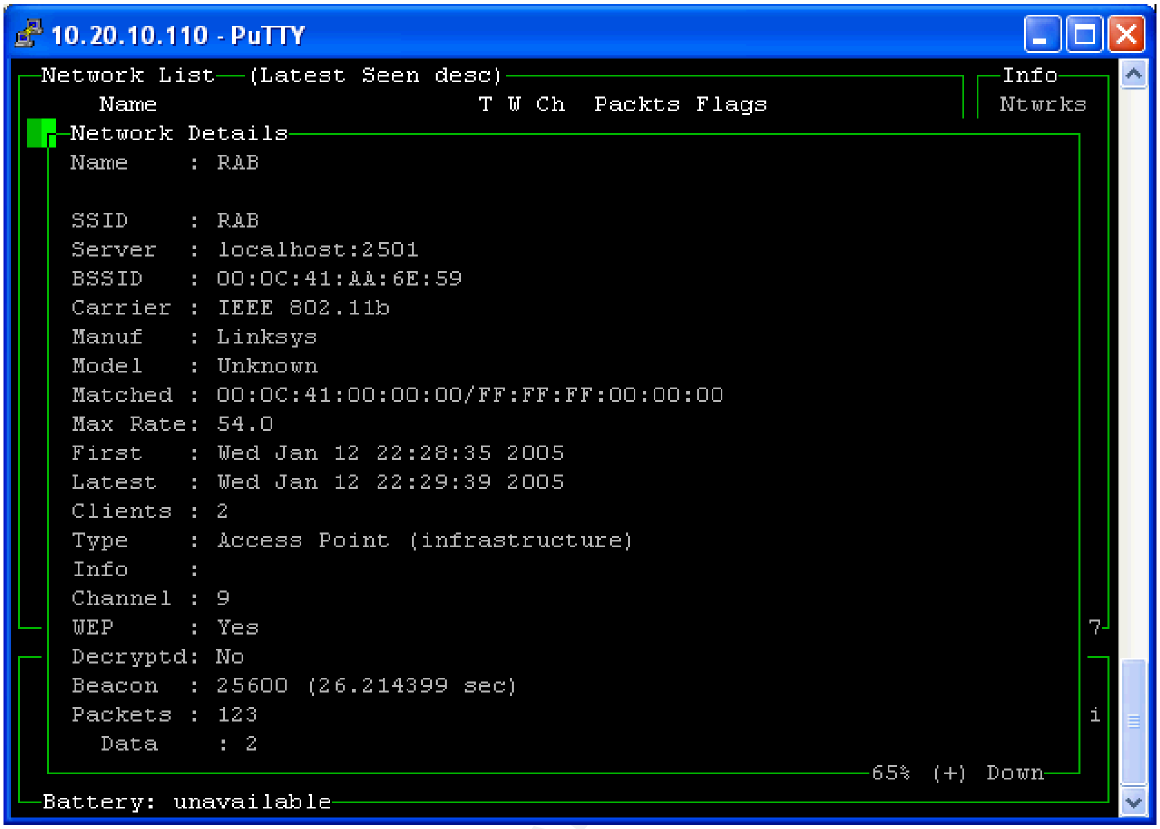
Kismet performs its scanning by hopping between the specified channels. If wireless packets are detected on the current channel, Kismet logs them and displays the configuration of the device in the user interface. Figure 1 below shows the Kismet display for a standard scan. Note that the ESSID or name of the network is displayed, as well as the type (access point or ad hoc station), whether WEP is enabled, the channel used by the access point, and the packet count. In the standard user interface configuration, WEP enabled access points are identified in green.



```
Network List—(Autofit)                                               Info
      Name                           T W Ch  Packts Flags          Ntwrks
      RAB                            A Y 009    121                     3
      <no ssid>                      A Y 009     83                Pckets
      RAB                            P N ---      1                   226
      linksys                        A Y 011      1                Cryptd
                                                                       32
                                                                     Weak
                                                                        0
                                                                    Noise
                                                                        1
                                                                   Discrd
                                                                       20
                                                                   Pkts/s
                                                                        0
                                                                   hostap
                                                                   Ch:   7

                                                                   Elapsd
                                                                 00:02:12
Status
  Connected to Kismet server version 2004.10.R1 build 20041025233409 on lo
  Found new probed network "RAB" bssid 00:06:25:1E:79:3A
  Associated probe network "00:06:25:1E:79:3A" with "00:0C:41:AA:6E:59" vi
  Found new network "linksys" bssid 00:0C:41:CA:99:01 WEP Y Ch 11 @ 11.00
Battery: unavailable
```

Figure 1 - access points detected using Kismet

Kismet can display additional collected configuration information for selected access points. Figure 2 below show specific details for the RAB access point.

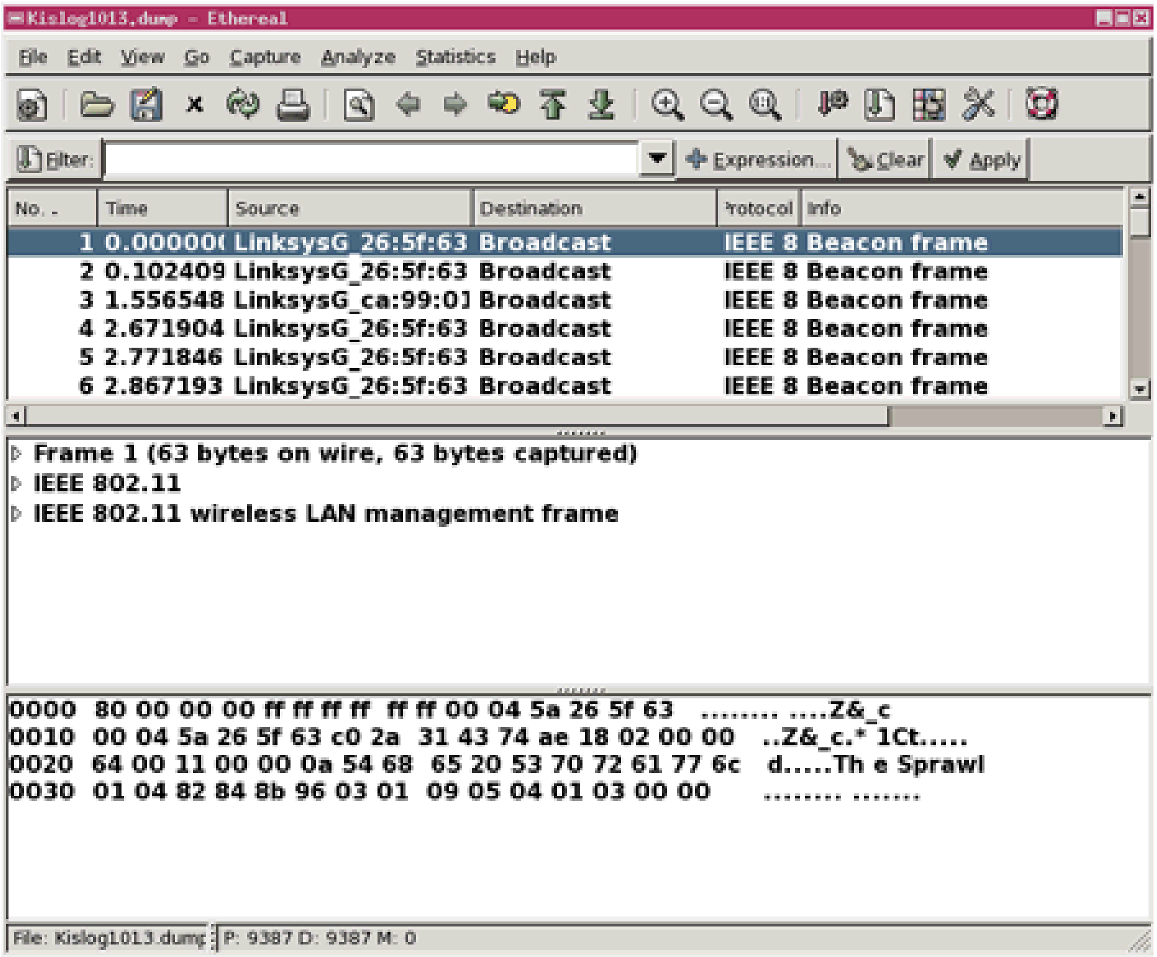


```
 Network List─(Latest Seen desc)                                Info
     Name                          T W Ch  Packts Flags          Ntwrks
   Network Details
   Name     : RAB

   SSID     : RAB
   Server   : localhost:2501
   BSSID    : 00:0C:41:AA:6E:59
   Carrier  : IEEE 802.11b
   Manuf    : Linksys
   Model    : Unknown
   Matched  : 00:0C:41:00:00:00/FF:FF:FF:00:00:00
   Max Rate: 54.0
   First    : Wed Jan 12 22:28:35 2005
   Latest   : Wed Jan 12 22:29:39 2005
   Clients  : 2
   Type     : Access Point (infrastructure)
   Info     :
   Channel  : 9
   WEP      : Yes                                                    7
   Decryptd: No
   Beacon   : 25600 (26.214399 sec)
   Packets  : 123                                                    i
     Data     : 2
                                                    65% (+) Down
 Battery: unavailable
```

Figure 2 - Access Point Details

4.2 Scanning

Once a WEP-enabled access point has been detected, the next step is to gather encrypted packets from it. This is done using the same tool used for detection. Kismet not only performs detection, but captures the beacon and data packets. The packets are stored in standard Packet Capture (PCap) format files. These files can be examined using any packet analyzer such as Ethereal (http://www.ethereal.com). Figure 3 below shows an Ethereal display of the packet contents. Note that Ethereal is able to identify the type of device, in this case a Linksys 802.11g access point.


Kislog1013.dump - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time      Source             Destination  Protocol Info
     1 0.000000( LinksysG_26:5f:63  Broadcast    IEEE 8  Beacon frame
     2 0.102409  LinksysG_26:5f:63  Broadcast    IEEE 8  Beacon frame
     3 1.556548  LinksysG_ca:99:0]  Broadcast    IEEE 8  Beacon frame
     4 2.671904  LinksysG_26:5f:63  Broadcast    IEEE 8  Beacon frame
     5 2.771846  LinksysG_26:5f:63  Broadcast    IEEE 8  Beacon frame
     6 2.867193  LinksysG_26:5f:63  Broadcast    IEEE 8  Beacon frame
```

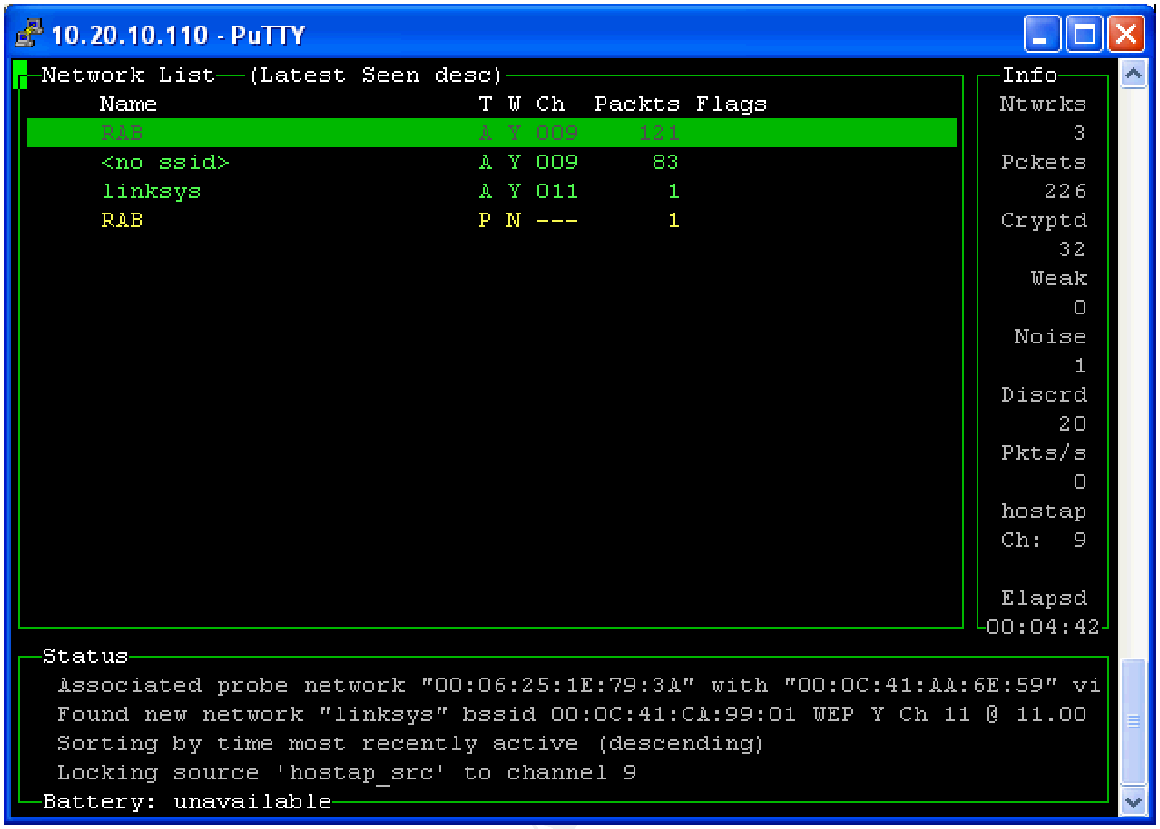
```
▷ Frame 1 (63 bytes on wire, 63 bytes captured)
▷ IEEE 802.11
▷ IEEE 802.11 wireless LAN management frame
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 00 04 5a 26 5f 63   ........ ....Z&_c
0010  00 04 5a 26 5f 63 c0 2a  31 43 74 ae 18 02 00 00   ..Z&_c.* 1Ct.....
0020  64 00 11 00 00 0a 54 68  65 20 53 70 72 61 77 6c   d.....Th e Sprawl
0030  01 04 82 84 8b 96 03 01  09 05 04 01 03 00 00      ........ .......
```

```
File: Kislog1013.dump  P: 9387 D: 9387 M: 0
```

Figure 3 - Ethereal Analysis of Wireless Capture

Kismet supports a “lock” function to temporarily suspend channel hopping. To capture packets from a particular access point, it should be highlighted in the user interface and the channel lock activated. From that point, all packets captured by Kismet will be limited to access points operating on that particular channel. It must be noted that if more than one device is using the same channel within range of the wireless sniffer, packets from all devices on that channel will be captured. If more granularity is desired, Kismet support filtering based on the device’s Basic Service Set Identifier (BSSID). Figure 4 below illustrates Kismet locked on channel 9. Note that in this case, both the RAB and the unidentified access point <no ssid> will be captured in this case.



```
Network List—(Latest Seen desc)                                 Info
     Name                       T W Ch  Packts Flags           Ntwrks
     RAB                        A Y 009    121                      3
     <no ssid>                  A Y 009     83                 Pckets
     linksys                    A Y 011      1                    226
     RAB                        P N ---      1                 Cryptd
                                                                   32
                                                                 Weak
                                                                    0
                                                                Noise
                                                                    1
                                                               Discrd
                                                                   20
                                                               Pkts/s
                                                                    0
                                                               hostap
                                                               Ch:  9

                                                               Elapsd
                                                             00:04:42
Status
 Associated probe network "00:06:25:1E:79:3A" with "00:0C:41:AA:6E:59" vi
 Found new network "linksys" bssid 00:0C:41:CA:99:01 WEP Y Ch 11 @ 11.00
 Sorting by time most recently active (descending)
 Locking source 'hostap_src' to channel 9
Battery: unavailable
```

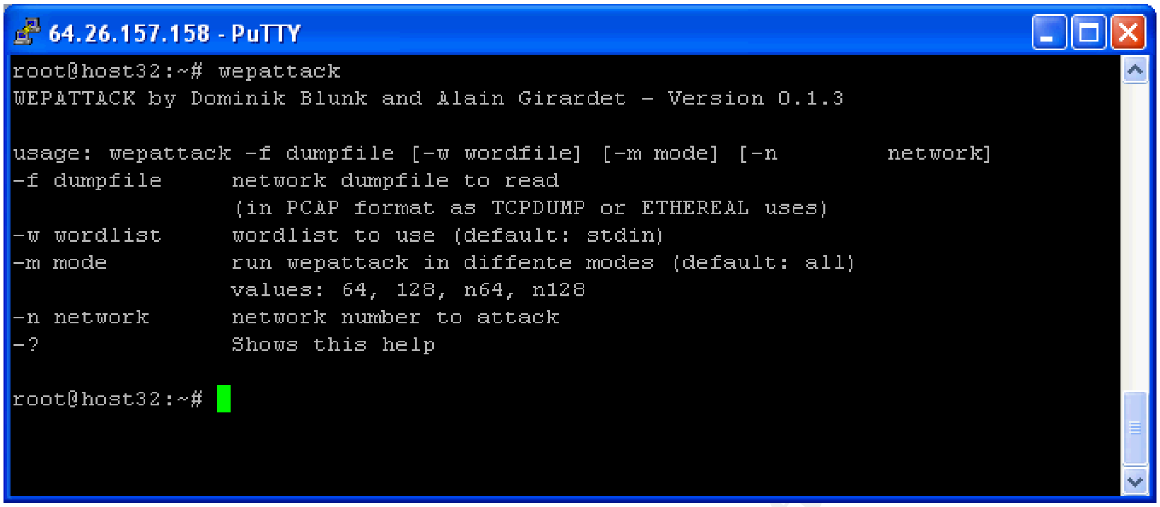
Figure 4 - Kismet Locked to Channel to Capture Data

4.3 Exploiting the System

Exploitation of the access point is performed in two steps. The first is to crack the WEP key using WEPAttack and John the Ripper. The second is to use the cracked key to gain access to the WEP secured network.

4.3.1 WEPAttack

WEPAttack uses a standard dictionary attack to attempt to create a match to the key used in the encrypted 802.11 packet. WEPAttack provides the following options:



```
root@host32:~# wepattack
WEPATTACK by Dominik Blunk and Alain Girardet - Version 0.1.3

usage: wepattack -f dumpfile [-w wordfile] [-m mode] [-n        network]
-f dumpfile      network dumpfile to read
                 (in PCAP format as TCPDUMP or ETHEREAL uses)
-w wordlist      wordlist to use (default: stdin)
-m mode          run wepattack in diffente modes (default: all)
                 values: 64, 128, n64, n128
-n network       network number to attack
-?               Shows this help

root@host32:~#
```

Figure 5 - WEPAttack Usage Information

-f <dumpfile> This option specifies the wireless packet capture containing the key that will be attempted to be cracked. The file must be in PCAP format, and must contain at least one encrypted data packet.

-w <wordlist> This option specifies the wordlist to be used for a dictionary attack. The expected format of the file is “words” separated by new lines (standard dictionary file format). The “words” can be any combination of alphanumeric and non-alphanumeric characters. If no word list is specified using this option, wepattack will accept the wordlist from standard input or STDIN. This is the way that John the Ripper is used in conjunction with wepattack.

-m <mode> Wepattack has four different modes, 64, 128, n64 and n128. The number 64 and 128 specify the key length to be used . Modes 64 and 128 use standard ascii translation of the dictionary word into a WEP key. No binary translation is performed in these modes. In modes n64 and n128, and standard MD5 hash is used to translate the word to a binary WEP key. If the –m option is not used, wepattack will attempt all modes for each applicable network in the capture file.

-n <network> If the scanning and capture was performed in an area with more than one encrypted network, wepattack will attempt to crack all WEP keys for which it has encrypted data packets. In these cases, it may be desirable to specify a single network to work with, to decrease the amount of time required to crack the key. To do this, it is necessary to run wepattack once against the capture file and note the network number associated with the BSSID of the desired network. Then the –n <network number> option is used to specify that network.

-? The question mark will display the help for WEPAttack.

Because WEPAttack can accept word lists through standard in (STDIN), it is able to be fed wordlists generated in an automated fashion. This is how it interacts with John the Ripper. It can also be used with a pre-existing wordlist using the -m option. From a speed perspective, this is preferable if it is suspected that the key might be contained in the dictionary.

One of the advantages of WEPAttack is the ability to select different modes, or to allow it to try all modes when checking whether a given word is valid as a WEP key. This provides considerable flexibility. As many people unwisely use a 64 bit WEP key, it may be advisable to run cracking attempts using the *64* and *n64* modes first. Knowing the type of access point can certainly assist in choosing the cracking mode. If it is known that the access point being tested employs the keygen method of generating binary keys, only the *n64* and *n128* modes should be used.

It is advisable to use the –n option to specify a single target access point where possible. By default, WEPAttack will attempt to crack keys for ALL networks in the capture file, thereby increasing the amount of time for the cracking session.

4.3.2 John the Ripper

John is primarily a password cracking utility designed to test the strength of user's passwords. It can be used to test both Unix and Windows passwords. One of John's strengths that makes it particularly useful in a WEPAttack based attack is its ability to generate lists of words either as variations on a word list, or by combinations of a specified character set.

John has the following four modes:

Wordlist Mode: This is the simplest mode John supports. John checks passwords against a wordlist file and optionally tries permutations of those words.
Single Crack Mode: In this mode, John gets account information on each user and uses pieces of it as passwords to try. For example, suppose the user account "leblanc" is owned by Patrick LeBlanc. John would try Patrick, LeBlanc, PaTrIcK, PaTRicK, and other permutations of information associated with leblanc to crack leblanc's password.
Incremental Mode: Also known as a brute force attack. Given a character set, John will try every combination of those characters up to 8 characters long.
External Mode: John's user can write pseudo-C functions that John uses to generate the words it tries. See the documentation for the details.

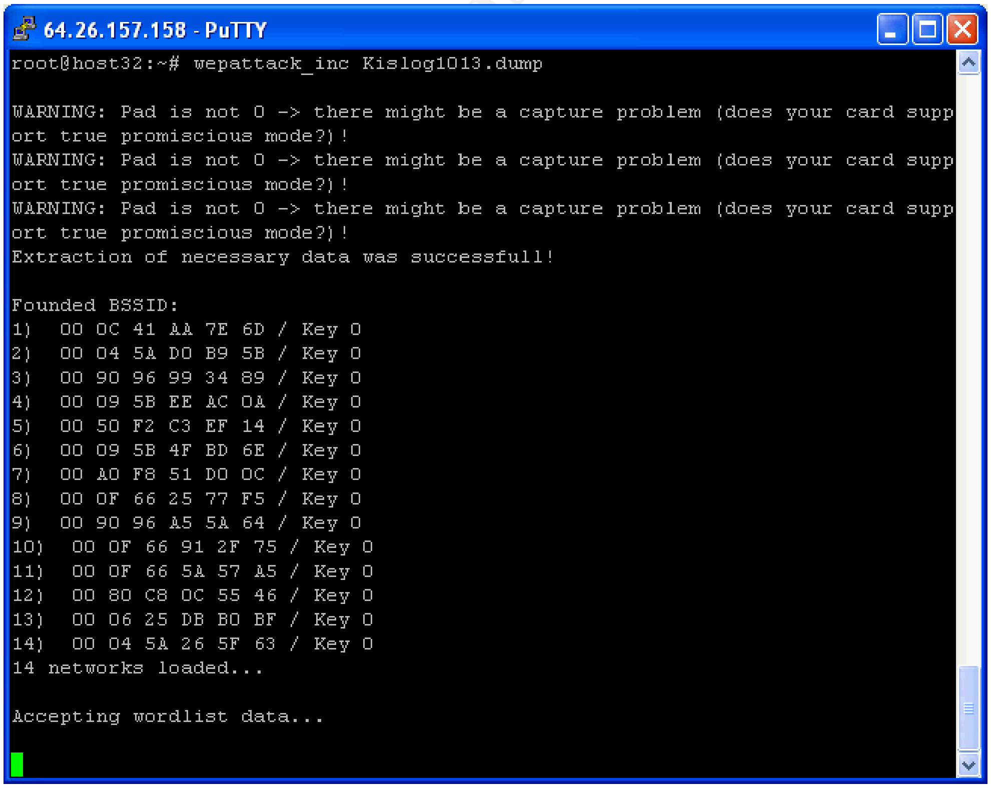
Currently, only Wordlist and Incremental modes are used in conjunction with WEPAttack. The WEPAttack package installed two shell scripts to assist in using John the Ripper to generate the keys. Wepattack_inc uses John in “Incremental mode” where it generates dictionary words based on rules regarding the allowable character sets, minimum and maximum password length. Wepattack_word uses John in “Wordlist mode” to manipulate a wordlist to create possible WEP passphrases.

WEPAttack comes with a 30MB wordlist for use in dictionary attacks. There are a wide variety of wordlists available on the internet. Some are specialized for particular target environments. OpenWall provides a very extensive wordlist (~450MB) which has already been manipulated by John the Ripper. This would be used with WEPAttack natively with the –w option.

4.3.3 Cracking the Key

To crack the WEP key for the target access point, a dictionary attack should be conducted first using either the –w option for WEPAttack, or using John the Ripper in wordlist mode using the wepattack_word script. If the dictionary attack is not successful, a brute force attack would then be conducted with John in incremental mode using the wepattack_inc script.

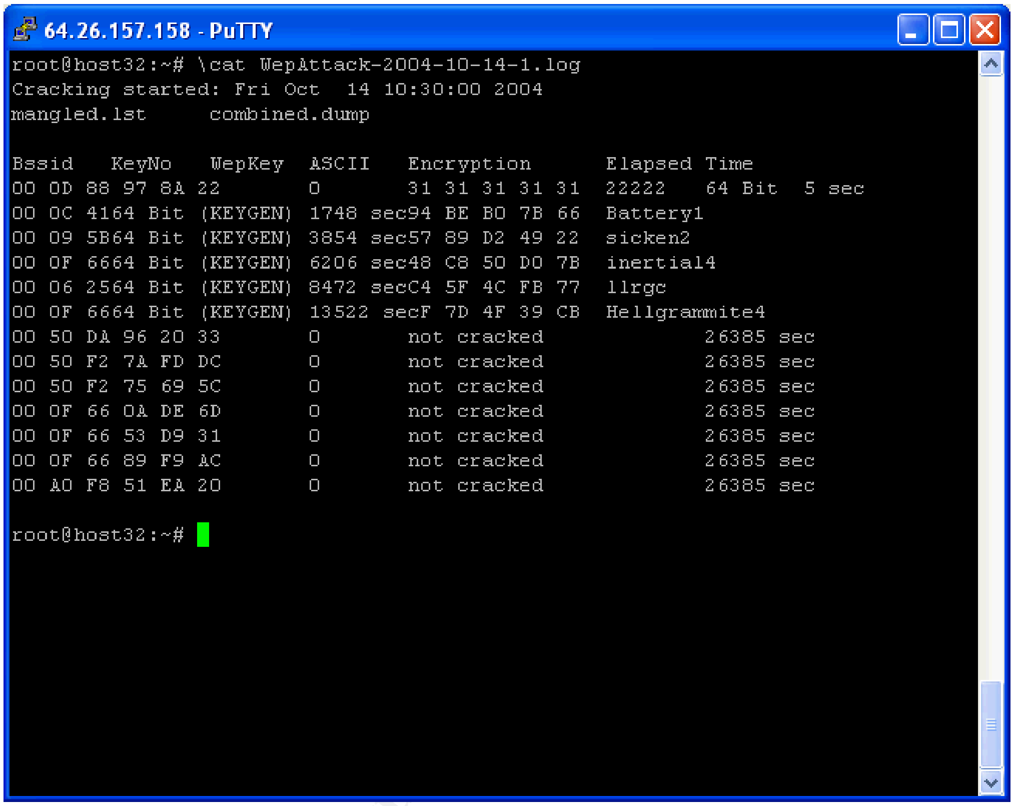
Figure 6 below illustrates WEPAttack being run in conjunction with John the Ripper operating in incremental mode. In the example, 14 networks were identified as having at least one encrypted data packet which could be used as part of a WEPAttack cracking session.



```
root@host32:~# wepattack_inc Kislog1013.dump

WARNING: Pad is not 0 -> there might be a capture problem (does your card supp
ort true promiscious mode?)!
WARNING: Pad is not 0 -> there might be a capture problem (does your card supp
ort true promiscious mode?)!
WARNING: Pad is not 0 -> there might be a capture problem (does your card supp
ort true promiscious mode?)!
Extraction of necessary data was successfull!

Founded BSSID:
1)   00 0C 41 AA 7E 6D / Key 0
2)   00 04 5A D0 B9 5B / Key 0
3)   00 90 96 99 34 89 / Key 0
4)   00 09 5B EE AC 0A / Key 0
5)   00 50 F2 C3 EF 14 / Key 0
6)   00 09 5B 4F BD 6E / Key 0
7)   00 A0 F8 51 D0 0C / Key 0
8)   00 0F 66 25 77 F5 / Key 0
9)   00 90 96 A5 5A 64 / Key 0
10)   00 0F 66 91 2F 75 / Key 0
11)   00 0F 66 5A 57 A5 / Key 0
12)   00 80 C8 0C 55 46 / Key 0
13)   00 06 25 DB B0 BF / Key 0
14)   00 04 5A 26 5F 63 / Key 0
14 networks loaded...

Accepting wordlist data...

```

Figure 6 - WEPAttack Cracking WEP Keys

Figure 7 below shows the output from a completed WEPAttack session. In this session, the keys of six out of 13 networks were successfully cracked. The first cracked network was employing a straight ASCII WEp key, where as the remaining five used the keygen or MD5 hash method for creating binary keys from the identified strings. All five used 64 bit WEP keys.



```
root@host32:~# \cat WepAttack-2004-10-14-1.log
Cracking started: Fri Oct  14 10:30:00 2004
mangled.lst     combined.dump

Bssid   KeyNo   WepKey  ASCII   Encryption      Elapsed Time
00 0D 88 97 8A 22       0       31 31 31 31 31  22222   64 Bit  5 sec
00 0C 4164 Bit (KEYGEN) 1748 sec94 BE B0 7B 66  Battery1
00 09 5B64 Bit (KEYGEN) 3854 sec57 89 D2 49 22  sicken2
00 0F 6664 Bit (KEYGEN) 6206 sec48 C8 50 D0 7B  inertial4
00 06 2564 Bit (KEYGEN) 8472 secC4 5F 4C FB 77  llrgc
00 0F 6664 Bit (KEYGEN) 13522 secF 7D 4F 39 CB  Hellgrammite4
00 50 DA 96 20 33       0       not cracked             26385 sec
00 50 F2 7A FD DC       0       not cracked             26385 sec
00 50 F2 75 69 5C       0       not cracked             26385 sec
00 0F 66 0A DE 6D       0       not cracked             26385 sec
00 0F 66 53 D9 31       0       not cracked             26385 sec
00 0F 66 89 F9 AC       0       not cracked             26385 sec
00 A0 F8 51 EA 20       0       not cracked             26385 sec

root@host32:~#
```

Figure 7 - WEPAttack Log File

4.4 Network Diagram

The following network diagrams illustrate common wireless network configurations to which an attacker may attempt to gain access. Examples are given for a basic home configuration and a more complex network using an access point positioned in a Demilitarized Zone (DMZ).

Figure 8 below shows a basic home wireless network using a wireless router such as a Linksys or Netgear. The home user gain access to the internet through the router, and uses the wireless access point to provide network access to their wireless-capable PDA and notebook computers.

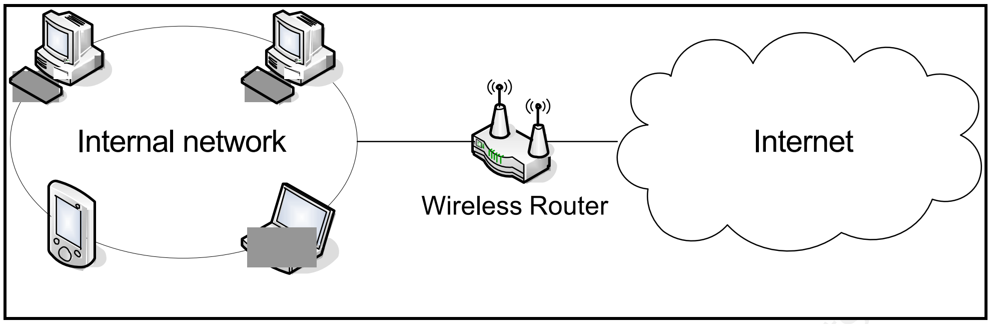


Figure 8 - Basic Home Wireless Network

Figure 9 below shows a more complex wireless network using a wireless access point placed in a DMZ. Wireless users may connect to the internet, or to the internal network, but are screened by the firewall.

In some cases, wireless users are considered as external to the network. They will be required to extranet solutions such as Virtual Private Network (VPN) connectivity to gain access to internal network resources. While this configuration places the internal network at less risk from a compromised WEP key, an attacker could still use this network to launch attacks against other systems on the Internet, or make use of the target network's bandwidth.

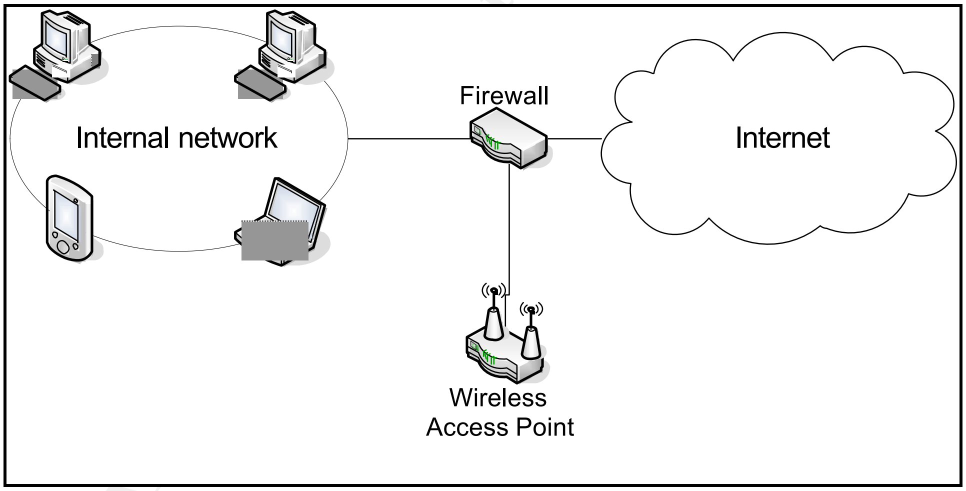


Figure 9 - DMZ Wireless Network

Figure 10 below illustrates the location of the wireless sniffer. Any Linux capable device could be used, including a notebook computer or PDA. Kismet sniffs the 802.11 beacon and data packets.

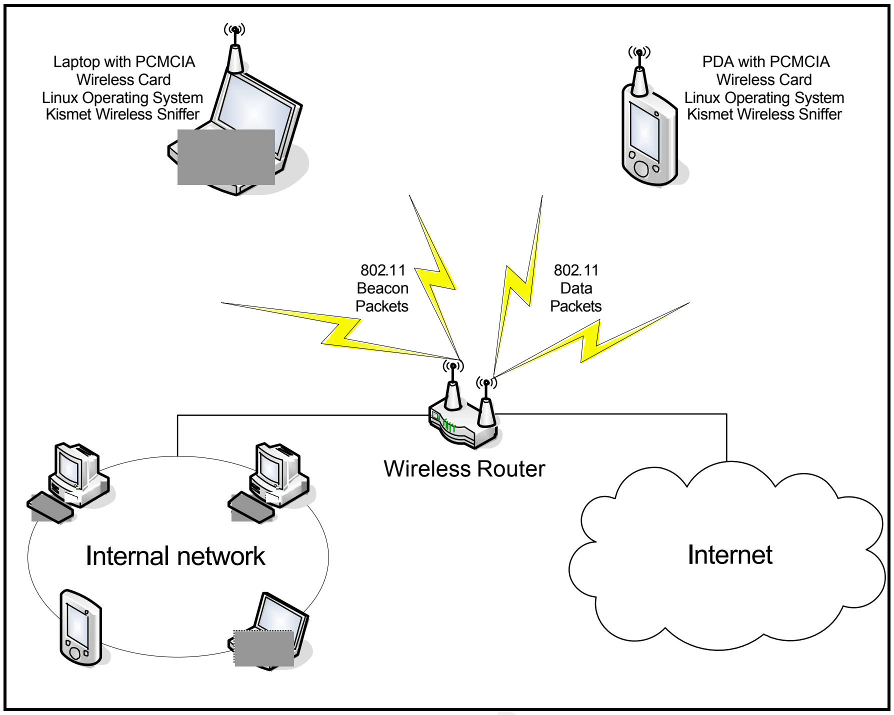


Figure 10 - WEP Key Sniffing Architecture

4.5 Keeping Access

Once access has been gained a number of options are available to the attacker. Using an network sniffer such as Ethereal, Ettercap, or DSniff, the attacker can sniff packets on the network and capture administration sessions on the access point. Once the attacker has captured the access point's administration userID and password, he can add his own MAC as an authorized address in the MAC filtering table, if this mechanism is used on the access point.

In addition to maintaining access to the access point, the attacker may launch attacks on other systems from his wireless system to gain access and control of those systems. Depending on the placement of the access point in the network architecture, the attacker could capture otherwise internal information and connections including login information for internal systems.

4.6 Covering Tracks

The primary method of detecting a rogue wireless device which is using a compromised key is through the active MAC logging mechanism in the access point. Any MAC addresses not associated with known network cards would be suspected as having unauthorized access.

There are a number of tools available to temporarily change the MAC address on network cards. Examples of these tools include ChangeMAC or randmac for Linux. Changemac allows the attacker to assign an arbitrary MAC address to his network card, while randmac sets a random MAC address.[7]

On Windows 2000 and XP, the MAC address can be changed using the network configuration tool or by making changing the following registry entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}[8]

Using Kismet, the attacker can determined over time legitimate MAC addresses which are in use with the target access point. Using one of the methods identified above, the attacker would then change the MAC address on his system to match one of the legitimate MAC addresses which is not in use at the time of the attack, and gains access under the guise of a legitimate user. This method also has the side effect of bypassing MAC address filtering, which is often used as an additional security mechanism.

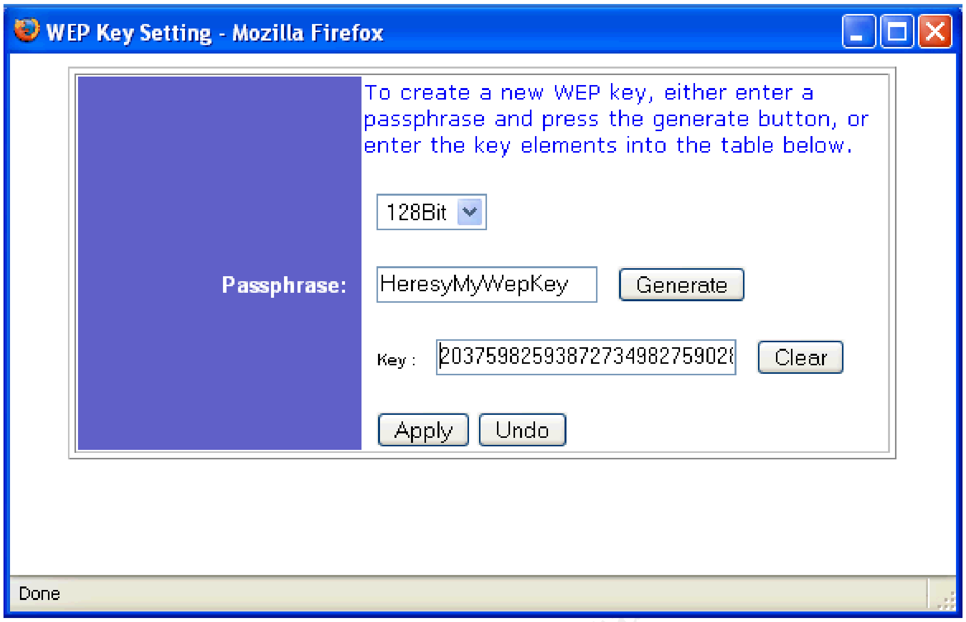
If the attacker gains administrative rights on the access point, he can also manipulate any audit logs on the access point to hide traces of his activity.

5 Incident Handling Process

5.1 Preparation

5.1.1 Configuring WEP on Access Point and Wireless card.

At a minimum, WEP should always be enabled on any access point not intended for public use. If other security mechanisms are available, they should be employed in place of, or in addition to WEP within the wireless network environment. The remainder of the section assumes that for whatever reason, WEP is being employed. Figure 11 below illustrates a sample configuration screen for enabling WEP on a Linksys access point. Note that in this case, 128 bit encryption is being used.



To create a new WEP key, either enter a passphrase and press the generate button, or enter the key elements into the table below.

128Bit

Passphrase: HeresyMyWepKey

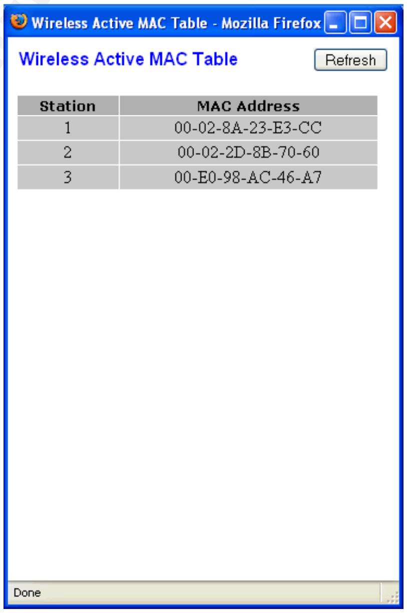
Key : 2037598259387273498275902

Figure 11 - WEP Key Configuration

5.2 *Identification*

5.2.1 Audit logs on access point

As indicated above, the active MAC table acts as an audit log for the MAC addresses of systems connecting to the access point. Regular review of this table is recommended to detect connections by unauthorized wireless devices. Figure 12 below shows a sample active MAC table from a Linksys wireless access point.

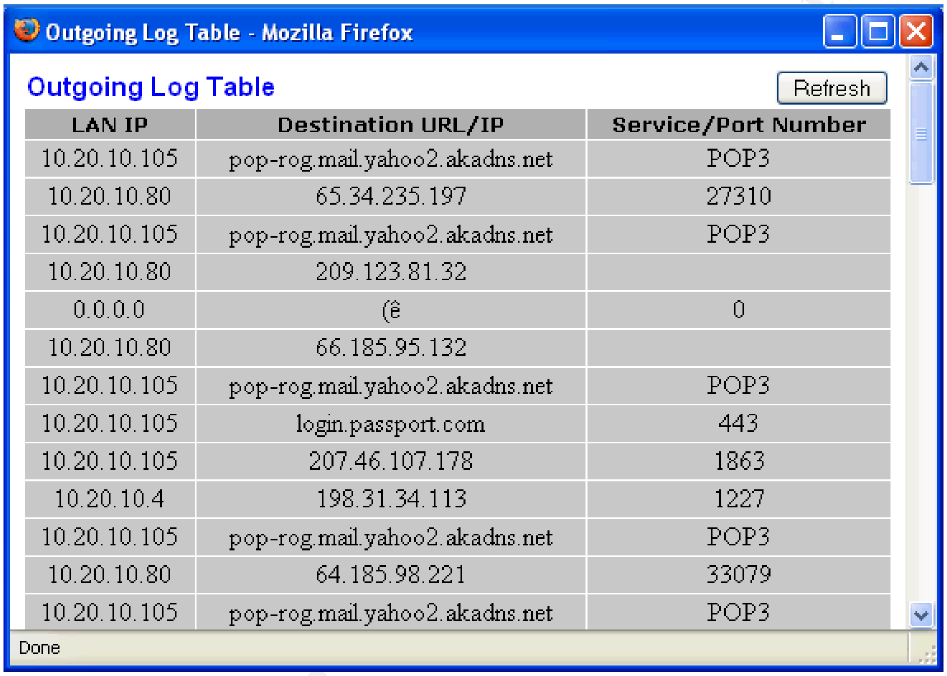


Wireless Active MAC Table

Station	MAC Address
1	00-02-8A-23-E3-CC
2	00-02-2D-8B-70-60
3	00-E0-98-AC-46-A7

Figure 12 - Access Point Active MAC Table

Most access points which include router and/or firewall capability provide logging of incoming and outgoing network connections. These logs can also provide an indication of a compromised WEP key. If the log indicates accesses to web pages or use of network protocols which are outside the normal use profile for the access point's normal user community, the source IP addresses of these connections should be investigated for possible compromise. Figure 13 shows a sample outgoing log table.



Outgoing Log Table

LAN IP	Destination URL/IP	Service/Port Number
10.20.10.105	pop-rog.mail.yahoo2.akadns.net	POP3
10.20.10.80	65.34.235.197	27310
10.20.10.105	pop-rog.mail.yahoo2.akadns.net	POP3
10.20.10.80	209.123.81.32	
0.0.0.0	(ê	0
10.20.10.80	66.185.95.132	
10.20.10.105	pop-rog.mail.yahoo2.akadns.net	POP3
10.20.10.105	login.passport.com	443
10.20.10.105	207.46.107.178	1863
10.20.10.4	198.31.34.113	1227
10.20.10.105	pop-rog.mail.yahoo2.akadns.net	POP3
10.20.10.80	64.185.98.221	33079
10.20.10.105	pop-rog.mail.yahoo2.akadns.net	POP3

Figure 13 - Access Point Outgoing Log Table

5.2.2 Audit logs on other systems connected to the same network

The audit or event logs of other systems on the same network as the access point may indicate a possible WEP key compromise as well. Such activities as port scans, a large number of failed logins or locked out accounts could indicate that an attacker has gained access to the network and is attempting to gain a foothold on other systems.

5.2.3 Law Enforcement Investigation of your Networks

If an attacker with unauthorized access to the access point is performing illegal actions such as trafficking in child pornography, or using it as a launching point for hacking attacks on other systems, the IP address to which these activities will be traced is that of the wireless router or default gateway for a stand-alone access point. As a result, any investigations of incidents related to a compromised access point could have serious consequences for the organization. If the attacker is masquerading as a legitimate user, it may be very difficult to clear the name of the individual without some other form of authentication to which the attacker would not have access.

5.3 Containment

5.3.1 Change WEP Key

If it is suspected that the WEP key for the access point has been compromised, one option is to change the key immediately. This will render the cracked key useless. However, it also impacts all legitimate users of the access point, who must be notified of the change and who must reconfigure their wireless devices with the new key. In a standard SOHO environment, this should be done immediately, as the number of devices to be reconfigured is small and all are usually under the control of the access point owner.

5.3.2 Place firewall between access point and rest of network

If wireless access cannot be disrupted for business reasons, an additional option is to introduce a firewall between the access point and the remainder of the network. This firewall would be configured to lockdown all outgoing connections. As individual users are validated, they would be given access through the firewall. This option provides the added benefit of being able to see the attacker’s attempted connections in the firewall logs, which might assist in identifying him.

5.3.3 Disable Access Point

If a WEP key compromise is suspected another alternative is to disable the access point’s wireless capability. For residential wireless routers, this is often the best option, as they all provide Ethernet connectivity as a backup. This direct wired connection can be used to conduct administration and analysis of the access point to attempt to determine the nature of the incident.

In a large environment where wireless connectivity makes up a larger percentage of their network connectivity, this may not be the preferred option.

5.4 Eradication/Recovery

Most of the activities of these two incident response phases are the same in this case. As a result, they will be discussed together.

5.4.1 Change the Access Point Administrative Password

The password for the access point should be changed immediately, as part of the eradication and recovery process. As stated above, it is highly likely that the attacker was able to capture the login for the access point and obtain administrative capabilities on the device.

5.4.2 Validate Firmware Version of the Access Point

Some older versions of access point firmware introduce vulnerabilities which an attacker might exploit. Validate the access point's currently installed firmware version is the one that is expected.

5.4.3 Validate Access Point Configuration

If an attacker gains administrative control of the access point, there a number of configuration items that could be altered to weaken the security of the access point, especially if it acts as a firewall to the Internet. These include but are not limited to:

- Firewall settings;
- Port forwarding;
- Anti-Virus configuration;
- Audit logging;
- Remote administration;
- IP filtering;
- Port Filtering;
- Remote upgrading;
- Static Routing; and
- DMZ host settings.

All of these setting should be validated as part of the eradication and recovery phases to ensure that the access point configuration is as expected.

5.4.4 Examine other systems on the network for root kits, etc.

Aside from validating the access point configuration, if a compromised WEP key for an internally connected access point is suspected, all internal systems should be examined for possible compromise. This includes the installation of backdoors, root kits, and rogue user accounts. In a large organization this could prove a daunting task, but if an attacker has gained access to the internal network through a wireless link, it is highly likely that he has used that foothold to attempt to gain access to other systems on the network.

5.5 Lessons Learned

5.5.1 Change WEP Key regularly

If it is necessary to use a static WEP key, it should be changed regularly. The frequency of the change should be based on a threat and risk assessment, but should not exceed monthly in a high-profile environment. Home users are less of a target, because they are usually attacked to gain access to their internet connection. In most cases, an attacker will merely pass by the WEP enable access point to one with less security enabled. That fact not withstanding, it is still good practice for home wireless users should changes their access point WEP keys on a regular basis as well.

5.5.2 Strategic Placement of access point

In order to reduce the visibility of a wireless access point, care must be take to locate it such that it provides adequate coverage for legitimate use, but does not provide strong radiation outside of the required area.

Figure 14 below illustrates the effect of strategic placement of the access point on an attacker's ability to sniff the wireless traffic. In example one, the access point is placed high in the building. While this gives excellent coverage to all users in the building, it also increases the coverage outside the desired area and make it easier for an attacker to first detect and then connect to the access point.

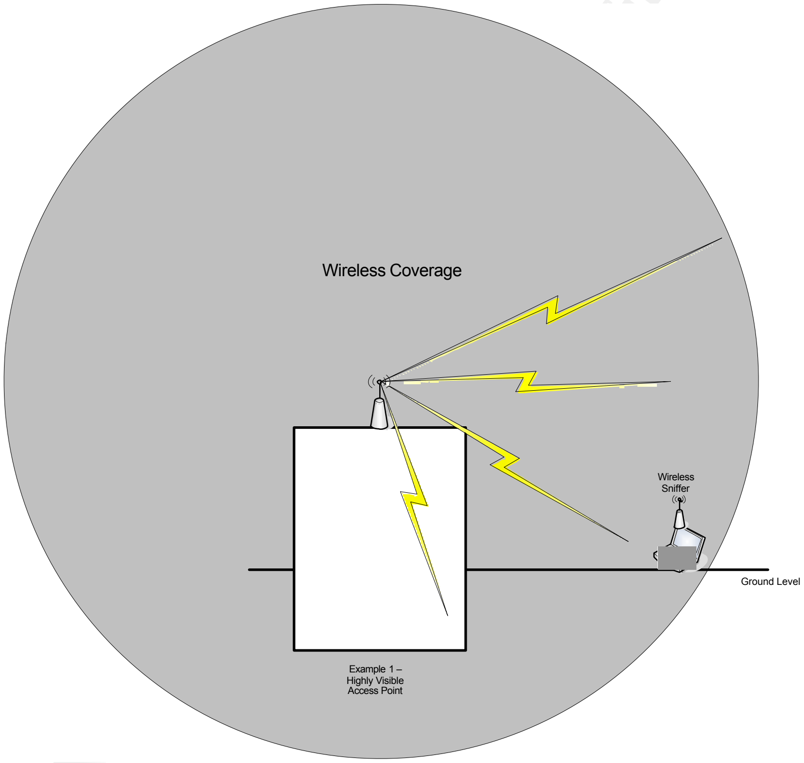


Figure 14 – Example 1: Non-Strategic Access Point Placement

In the example in Figure 15 below, the access point is placed below ground level. As a result, it's emanations provide coverage for the legitimate users in the building, but would be more difficult for an attacker to detect, due to the cone-shaped pattern from the ground absorbing some of the radio waves.

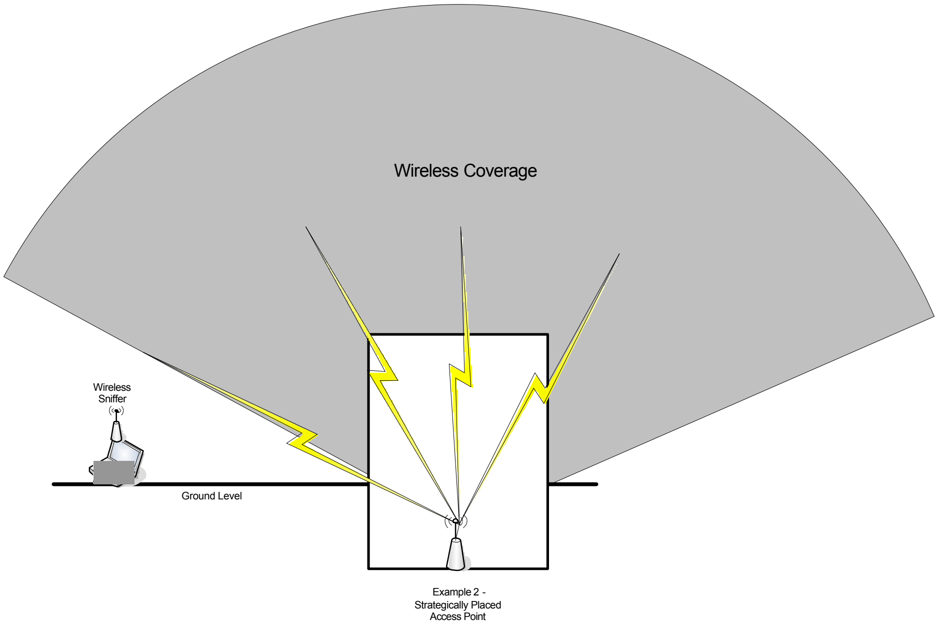


Figure 15 - Strategic Placement of Access Point

5.5.3 Use of Open System WEP authentication.

As indicated above, Open Network WEP authentication provides dynamic WEP key generation between the client and access point. While this does not protect against WEP vulnerabilities related to IV generation, it will help reduce the susceptibility of the network to brute force attacks on static keys.

5.5.4 Use a more complex WEP key

As with any brute force guessing attack, the more complex the WEP key, the harder it is to guess it. Ways to introduce complexity into the key include use of non-dictionary words, using numbers and non-alphanumeric characters, and using multi-word phrases instead of single words.

Examples of effective passphrases might be “Th1s1sMyP@ssPhr@s3” instead of “passphrase”.

5.5.5 Use of Secondary Authentication

Many higher end access points provide hooks for the use of external authentication mechanisms such as RADIUS to authenticate users before allowing access to the wireless network. This solution is usually only used in corporate wireless environments, as the complexity of configuring this type of architecture is generally beyond most home users skill sets and requirements.

5.5.6 Use of WPA/802.11i

Wireless devices using 802.11i or 802.11g with WPA provide a significant security increase over the use of WEP. If these protocols are available, they should be employed within the wireless infrastructure. In some cases, the firmware of wireless devices can be upgraded to support WPA.

6 Conclusions

Overall, WEP is certainly not the best mechanism for securing a wireless network. It has a number of inherent security vulnerabilities which are overcome by newer wireless security protocols and security measures such as 802.11i and WPA. However for a number of reasons, including the requirement to support legacy wireless devices or operating systems which do not support these new security measures, it may be necessary to employ WEP within a wireless environment.

Regardless of the problems, there are ways to reduce the risk associated with using WEP. The use of complex passphrases as WEP keys which are changes on a regular basis can reduce the risk associated with brute force attacks on the WEP keys. The use of open network WEP to create dynamic WEP keys, where possible is preferable to the use of static keys.

References

[1] Kismet Wireless (http://www.kismetwireless.net)

[2] WEPAttack (http://wepattack.sourceforge.net)

[3] John the Ripper (http://www.openwall.com/john)

[4] Mitchell, Bradley; WLAN Standards - 802.11b 802.11a 802.11g - Which One is Best? http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm)

[5] Wikipedia, the Free Encyclopedia - 802.11i (http://en.wikipedia.org/wiki/802.11i)

[6] Ossman, Michael, "WEP, Dead Again, Part 1", December 14, 2004 (http://www.securityfocus.com/infocus/1814)

[7] ChangeMAC for Linux - http://galeb.etf.bg.ac.yu/~azdaja/changemac.html

[8] Changing MAC Addresses on Windows 2000 and XP http://www.nthelp.com/NT6/change_mac_w2k.htm