Global Information Assurance Certification Paper

Layered Wireless Security Case Study

GSEC Version 1.4b

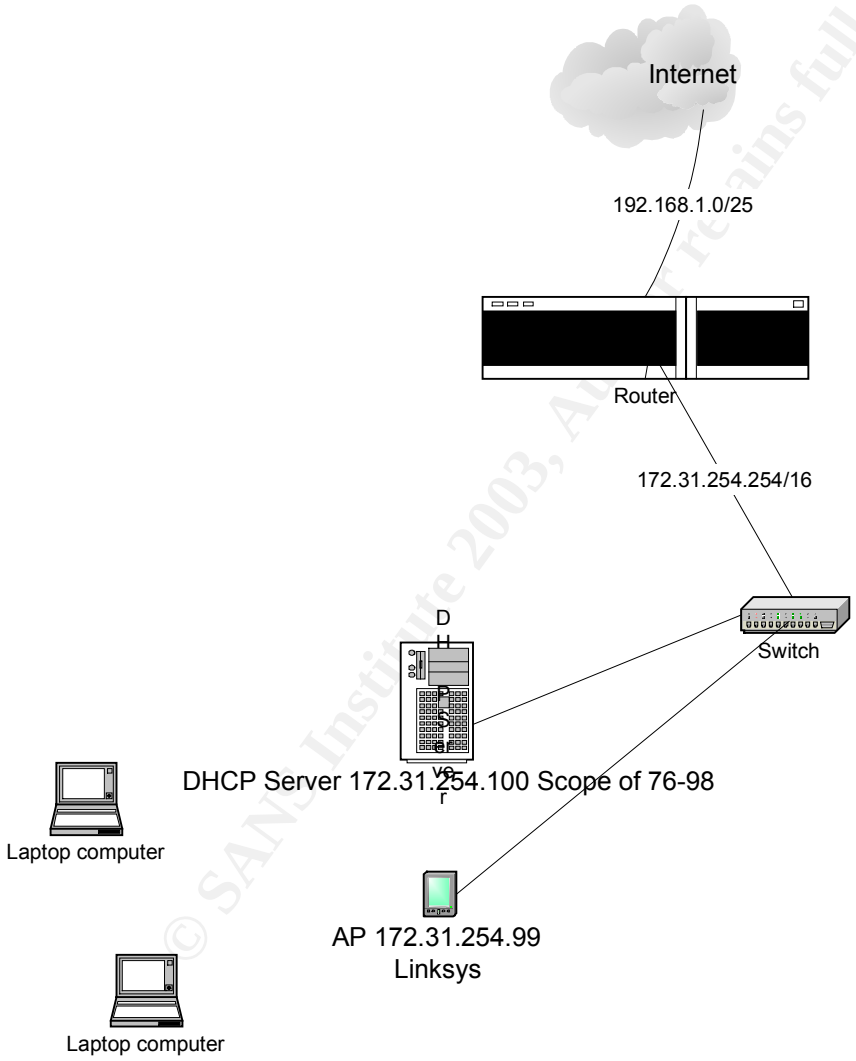
Jennie Collins

July 16, 2003

Table of Contents

Introduction

The objective of this study is to implement layered 802.11b wireless security and to attempt to break each layer to see how relevant each layer is for overall security. In addition, I needed to consider the best method of securing a wireless LAN while providing reasonable convenience to business and end users. At the physical layer I implemented WEP; at the data link layer I implemented MAC filtering; and at the network layer I implemented VPN along with session layer protocol SSH. To start the study, I designed a wireless LAN. It was simple setup consisting of a router, a switch, a DHCP server, an AP, and 2 laptops. Below is the network setup with the appropriate IP's:



Network Configuration/Layered One Implementation

The first task was to set up the DHCP server. The DHCP server was a Windows 2000 box with a scope of 76-98. A scope was set to limit the range of IP allowed onto the test

network. For example, the only IP's that the laptops could be assigned were 172.31.254.76-172.31.254.98. Again, the scope was not mandatory-it was a way to limit IP's. Next, I set up the Linksys Access Point. Below are screen shots from the Linksys web interface, which I used to configure the access point.

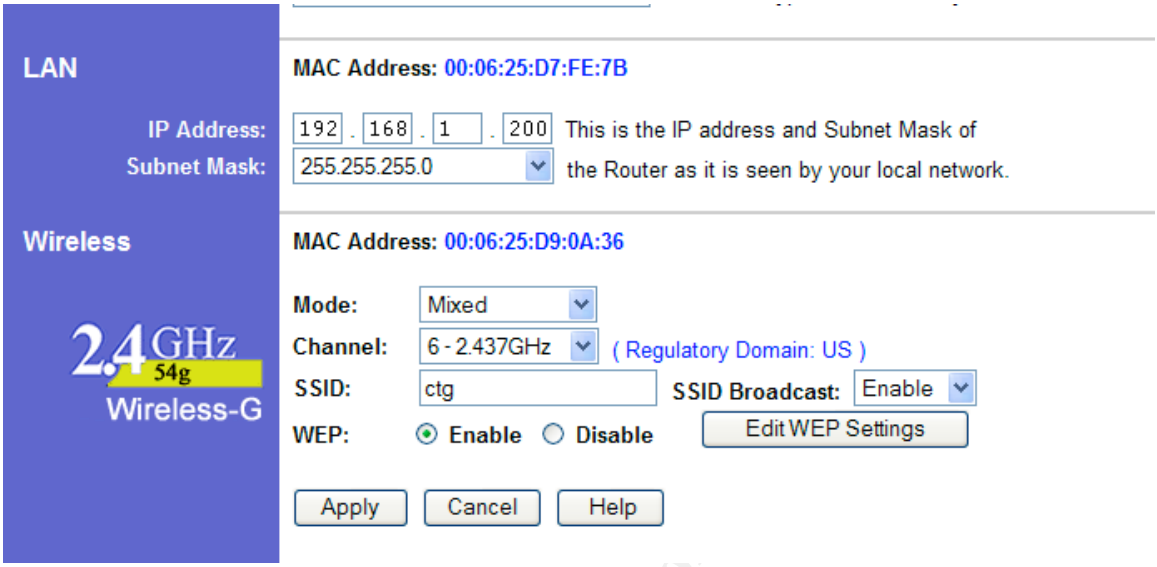


Figure 1 Linksys web interface

I changed the SSID to ctg, enabled SSID broadcast, and changed the default password of the Linksys AP (it's is general knowledge that the default password for Linksys equipment is Admin). I then enabled the access point with a WEP 40 bit key. WEP uses RC4 algorithm. See the "WEP & RC4" section for a more descriptive understanding of WEP's security flaws. For example, tools such as Airsnort and WEPCrack have already cracked this algorithm. Newer versions of WEP can also be configured with a 128-bit key, but again, Airsnort and WEPCrack have cracked this key as well.

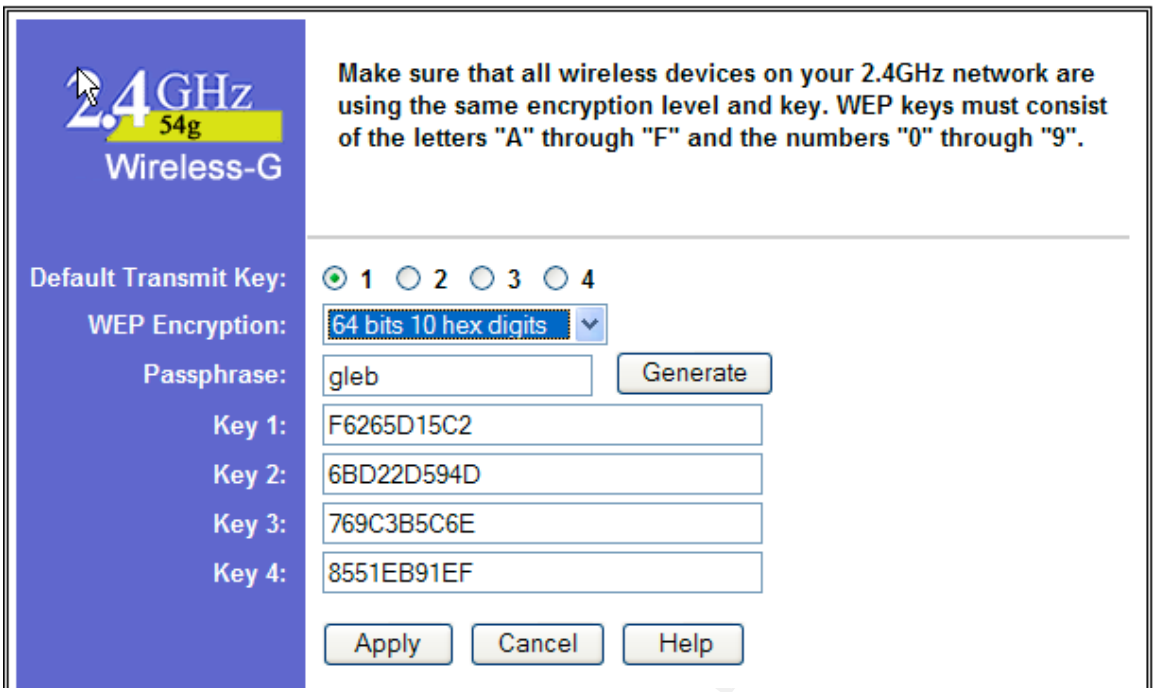


Figure 2 Linksys web interface

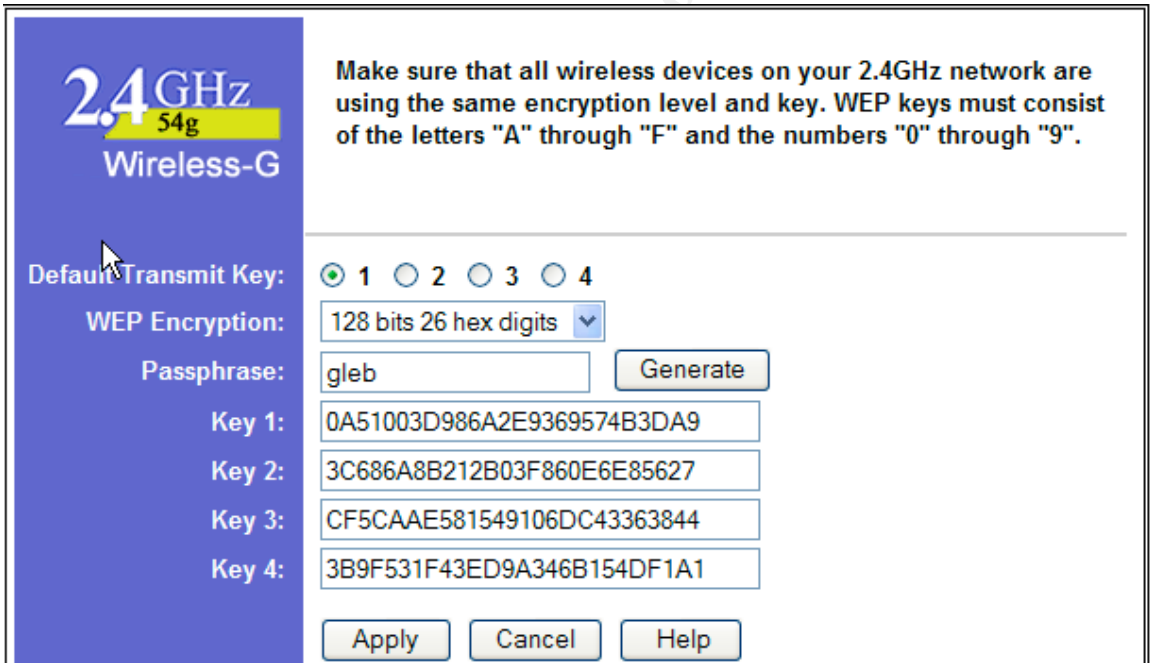


Figure 3 Linksys web interface

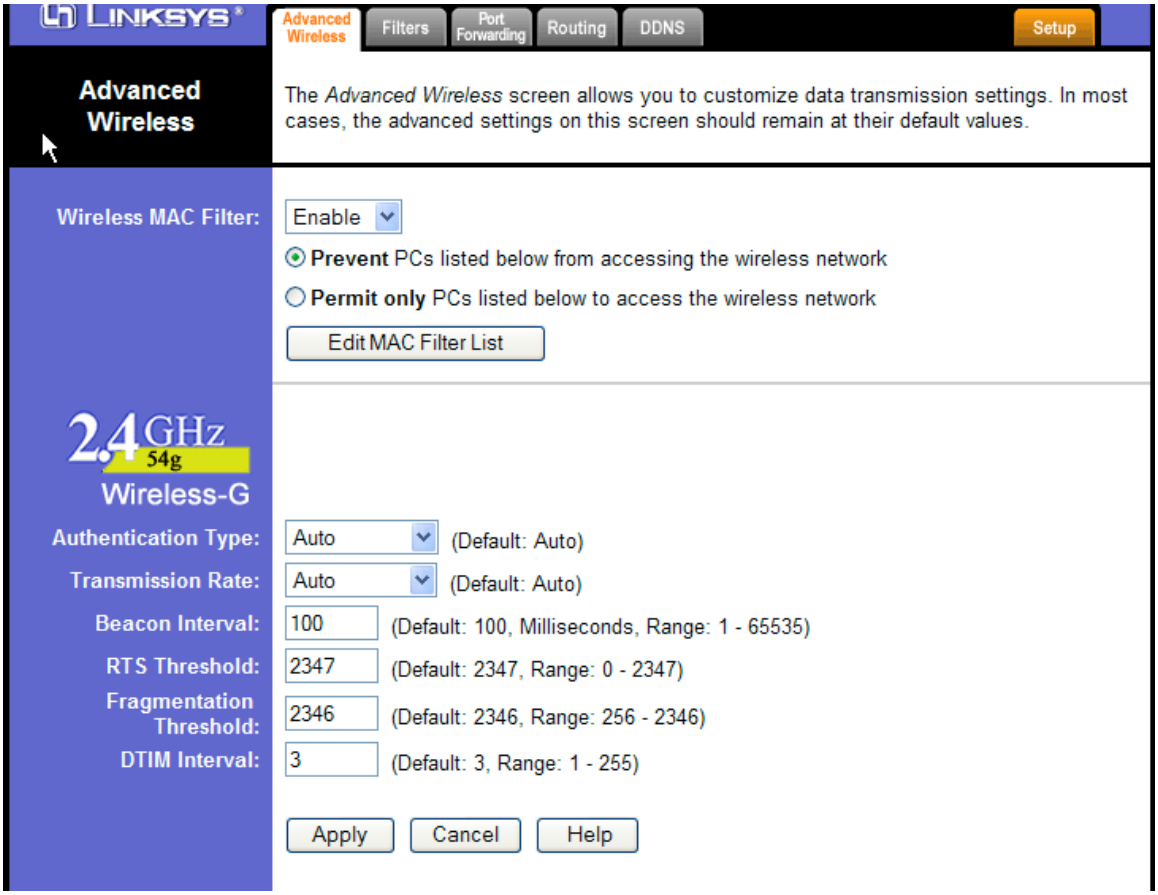


Figure 4 Advanced Wireless Features

Layer One Attack

I attempted to crack WEP with Airsnort. I used KNOPPIX/Airsnort and RedHat 9.0/Airsnort as well. What I thought was going to be an easy security break turned out to be just the opposite. With KNOPPIX/Airsnort, I was able to capture traffic, but since KNOPPIX runs from a CD, my memory buffer filled and I would have had to "dump it" before I could get enough data to translate. I was able to run interface in promiscuous mode by using "any" for the network device preference and "other" for the card type preference.

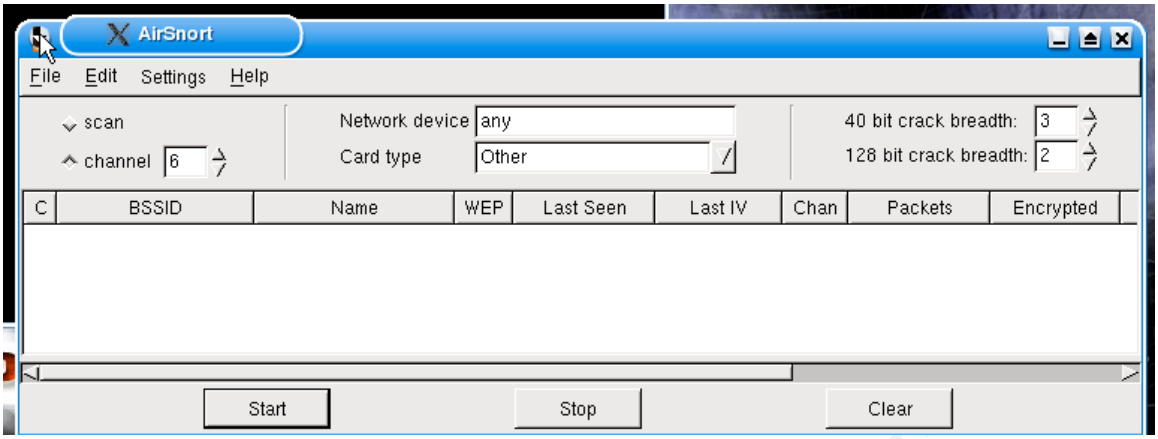


Figure 5 Airsnort

With RedHat 9.0/Airsnort, I couldn't put the card into promiscuous mode without patching the driver.[1] After patching the driver, I still ran into memory buffer issues. I also couldn't find any documentation on how to change the buffer settings of airsnort. With most freeware tools, documentation is limited and at best, up to your own interpretation.[2] I was able to capture 802.11 packets with Link Ferret[3] since if has it's own set of drivers, but again, I ran into issues with buffer overflow.

The purpose of trying to capture as many frames as possible was to decipher what the WEP base key was and to use it to gain access to the network has an unauthorized user.

Network Configuration/Layered Two Implementation

The next layer of security implemented was MAC filtering. I had the option of configuring a CISCO switch, but instead I used the built-in features of the Linksys AP included MAC filtering.

Layer Two Attack

I used the SMAC[4] tool to spoof a MAC and I was able to get onto the network. An attacker would not be aware of the MAC addresses that were allowed to access the network unless they cracked WEP and then sniffed the network for associations. By putting the network card in promiscuous mode an attacker can sniff traffic and determine what MAC address are currently residing on the network. Those addresses have the potential of being spoofed and allowed access. For now, SMAC can only be used on Windows 2000 and XP machines. Below are captures of a real MAC joining the network and then a rogue MAC that has joined with the network by stealing the real MAC. For further explanation of the frame types, please see the "Wireless Frames" section.

---

[1] http://airsnort.shmoo.com
[2] http://airsnort.shmoo.com
[3] http://www.linkferret.ws/wireless/wireless.htm
[4] http://www.klcconsulting.net/smac/

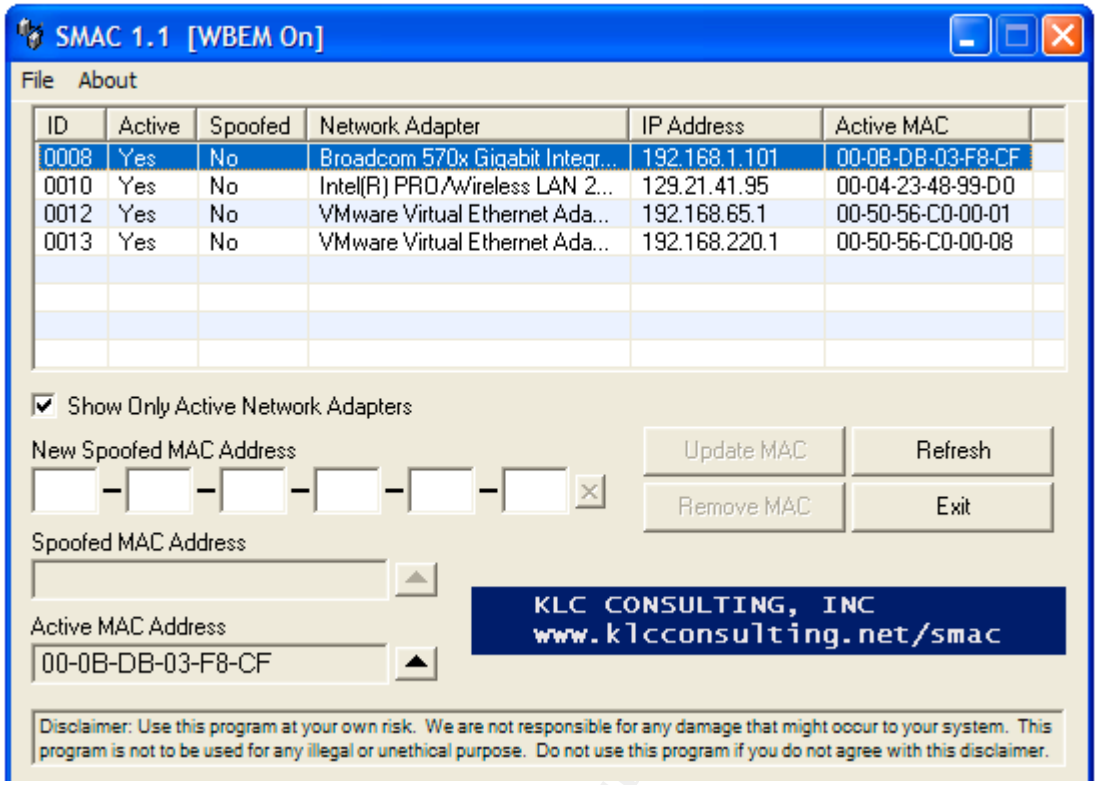
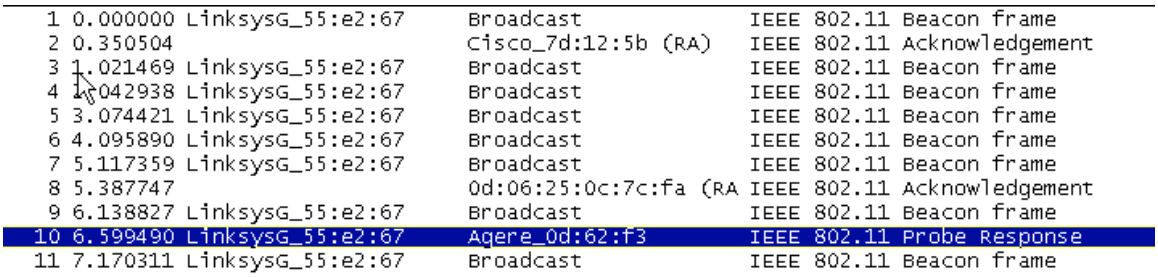


Figure 6 SMAC

```
  1 0.000000  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  2 1.031484  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  3 2.052952  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  4 3.074421  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  5 4.095890  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  6 5.127373  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
  7 6.008640  10.1.2.1              10.1.2.255            RIPv1       Response
  8 6.078741  LinksysG_55:e2:67     Acer_81:d8:35         IEEE 802.11 Probe Response
  9 6.148842  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 10 6.299058  LinksysG_55:e2:67     Acer_81:d8:35         IEEE 802.11 Deauthentication
 11 7.170311  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 12 7.570887  LinksysG_55:e2:67     Acer_81:d8:35         IEEE 802.11 Probe Response
 13 7.741132  LinksysG_55:e2:67     Acer_81:d8:35         IEEE 802.11 Authentication
 14 7.741132  LinksysG_55:e2:67     Acer_81:d8:35         IEEE 802.11 Association Response
 15 8.191780  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 16 9.223263  LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 17 10.244732 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 18 11.266200 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 19 12.287669 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame

 20 13.319152 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 21 14.340621 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 22 15.201860                       Cisco_d5:82:6f (RA)   IEEE 802.11 Acknowledgement
 23 15.362090 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 24 16.383559 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 25 17.415042 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
 26 18.436511 LinksysG_55:e2:67     Broadcast             IEEE 802.11 Beacon frame
```

Figure 7 Ethereal



1	0.000000	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
2	0.350504		Cisco_7d:12:5b (RA)	IEEE 802.11 Acknowledgement
3	1.021469	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
4	1.042938	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
5	3.074421	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
6	4.095890	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
7	5.117359	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
8	5.387747		0d:06:25:0c:7c:fa (RA	IEEE 802.11 Acknowledgement
9	6.138827	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame
10	6.599490	LinksysG_55:e2:67	Agere_0d:62:f3	IEEE 802.11 Probe Response
11	7.170311	LinksysG_55:e2:67	Broadcast	IEEE 802.11 Beacon frame

Figure 8 Ethereal

Wireless Frames

The following below captures I captured during layer one and layer two attacking.

"A typical beacon frame is approximately fifty bytes long, with about half of that being a common frame header and cyclic redundancy-checking (CRC) field. As with other frames, the header includes source and destination MAC addresses as well as other) information regarding the communications process. The destination address is always set to all ones, which is the broadcast Medium Access Control (MAC) address. This forces all other stations on the applicable channel to receive and process each beacon frame. The CRC field provides error detection capability."[5]

"The beacon's frame body resides between the header and the CRC field and constitutes the other half of the beacon frame. Each beacon frame carries the following information:"[6]

Beacon interval
The beacon interval by default is set to send ten beacons per second. The beacon interval is set to such a constant signal to ensure that each host on the network has the most current timestamp with each beacon transmission. See Figure 1

Timestamp
The timestamp synchronizes the host's local clock. The timestamp will only be updated if the host does not the have the most current timestamp associated with the beacon interval. See Figure 1.

[5] Geier, Jim. (2002, August 15). Understanding 802.11 Frame Types. Retrieved May 15, 2003 from http://www.80211-planet.com/tutorials/print.php/1447501

[6] Geier, Jim. (2002, August 15). Understanding 802.11 Frame Types. Retrieved May 15, 2003 from http://www.80211-planet.com/tutorials/print.php/1447501

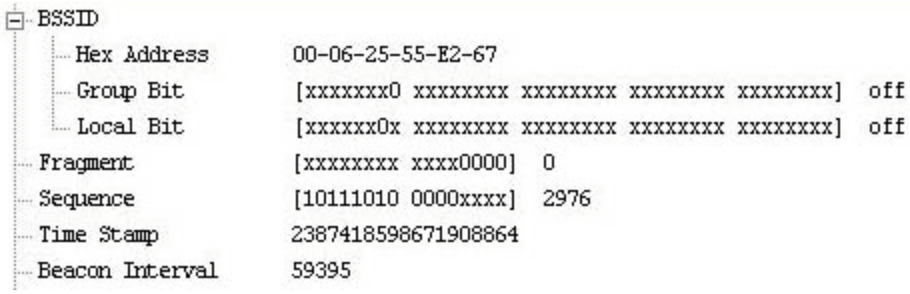


Figure 1

Service Set Identifier (SSID)

The SSID, the Service Set Identifier, is the identifier that separates networks. Ideally SSID's are set to unique name, are longer than eight characters, and are changed from their set default. SSID's also should be set not to broadcast their names if they want to be anonymous to unauthorized users. I changed the SSID of my network to ctg. See Figure 2.

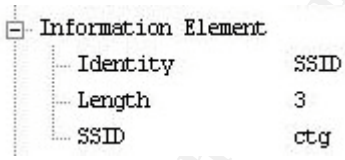


Figure 2

Supported Rates

Supported rates describe which rates the network supports. Figure 3 shows that my configured ctg WLAN supports 1.0MB, 2.0MB, 5.5MB, and 11.0MB rates.

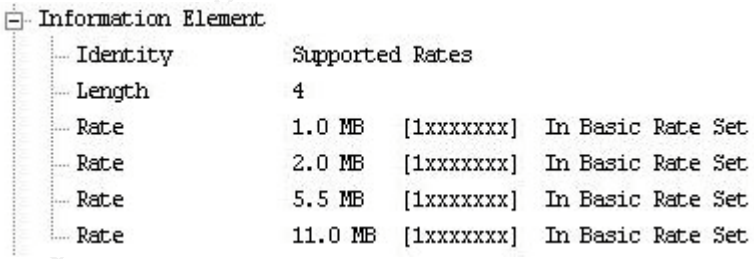


Figure 3

Parameter Sets

The parameter set identifies how the beacon moves around the network. For example, in Figure 4 below, the Identity of my parameter set is DS (Direct Sequence) Spread Parameter Set. A direct sequence spread spectrum transmits over an allowable band.

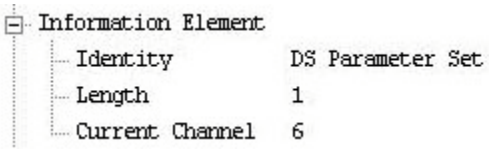


Figure 4

Capability Information

The capability information states the requirements that access point/stations must conform to, to be associated with the network. See Figure 5.

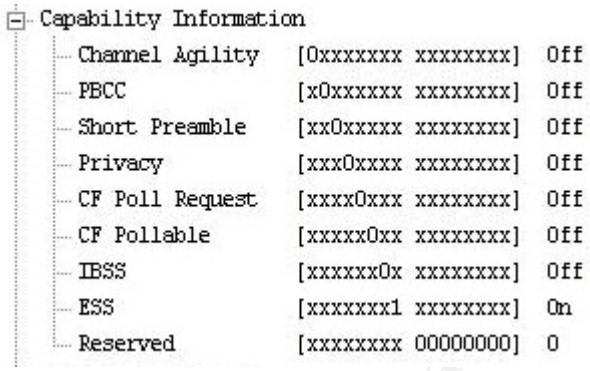


Figure 5

Traffic Indication Map (TIM)

The TIM is sent with each beacon frame to monitor access points that have queued packets and the associated access points are ready to with accept them. See Figure 6.

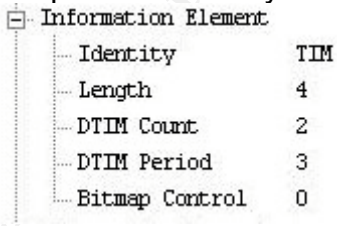


Figure 6

The next frame discussed is the probe response. A probe response is sent after a probe request is received. The probe response will send the SSID of the AP that responds to

the probe request where the broadcast SSID is set to 0.

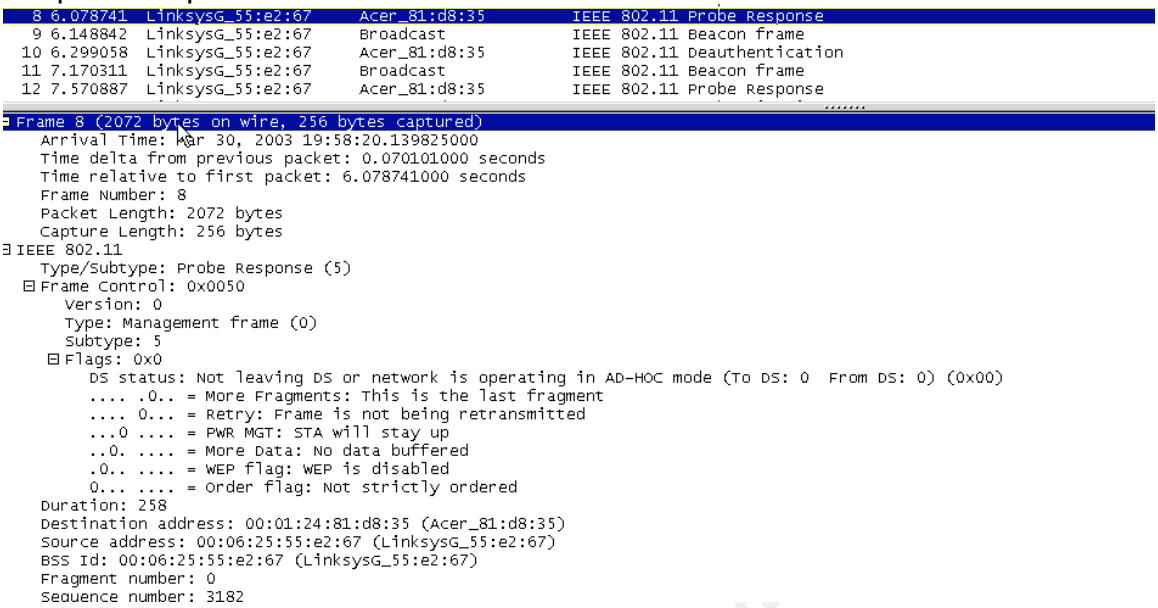


Figure 9 Ethereal captures

The next frame discussed is the authentication frame. The authentication frame either accepts or rejects the host MAC address that tries to authenticate onto the network.

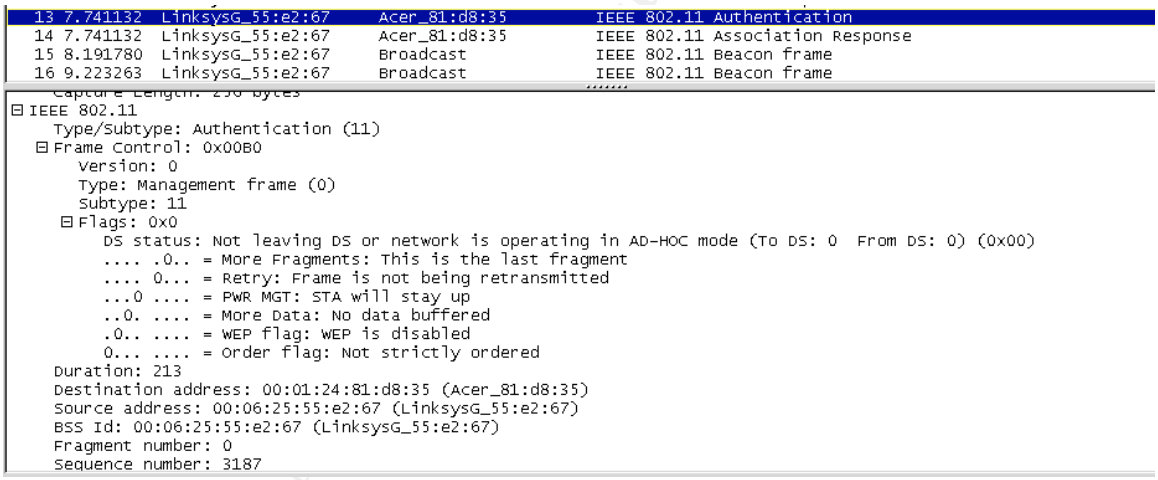


Figure 10 Ethereal captures

The next frame discussed is the association response. The association response sends an acceptance or rejection to the host that is trying to associate with the AP.

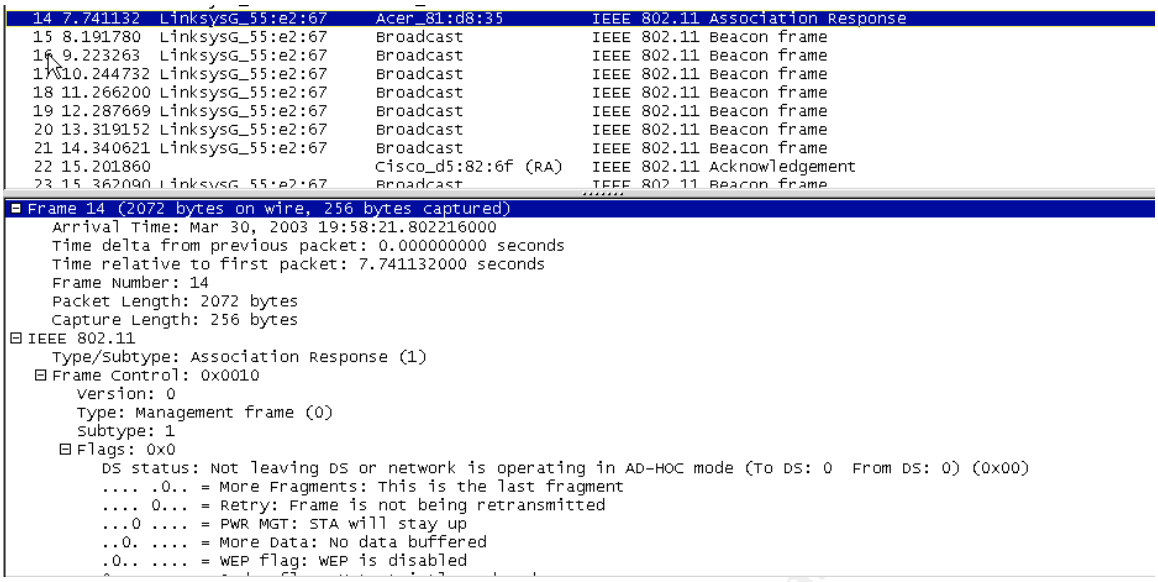


Figure 11 Ethereal captures

The next frame discussed is the deauthentication. The deauthentication frame terminated the secure connection between two access points/stations.

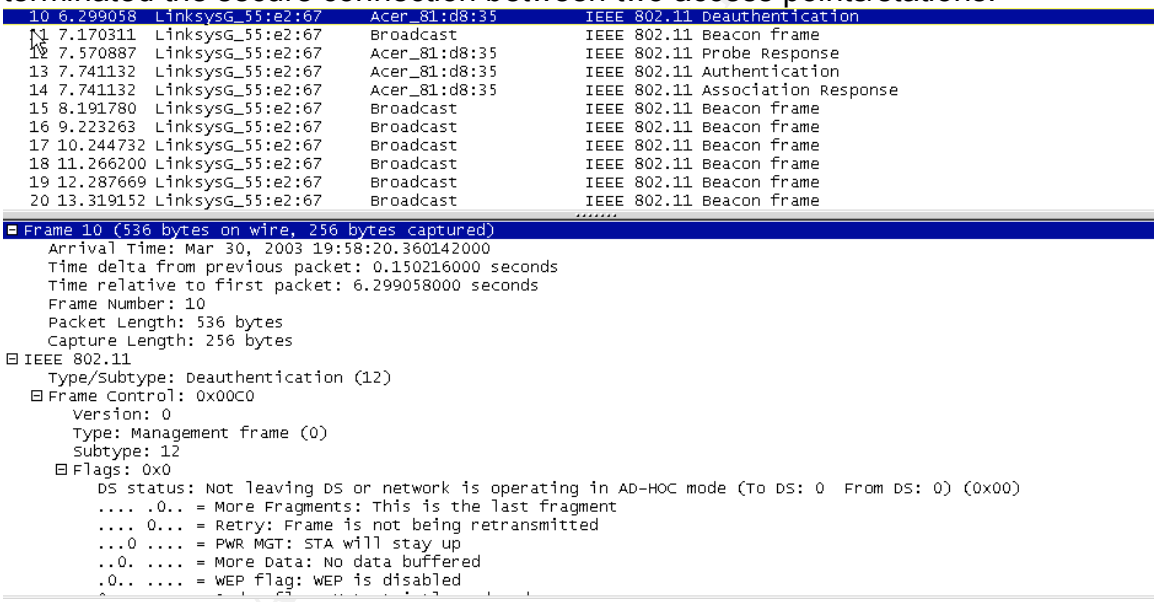
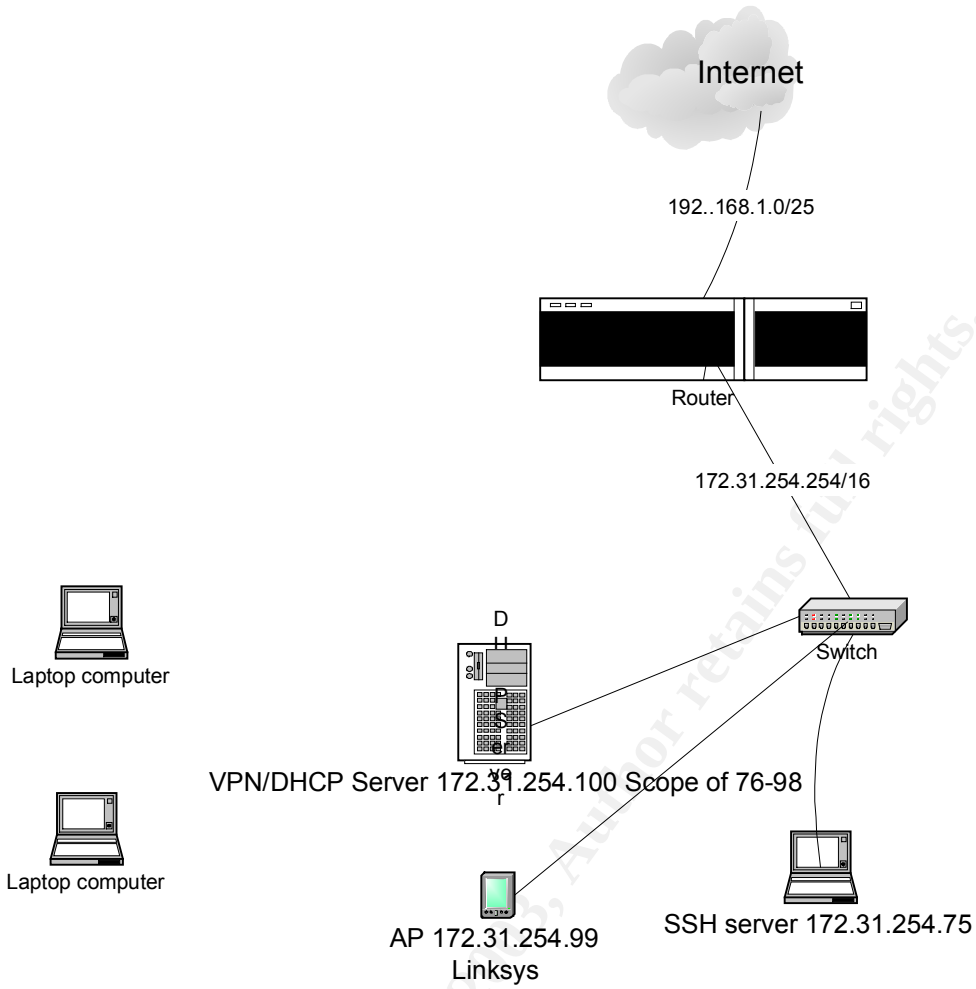


Figure 12 Ethereal captures

Network Configuration/Layer Three Implementation

Last, I we added a VPN server and SSH server. I combined the VPN server with the DHCP server and used a RedHat 9.0 Server Laptop for the SSH server. The new network was the following:



At this stage WEP was enabled and MAC filtering was configured. Users would now have to VPN into the network and then having then run a SSH client to make any changes to the AP. This is the most secure setup. I did run into some issues when trying to configure OpenSSH on the Windows 2000 DHCP server. I set up the VPN server on the Windows 2000 Server (DHCP server). It was very simple, except for one option that caused us a small headache. Each user by default did not have rights to access RAS or dial-up services. I had to enable that option under the user property interface. I then could VPN in from a wireless client using Microsoft's built-in VPN client. I now had a secure tunnel that was also encapsulated in a WEP encryption packet. An external client could now receive an internal IP address. In order to gain secure access to the AP I had to limit the IP addresses. Since wireless clients receive dynamic IP addresses from the DHCP server, it would be very difficult specify those addresses.

After speaking with a network engineer I was informed that access points themselves could be setup to limit IP addresses, and in addition only allow SSH access from remote clients. This type of topology works great with our VPN tunneling. Once a VPN tunnel is established from the wireless client to the VPN server, a dynamic internal address is given to that client. After which a SSH client (still the same wireless client) would gain

access to the AP. During our experimentation we encountered a problem that did not allow access to the OpenSSH server from any client. After some research I determined that appropriate user privileges must be in place before a client could SSH in. By placing the SSH users in a special group and granting that group Administrative rights resulted in a successful login process. This is an obvious security issues, since any SSH client is given Administrative rights. More time was needed to fully determine if I could get away with placing the SSH users in a lower access group.

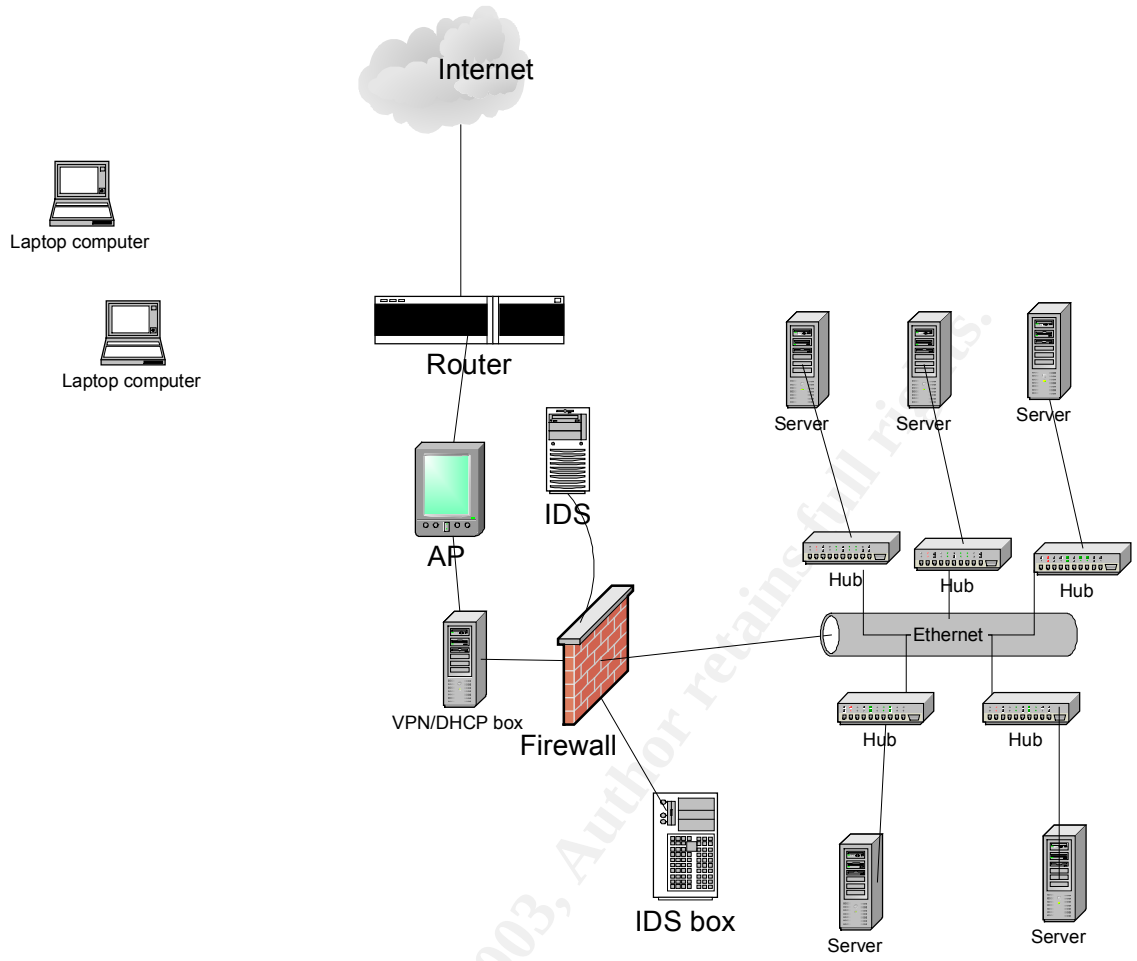
Since our AP did not provide for SSH access, we once again consulted a network engineer. The network engineer demonstrated how it would work in a real world environment. RIT is currently using Cisco APs that allow for remote SSH management. Using the same VPN tunneling and Putty SSH client, the engineer gained access to an AP in a matter of seconds. The access point was configured to only accept IP addresses that were received via a VPN connection form the wireless client. In addition, the limited IP addresses could only gain access to the AP via a SSH connection.

The good thing about VPN is the encrypted tunnel is authenticated through a separate service running on the internal network. AP does not play big role in VPN communication. Therefore if the AP was to be compromised, VPN tunneling would still be secure. I did encounter some problems with VPN tunneling due to our network topology. First, VPN packets when transmitted get encrypted as one big packet. NAT networks have problems reading those packets, since NAT requires for breaking down of the packet to read necessary header information. The same is true for firewalls that are configured for stateless data inspection. The simplest solution that we found was to upgrade your current software/IOS that supports NAT and firewalls. The upgrade contains certain filters that recognize VPN traffic. In some cases actual hardware needed to be upgraded. In case of a PIX Firewall, there are no IOS upgrades only hardware.

Layer Three Attack

When trying to attack the VPN connection, I concentrated on the fact that the security vulnerabilities lied in the wireless connection to the VPN. Since the VPN server was a Windows 2000 server, I searched for know vulnerabilities, but couldn't' find any that would infiltrate the network. Again, to infiltrate I would have had to decrypt the layers of encryption on the packets- the first is WEP, second is VPN tunnel, and the third is SSH traffic.

By implementing a wireless VPN connection, I reduced potential security vulnerabilities. The only unencrypted traffic area would be the wireless connection being made to the initial VPN connection. Our network configuration was not set up securely though. As you can see from the above diagram, a wireless user could bypass the VPN since the AP and the VPN server were on the same switch. Ideally, the network should have looked like this to implement VPN with wireless:



You will notice that this network also consists of 2 IDS boxes, one in front of the firewall and one behind the firewall. This is added protection. You can investigate activity in the DMZ and the internal network and also to monitor the firewall rule set is consistent.

Lessons Learned/Obstacles

After all the hype I heard on how easy it was to crack WEP, I found out the hard way that it wasn't as easy as we anticipated. Without a well-equipped laptop, ample amount of time, and sufficient amount of encrypted traffic cracking WEP can be a bit frustrating. I did see a display at the SANS Portland conference with BSD and the new WEPCrack tool on sourceforge.net. The two attendees were able to crack WEP in 30 minutes. The WEP key they cracked was 40 bit. After our frustration with trying to crack WEP, I spoke with a network engineer. He discussed the implementation he used. WEP is implemented on his network, but he added that it was a management nightmare it would cause. Also, he also added that once you hand out the WEP keys, it's just like a password and sooner or later it will get into the wrong hands. The network engineer also mentioned that the CISCO access points used on campus allow WEP and non-encryption to be enabled at the same time. He also has implemented VPN and SSH for accessing access points and routers. The way it works is that once you VPN into the

network, you then use the SSH client to access the AP or router. The configuration also only allows one IP to connect to the AP or router at a time. The security issue is the wireless connection used to VPN into the network.

Other obstacles we encountered on the way were capturing and configuration issues with Ethereal, Link Ferret, and Airsnort. Although the latest release of Ethereal allows 802.11 captures, I was unable to set the wireless adapted into promiscuous mode to do so. Ethereal does however work on the Linux side, but you need to patch the wireless adapter as well for it to be set in promiscuous mode. Link Ferret worked well. Since is has its own set of drivers, capturing 802.11 frames was easy. The issue was when you wanted to restart a capture. I also ran into the issue of compatibility with Centrino technology. Again, my Intel 2100 adapter could not be put in promiscuous mode. I had the same issues with Airsnort buffer preferences and promiscuous mode as well.

WEP & RC4

This section is just a little background information on how WEP works and what the security flaw is. WEP stands for Wired Equivalent Privacy. WEP security is based on a scheme called RC4 that involves a "shared secret keys" along with system-generated values as well. When people speak of 64 bit or 128 bit encryption, the actual key length is 40 and 104 bits with 24 bits of system-generated data.

The in order to crack WEP, the following information is needed: the ability to capture a large number of transmitted data, the ability capture packets over an extended period of time, and a relatively powerful machine to decipher the packets to reveal the WEP key.

The weaknesses associated with WEP include forgery, weak-key attacks, collision attacks, and replay attacks. Forgery occurs when a transmitted packet(s) is captured. Once the packets are captured, the payload is changed and the packet is resent. This forgery will allow a potential attacker to authenticate. Weak-key attacks occur when potential attackers capture packets and examine the RC4 key that is created by the concatenatation of the RC4 base key and the Initialization Vector (IV) packet. Since the RC4 algorithm doesn't change the RC4 base key, attackers can captures enough packets to find the base key by analyzing the associated IV packets. Collision attacks occur when the key is send with the same IV packet allowing the data to be discovered. Last are replay attacks. Replay attacks occur when a session of transmitted data is captured and then replayed at a later time. With WEP, there is no way to check whether a transmission is the original session or a replayed one.

Best Wireless Network Practices

Best practices are only as good as the documented processes and procedures in place for the network engineers and network administrators to adhere to. If engineers want to implement a design that is not in compliance with such processes, a change control process needs to be in place as well. The change control process should also follow a separation of duties so engineers who are requesting the change are not auditing and approving it. Again, best practices must also compliment business continuity. Business drives technology, not vice versa.

Wireless processes and procedure should explicitly state what you are trying to secure and why. Production and non-production business assets need to be protected from physical theft, data theft, and physical damage. Access and authentication are also instrumental for any wireless policy. Policies designed for not only local users, but also virtual employees as well. Again, if these policies do not exist, create them. If theses policies are not implemented, implement them. Tracking network users on a LAN are hard enough, monitoring on a WLAN can be exhausting, if not impossible if policies aren't in place.

When implementing wireless, businesses need to decide whether they want to incorporate wireless into their existing infrastructure or whether to contrast an entirely different scheme. Incorporated wireless into the predefined network also for the reuse of the Ethernet controlled devices. Engineers placement of wireless devices into the current network topology will have a direct impact on the now wireless LAN. For example, AP placement needs to confine to protected areas of the network. These areas would be behind firewalls and VPNS. In addition, wireless applications may require protected access to the" intranet and/or Internet, affecting routers, firewall rules and VPN policies. A DMZ can protect the WLAN from Internet threats while protecting the wired intranet from WLAN threats."[7]

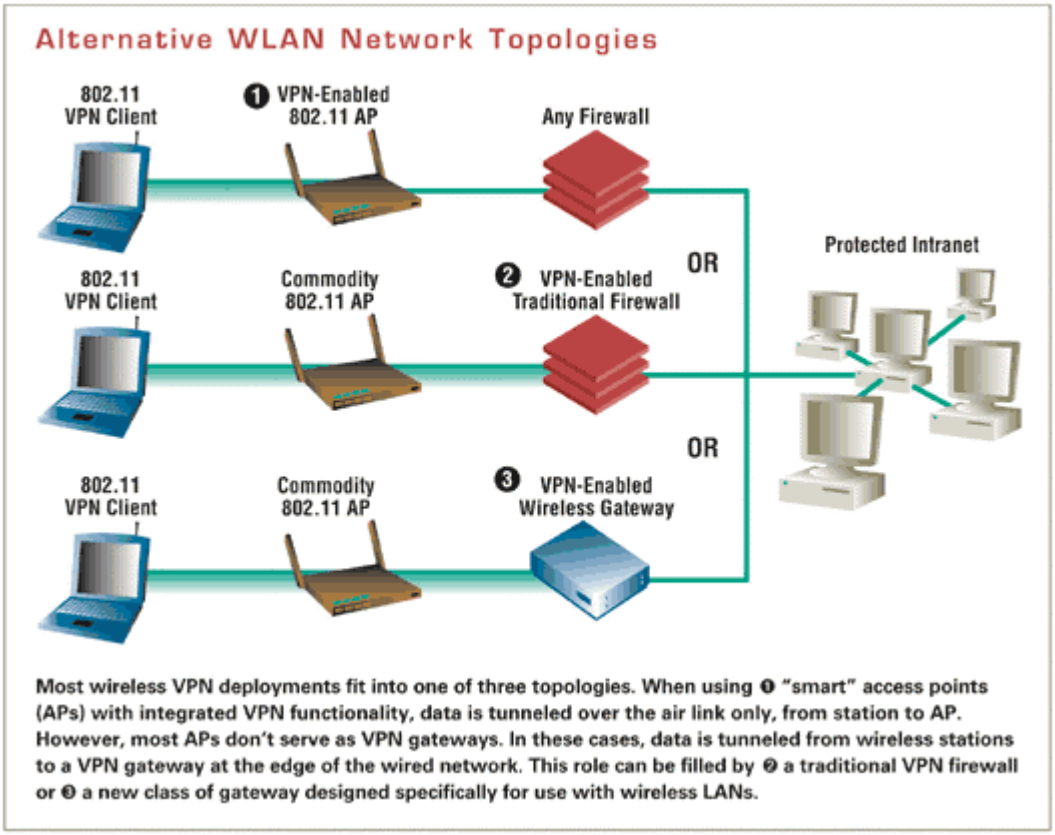


Diagram 1 from http://www.securesynergy.com/library/articles/060-2003.php

[7] Phifer, Lisa. (2003, May 17). Air Safety. Retrieved May 17, 2003 from http://www.securesynergy.com/library/articles/060-2003.php.

802.11's current standard security is composed of authentication and encryption, such as WEP. As stated earlier, when shared-key authentication is enabled, hosts can only associate with the AP if the AP and the host trying to associate are configured with the same known 40- or 104-bit key. By configuring the SSID correctly, meaning with a unique name that is eight or more characters, and disabling SSID broadcasting, will lower the risk of unwanted users. Hosts that operate Windows XP can automatically join any discovered network by default. This can be automatic join can be disabled by disabling the QoS service. Again, if the SSID is not broadcasted, XP will not join unless the user is running an application such as Netstumbler. Many AP's have the ability to filter MAC addresses. This filter can allow or block the specified MAC addresses, but MAC addresses can be forged as previously mentioned before with SMAC.

VPN access should be used for all virtual employees. With layer three security, the only main security risk is when the user is connecting making the wireless connection to the VPN device. There is always the possibility for a sniffer to be running on the network

Penetration test and vulnerability assessment tools should be used on a regular basis. WLAN traffic can be captured and analyzed for suspicious behavior. For example, as stated above in the WEP and RC4 section, captured frames can show weak-keys and replay attacks, as well as "excessive de-associate (disconnect) frames, repeated EAP handshaking or WEP errors suggest attack. Stations or APs in open-system mode or without WEP can be flagged as policy violations."[8]

Conclusion:

Wireless is a steamroller. Companies will be forced in some capacity to adhere to the changing wireless standards. The layered approach to wireless implementation is the most effective to ensure a secure network. A layered approach will force potential infiltrators to not only have to have the authorization to authenticate via VPN/SSH, but also break the encryption and authenticate with a valid MAC address. Following industry best practices along with your businesses processes and procedures should instill an acceptable level of security.

List of References

1. http://airsnort.shmoo.com. Retrieved May 15, 2003
2. http://www.linkferret.ws/wireless/wireless.htm. Retrieved May 15, 2003
3. http://www.klcconsulting.net/smac/. Retrieved May 15, 2003
4. Geier, Jim. (2002, August 15). *Understanding 802.11 Frame Types.* Retrieved May 15, 2003 from http://www.80211-planet.com/tutorials/print.php/1447501
5. http://searchnetworking.techtarget.com/gDefinition/0,294236,sid7_gci853455,00.html. Retrieved May 15, 2003

[8] Phifer, Lisa. (2003, May 17). *Air Safety.* Retrieved May 17, 2003 from http://www.securesynergy.com/library/articles/060-2003.php.

6. Phifer, Lisa. (2001, April 26.) *Wireless Privacy: An Oxymoron?* Retrieved May 20, 2003 from http://www.isp-planet.com/technology/2001/wep.html.
7. Phifer, Lisa. (2003, May 17). *Air Safety.* Retrieved May 17, 2003 from http://www.securesynergy.com/library/articles/060-2003.php.
8. Wexler, Joanie.(2001, August 29). *VPN and Wireless LAN Security.* Retrieved May 15, 2003 from http://www.nwfusion.com/newsletters/wireless/2001/00960610.html
9. Grosser, Richard C. (2002. October 23). *A Layered Approach to Security for Wireless Networks.* Retrieved May 15, 2003 from http://www.computerworld.com/securitytopics/security/story/0,10801,75330,00.html.

Works Cited

1. Phifer, Lisa. (2003, May 17). *Air Safety.* Retrieved May 17, 2003 from http://www.securesynergy.com/library/articles/060-2003.php.
2. Geier, Jim. (2002, August 15). Understanding 802.11 Frame Types. Retrieved May 15, 2003 from http://www.80211-planet.com/tutorials/print.php/1447501

Appendix Free Wireless Tools

The following tools are all available at www.networkintrusion.co.uk/wireless.htm. Unfortunately, some are commercial, but you can download trial copies.

1. BSD-Airtools-
2. NetStumbler
3. Kismet
4. FakeAP
5. Airsnort
6. WaveStumbler
7. Wireless Scanner
8. Airosniff
9. Airopeek
10. StumbVerter
11. AP Scanner
12. Sniff Wireless
13. WEPCrack
14. Prism2
15. MiniStumbler
16. SSIDsniff
17. MacStumbler
18. WaveMon
19. PrismStumbler
20. AirTraf

21. MogNet
22. AirMagnet
23. Isomair
24. Air-Jack
25. AirDefense IDS
26. WiFiScanner
27. witools
28. Aerosol
29. WLAN Expert
30. WaveScanner
31. WaveSentinel
32. Airsnare: http://home.attbi.com/~digitalmatrix/airsnare/

Acronyms

1. LAN: Local Area Network
2. WEP: Wireless Equivalent Privacy
3. MAC: Media Access Control
4. VPN: Virtual Private Network
5. DHCP: Dynamic Host Control Protocol
6. NAT: Network Address Translation
7. RAS: Remote Access Server
8. IP: Internet Protocol
9. AP: Access Point
10. SSID: Service Set Identifier
11. NIC: Network Interface Card
12. SSH: Secure Shell
13. DMZ: Demilitarized Zone

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event