Global Information Assurance Certification Paper

Author: Sharon Page
Version: 1.4b
Title: Secure Wireless At Home?
Certification: Security Essentials, GSEC
Date: 3 February, 2003

Abstract
As wireless equipment has become cheaper and easier to install, more home personal computer (PC) users are choosing to set up their own home wireless networks. As a consequence, the homeowner is exposed to a variety of wireless and non-wireless security vulnerabilities they may be unaware of and/or do not know how to fix. Thus, the ability to identify the security vulnerabilities that exist on the homeowner's PC as well as the ability to secure the wireless equipment is becoming a critical issue.

By establishing a home-based wireless network we will explore the possibility of installing a secure wireless network using commercially available wireless equipment commonly found in neighborhood computer stores. Methodically, we will identify what security vulnerabilities exist on the evaluation PC then secure them. Further security measures such as implementing access control and adding anti-virus software will be applied to harden the PC. These steps will be performed before the wireless network is set up to decrease exposure to security vulnerabilities that might be imported when the wireless network is added. For the purpose of this paper, two wireless access point appliances, D-Link and Linksys, will be compared for their security features, security configuration flexibility and ease of use. From that comparison a determination will be made as to which appliance best meets our needs. Next we determine the most secure location for the wireless access point to limit its emissions outside the house, but keeping the signal accessible from various points within the house. Post-installation, the security features and configurations on the wireless access point and the PC will be further configured to limit exposure to wireless security vulnerabilities. After the wireless environment has been set up, a network scan will be performed to identify remaining security vulnerabilities or determine if new vulnerabilities have appeared after implementation of the wireless changes. In addition a war-driving test will be conducted around the exterior of the house to determine the emanation distance of the wireless access point. In the end some risk may need to be accepted to take advantage of the convenience of a wireless environment.

1 Introduction

The focus of establishing a wireless network in a home environment is to determine the efforts that should be taken to install a secure wireless network. While documenting the process, information will be provided that is necessary to protect the PC and wireless access point against hackers. This requires setting up several different security tools and secure configurations on both the PC and the wireless access point, called "Defense in Depth".

1.1 Current home network environment

Current Internet access is achieved via cable modem. The cable company does not provide static IP addresses to each residential Internet customer. Instead a range of IP addresses are available to homeowners and a Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign an IP address each time a PC user logs onto the Internet.

I have purchased a new Toshiba Satellite Pro 6100 laptop, which I will be using to establish the wireless network in my home. The PC has the following configuration:

- Intel Pentium 4 M, 1.8 GHz
- Windows 2000, Version 5.02195 Service Pack 2
- Internet Explorer, Version 5.5, Service Pack 2
- Norton Antivirus Software

A Toshiba PCX2200 Toshiba cable modem will be used as the cable access point.

1.2 Describe security problems

The evaluation PC has the following several security problems:

- Lacks current application versions and patches.
- Has no firewall application.
- Needs antivirus software signature list update. New viruses and worms are introduced to the Internet every day so the signature list used to find them must be updated with the new signatures for them. Additionally, new security vulnerabilities are being discovered daily by hackers, making it impossible to prevent every potential hacker attack. For this reason no financial and sensitive data are put on the computer used to access the Internet.

A weakness of the Internet access via cable modem is the assignment by the cable company of a new IP address each log on. Thus I am forced to allow the use of DHCP in my home network environment. A hacker can use a DCHP client to access the wireless access point to request an IP address. Most DHCP servers do not authenticate the user and will provide an internal IP address to the hacker. This also allows a neighbor with a wireless device to inadvertently get onto your wireless network if other security measures are not enforced.

A second weakness of Internet access via cable modem is that the Internet access is always "on" and accessible by others if no security measures are taken.

2 Prepare for wireless access

2.1 Fix existing security problems on the PC

Before implementing the wireless access point, several PC upgrades need to be made to secure the PC. The wireless connection will make it easier for an unauthorized user to access the wireless access point. If the hacker can access your access point's signal then they can access the homeowner's PC. The PC needs security controls in place to prevent an attacker from logging on. If an attacker is able to bypass the security

controls and access the computer, the PC should be configured to limit the damage an attacker can do to the computer. This will help mitigate some of the risks a homeowner takes when using a wireless Internet connection. The preparation strategy will address:

- Systems security hardening
- Anti-virus updates and management
- Firewall installation and configuration
- Access point comparison analysis

2.1.1 Harden the personal PC

The PC needs to be secured by upgrading the operating system and other applications to eliminate known security vulnerabilities. Most of the systems that have been successfully attacked in the past did not have patches installed for well-known security patches. Hackers scan networks on the Internet and send out numerous attacks against known vulnerabilities. They eventually hit the systems that have not fixed these security vulnerabilities.

In order to determine what systems were not running with the current update and patches I used an application readily available over the Internet. Microsoft provides a tool on their web site which provides the capability of scanning a PC for Microsoft applications that are out of date and missing security patches. (http://v4.windowsupdate.microsoft.com/en/default#.asp) After selecting the option to search for applications that need to be updated, it scanned my PC and then listed all of the applications that were obsolete and the patches that needed to be added. The web site also allows the user to install the patches as well. This option was used to upgrade my system software versions and patches.

After the software upgrades and patches were downloaded from the Internet the Norton AntiVirus scanned all of the files on the computer to determine that no viruses or worms were introduced

The guidelines provided by the National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System* were used to determine other changes that were needed to harden the PC.

- Turned off services that were not needed
- Changed some default configurations
- Turned on the auditing and logging capability
- Disabled the guest account and changed the admin userid to ensure that unknown users could not use that account to log onto my computer.
- Set up the PC to require the input of a password to log on and set up the password security policies. To set the security settings I selected **My Computer** icon, the **Control Panel** icon, then I selected the **Administrative Tools** icon, then **the Local Security Settings** icon.
- Turned on the Application log, Security log, and System logs to provide the auditing and logging capability. The logs were set up at 512 KB and set to

overwrite events older than 7 days. The PC is configured to log the following events: information, warning, error, success audit and failure audit.

2.1.2 Install personal firewall

When accessing the Internet everyone should use a firewall to prevent hackers from being able to access or log onto their computer. In a home environment this firewall is called a personal firewall. The personal firewall software will be installed and configured on the PC. Rules must be set up on the firewall to deny any traffic originating from the Internet unless explicitly allowed by a firewall rule.

ZoneAlarm Pro 3 was chosen as the personal firewall to install on my PC because it is inexpensive and several articles on firewall comparisons give it a good rating, saying it has the capability to check outgoing as well as incoming traffic. It provides wireless Network protection if it is decided to install it on the wireless access point device. "Unlike other personal firewalls, ZoneAlarm Pro includes Program Control to protect against known and unknown Internet threats. Program Control monitors all outbound traffic to prevent rogue programs from transferring your valuable data to a hacker."[2] It also provides Ad Blocking and Cookie Control.

When ZoneAlarm Pro installs it provides 10 pages of GUI screens that ask questions about how the installer wants the firewall to be set up and configured. It sets up three zones: Trusted, Internet and Blocked. The ZoneAlarm firewall was configured with a password so hackers cannot make changes to the firewall without the password. In addition, ZoneAlarm requires the user to OK new outgoing Internet connections with the password. ZoneAlarm also has a "Stop" button that allows the user to instantly stop Internet access if a hacker is found on the computer. The user right cl.icks on the **ZoneAlarm** icon and select either "**Engage Internet Lock**" or "**Stop all Internet activity**".

The firewall was configured to log the following events:

- new programs,
- changed programs,
- new program components,
- changed program components.

The firewall was also configured for the following:

- Cookie control was set to medium. This means that it blocks cookies from tracking sites but allows cookies for personalized services. This control helps protect the users privacy.
- Ad control was set to medium. Ads are blocked that do not load in a certain amount of time. The default setting is 3 seconds. It also blocks all popup/under and animated ads. This helps to prevent interruption of the users Internet work
- Mobile Code Control was enabled. This blocks active page elements that can be distracting or malicious. However, turning this feature on may prevent some pages from loading. For example, with it set I am unable to use the on-line support feature provided by my Internet cable provider.

- Internet Zone Security was set to medium which means that the PC is visible to the Internet but is in protected mode. Other computers cannot share your computer's resources. Incoming NetBIOS is blocked. This is the location where ICMP, UDP, etc can be blocked
- MailSafe provides virus detection on incoming e-mail attachments. As the Norton Antivirus software is being used on my evaluation PC, this option has been turned off. However, sometimes it may be a good idea to use both virus protection packages. Each has its own signature list to check against so each may detect viruses that the other antivirus package does not detect.

Initially the Internet Security level was set on High. At that setting ZoneAlarm would not allow the PC to log onto the Internet via the cable modem because of the need to allow DHCP to pass the IP address for each log in. To log onto the Internet the Internet Security level had to be lowered to Medium to accept the new IP address.

2.1.3 Upgrade Antivirus software

The laptop came with the Norton Antivirus software; however, the antivirus signatures were out of date. New viruses and worms are introduced into the network daily so the antivirus signatures require frequent updates. When initially installing the Norton Antivirus software, I set it up to send an alert when the signatures were out of date and allow me the option to download and install the signature updates to bring the package up to date. At least once a week I log into the Norton web site and download new and revised signatures.

The Antivirus package was set up to scan all incoming email for viruses before it is delivered to Microsoft Outlook. To prevent turning on viruses or worms that are hidden in files that you want to down load from the Internet, users should save the file from the Internet to a download directory, then an antivirus scan should be run against the file to determine it is virus free. Do not open a file that has a virus in it. If a user opens a file from the Internet before it is scanned they could be introducing a virus to their system.

2.2 Compare different vendors' wireless access point equipment

There are several vendors that provide wireless access points. The choices have been limited to vendors that are available at computer retail stores, such as Best Buy and CompUSA, where the typical homeowner buys computer equipment. The common wireless access point vendors that will be reviewing are D-Link and Linksys.

The D-Link *Air*Plus line of 2.4GHz wireless Access Point router delivers data transfer rate capabilities up to 22 Megabits per second (Mbps). Model DI-614+; a quad-mode Wireless Access Point, has a 4-port switch to allow direct connect to computers.

The Linksys Wireless Access Point Router with 4-Port switch (BEFW11S4) has a data rate of 11Mbps. It supports universal plug-and-play for easy configuration. It has a 4-port switch to allow direct connect to computers.

When conducting a comparison of the wireless access point security features it is necessary to determine what the wireless security issues are and what security features will provide protection against them. When it is know what security capabilities are needed we will review the two wireless access points' security features and compare their capabilities and configurability.

2.2.1 Wireless Security Issues

A wireless access point should have the capability of being set up as securely as possible. Following are a list of four wireless security issues and the security features that are needed to mitigate the risk of these security issues:

1. Eavesdropping - In a wireless environment it is very easy for to do. Wireless receivers are cheap and easy to get. To make matters even worse it is almost impossible for the homeowner to detect if someone is eavesdropping as they can be hundreds of feet away. To mitigate the risk of eavesdropping the following security features should be used:
   - **Direct Sequence Spread Spectrum** (DSSS) chops the transmission signal into small pieces and spreads the pieces across the frequency domain. The algorithm used to break up the signal uses a unique spreading code. Only the receiver that knows the unique spreading code can recover the code in a readable format. An unintended receiver sees only a low power background noise and it is usually ignored. The problem with this signal modulation technique is that it is susceptible to noise corruption. Because of this DSSS generates redundant signal pieces to allow for recover of the signal if part of the data is loss.
   - **Encryption** in simple terms means scrambling the data with a secret key at the sending end and unscrambling the data with the same key at the receiving end. The 802.11b wireless standard encryption method is called Wired Equivalent Privacy (WEP). WEP uses an RC4 Key Scheduling algorithm which has been found to be easy to break. It has also been found that using a larger secret key does not provide any more security. Several free tools (i.e., AirSnort, WEPCrack, etc.) that can break the RC4 key are available in the Internet. Using WEP will keep the casual user from being able to read your data. Other encryption methods, such as IPSec, SSL, and SSH should be used to help secure the data. Any connections used to access your business should go through a VPN.
   - Authentication and access control should be used to keep unauthorized users from connecting to the network. The **Service Set Identifier (SSID)** is used like a password to access the wireless network. The wireless access point can also use a **Media Access Control (MAC)** address to control access to the wireless network.
   - **Disable the SSID broadcasting** feature to prevent an attacker from obtaining the SSID. The attacker needs the SSID to be able to access the wireless access point.
2. Theft or loss of wireless devices - This is a risk for both wired and wireless networks. We are limiting this risk to the loss of a laptop as it is more mobile than a PC and Personal Digital Assistants (PDAs) are not part of this wireless

network environment. If a laptop is lost or stolen the encryption keys on the wireless card and any other data on the computer can be accessed by the person that recovers the computer. With that information that person could then access your wireless network. To mitigate the risk of losing a laptop, the following security features should be used

- Use a laptop cable lock if the home laptop is taken outside of the home.
- Set up the laptop to require a password to log on.
- Encrypting the data on the laptop could be done, but that is beyond the scope and resources available for my home wireless environment.

The wireless access point stays in the home so no extra precautions are needed to prevent its loss.

3. Denial of Service (DOS) - Wireless networks are very susceptible to DOS attacks because the attacker can jam the wireless signals with massive radio interference if they have a transmitter that is powerful enough. The person trying to jam the wireless signal could be hidden in a vehicle near your house. In addition, the transmitter that would be needed to generate the attack is cheap and is easy to set up. Unintentional jamming could be caused by electronic devices within the home such as a motor, monitors, or 2.4 GHz telephones. To mitigate the risk of DOS the following security features should be used:
   - Shield the home. This option is too expensive and impractical for this homeowner. Usually an attacker would not keep the jamming up for long periods of time. It is more likely that a business would be targeted for jamming than an individual homeowner.
   - Change the location of the wireless access point. If the DOS is caused by electrical equipment in the home, the homeowner should change the **location of the wireless access point** to move it away from the electronic equipment affecting it.
4. Masquerading - In this type of attack, the hacker makes their computer look like it is a legitimate user of the network. This can be accomplished two different ways.
   A) Obtain the wireless access point's SSID and then request an IP address for the attacking computer. The DHCP servers on the wireless access point do not normally authenticate the user and provides the attacking computer with an IP address. At this point, the attacker's machine is on the network and can communicate with the other computers in the network.
   B) Set up a rogue wireless access point that looks like the homeowner's wireless access point. If its signal is stronger than the homeowner's, then the homeowner's computer will attach to the rogue wireless access point. The rogue equipment could store information that is sent over it.

   To mitigate the risk of masquerading the following security features should be used:
   - To prevent this type of attack the **wireless access point must be set up to authenticate the computer before it allows the connection**. The Media Access Code (MAC) address can be used for this. The "MAC address is a unique number that is assigned by the manufacturer to any Ethernet networking device that allows the network to identify it at the

hardware level." [8] The access point can be set up to allow connections only with certain MAC addresses. This will help keep your neighbors or casual hackers off, but serious hackers will know how to get the MAC address and set up their computer to spoof the MAC address.

- The wireless access point SSID should be changed from the default setting. The SSID functions as a password for joining the wireless network. All of the packets contain the SSID in the header.

2.2.2 Default security settings for each access point

Linksys default setting:

- 64 Bit encryption, (turned off)
- the Passphrase field is empty (used to generate encryption keys)
- The SSID is “linksys”
- Channel is set to 6

D-Link default settings:

- Encryption turned off
- The SSID is “default”
- To allow traffic from the Internet to enter your local network, you will need to open up ports or the router will block the request.
- Channel is set to 6

2.2.3 Security capabilities of each access point equipment

	D-Link AirPlus DI-614 (www.dlink.com)	**Linksys - BEFW11S4 Ver 2** (www.linksys.com)
802.11b	Yes	Yes
Encryption	64/128/256 Bit WEP	64/128 Bit WEP
NAT	Yes	Yes
Mac Address filtering	Yes	Yes
IP Address filtering	Yes	Yes
Port filtering		Yes
URL / Domain Name Filtering	Yes	
Domain Blocking	Yes	Yes
Supports IPSec & PPTP Pass-through	Yes, & , L2TP	Yes
DMZ Hosting	Yes	Yes
Configured to filter internal users’ access to the Internet.		Yes
Change SSID name	Yes	Yes
Remote access via VPN	Yes	Yes
Disable SSID broadcast	Yes	Yes
Signal Modulation	Direct Sequence Spread Spectrum (DSSS)	Direct Sequence Spread Spectrum (DSSS)
Range:		

Indoors	328 ft	300 ft
Outdoors	1,312 ft	1,500 ft

2.2.4 Decide which access point to purchase

Both devices have the following security capabilities which are needed to defend against the Section 2.2.1 Wireless Security Issues:

- WEP encryption
- DSSS
- SSID authentication
- MAC address filtering
- Ability to disable the broadcasting of the SSID
- Supports IPSec and PPTP Pass-Through by allowing the homeowner to access their network remotely over the Internet through a Virtual Private Networking (VPN).

Other security capabilities that both wireless access points provide are as follows:

- Network Address Translation (NAT) which protects the user from outside intruders gaining access to the user's private network. The wireless router interfaces the Internet with the public IP address. It assigns private IP addresses to the computers inside the router's network. The private IP addresses cannot be seen from the Internet. NAT is used to secure wired and wireless networks.
- Multiple and concurrent IPSec, L2TP, and PPTP sessions so multiple users behind the DI-614 + router can securely access corporate networks through various VPN clients.

D-Link AirPlus Wireless Network DI-614

- Provides a firewall that supports content filtering based on MAC address, IP address, URL and/or Domain Name via the Freedom firewall.

Linksys EtherFast® Wireless AP + Cable/DSL Router supports the following:

- Use the ZoneAlarm Pro* (firewall) and PC-cillin software (antivirus software)
- The ZoneAlarm can be configured to filter internal users' access to the Internet.
- Provides a capability to do port filtering.

Upon a direct comparison of the two devices there is not an appreciable difference in their security capabilities. Initially the decision was made to use the D-Link AirPlus Wireless Network DI-614+ router as it allows the use of a larger encryption key for the WEP and the D-Link data rate is twice as high as the Linksys device. In addition, my computer is already configured with the ZoneAlarm Pro firewall which provides most of the other differences

2.3 Implement wireless network environment

2.3.1 Determine location to place wireless access point

The location of the wireless access point (WAP) is important. It can affect how far the wireless signal travels and where the computers can get the signal within the house. When determining where to place the WAP one must try to get the signal to go throughout the house but at the same time try to limit how far the signal travels outside the house.

My wireless network was installed in a single family home which is located on one acre of land. This will allow a little leeway in the placement of the WAP as the neighboring houses are not immediately adjacent to the house. In addition, the house is built of block and brick which should further limit the distance the signal can travel outside the house.

The higher the WAP device is located in the house, the farther the wireless signal will travel. I have decided to place the device in the basement. This has the added advantage that the basement is surrounded by dirt and slate which should limit the wireless signal from traveling in a horizontal line outside of the home. The disadvantage is that the WAP device is next to an outside wall so the signal has to travel almost 100 feet to reach any wireless computer that is located on the other side of the house. The number and types of objects that the signal must pass through may further limit the range. Walls that are at an angle will also appear denser to the signal. This will lower the data rate on those Internet connections. Within the house, electrical devices, such as 24 GHz wireless phones, monitors, microwaves, UPS units and motors may also interfere with the wireless signal. The Wireless access device should be kept at least 3-6 feet away from the electrical devices that are generating RF noise. [15]

2.3.2 Install and secure the wireless access point

Before powering up the wireless device, one must hook up the wireless access point to the cable modem and the PC with RJ45 Ethernet cables. The power now can be turned on to the wireless access point and the PC that will be used to configure the wireless router. Each vendor provides specific instructions for the installation of their products.

Before making any changes to the router the PC network settings must be configured to get an IP address automatically because the cable modem requires the use of DHCP. For Windows 2000

1. click the ***START*** button
2. click ***Setting***
3. open the ***Control Panel***
4. double-click ***Network and Dial-up Connections*** icon
5. double click ***Local Area Connection*** icon
6. click the ***Properties*** button
7. select Internet ***Protocol (TCP/IP*)**
8. click the ***Properties*** button

9. select ***Obtain an IP address automatically***
10. click the ***OK*** button
11. restart the PC

The next step is to access the router and configure it to get access to the Internet through the cable modem. The steps will differ depending on the wireless access point device that is used, but all allow for setting up a user name and password authentication to the unit. Other items that can be configured are the Service Set Identifier (SSID), a unique name for the wireless network; input a static IP address if you are assigned one or select the dynamic IP option, encryption level via WEP; select a channel; and enable/disable SSID broadcasts.

Most of these items need to be changed from their default mode to provide multiple layers of security after the wireless network connections have been made.

2.3.2.1 Change SSID/Disable SSID Broadcasts

After the wireless network has been installed the wireless router configuration should be modified to change the default name of the SSID. This will prevent the casual wireless users that are using their default SSID from accessing your wireless network by mistake.

Most wireless access points broadcast their SSID by default. The broadcast function should be disabled to make it harder for the war driver to find the wireless network.

Another measure of security for a wireless network SSID name is it to periodically change the SSID name. This should be done at least once every 120 days or if you suspect someone has discovered your SSID name.

2.3.2.2 Change the default password for the Administrator account.

The password used to log onto the wireless device has administrative permissions. After the wireless network environment has been established the password should be changed. The wireless access point configuration settings (SSID, WEP keys, etc.) are stored in the firmware of the device. If a hacker finds the administrator's password, then he will be able to change the configuration of the device. The administrator's password should be changed on a regular basis, at least once every 120 days.

2.3.2.3 MAC Filtering

Enable MAC Address filtering. MAC Address filtering will allow the user to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

At this point the D-Link installation wizard will ask for the network adapter in the users computer. Each network adapter has a discrete Media Access Control (MAC) address

2.3.2.4 Set up WEP

Wireless networks are vulnerable to eavesdropping. Anyone who has a laptop with a wireless card can scan for wireless access points, intercept the wireless transmissions and get onto the Internet from it via DHCP client software. For my purposes, I will enable WEP 128-bit Encryption. Encrypting the data going across the network will keep the casual observer from seeing the data.

Wired Equivalent Privacy (WEP) is the encryption protocol provided by the 802.11 standard. Security goals of WEP are confidentiality, data integrity, access control. The main objective of WEP is to protect data transmitted within a WLAN from eavesdropping. WEP uses the RC4 encryption algorithm to encrypt the data. RC4 is a symmetric algorithm. A symmetric algorithm relies on a single shared key that is used at one end to encrypt plain text into cipher text, and decrypt it at the other end. The sender and the receiver use the same secret key.

A determined hacker can pull off and save enough data to run a cracker program against it, get the encryption key and then decrypt the data. Setting up WEP encryption will slow down the response that you receive from the Internet

WEP encryption is weak but it is better than letting the data go in the clear. At least the hacker will have to make some effort to read your data. The user has to input a 58 HEX character key onto the wireless access point and the wireless card device located on the PC.

Due to weakness in WEP encryption the WEP encryption keys should be changed at least every 120 days or if I suspect someone has gotten access to my wireless network.

2.3.3 Secure the wireless client

The wireless client is the home PC or laptop. After the wireless access point is installed the wireless card on the PC or laptop will be installed and configured. The card SSID, channel number and the WEP encryption key is configured to match the Wireless access point.

After loading the wireless drivers and making several changes to the PC you need to determine that the computer's software still has the most current software service packs and security patches. To do this, I logged onto the Microsoft web site, http://v4.windowsupdate.microsoft.com/on/default#.asp. From there ran the option to search for Windows 2000 applications that need to be updated. It showed that my system was current with all of the service packs and security patches.

2.3.3.1 Configure client platform

To limit the damage that a hacker could do to a PC turn off file and print sharing. That way if a hacker gets into your wireless network they will not be able to access your files.

In addition I have turned off the LAN settings:

1. Double-click ***My Computer***

2. Double-click ***Control Panel***
3. Double-click ***Internet Options***
4. Click the ***Connections*** tab
5. Check ***Never Dial Up a Connection***
6. Click the ***LAN Settings***
7. When the Local Area Network (LAN) Settings window appears, **uncheck all boxes**
8. Click the **OK** button
9. Click the **Apply** button if necessary
10. Click the **OK** button
11. Exit the Control Panel and restart the computer

2.4 Lessons Learned on Actual Wireless Network Installation

When initially installing the D-Link wireless router I changed the SSID name, channel, and turned on WEP at the 256 Bit key encryption level. Then I installed a D-Link wireless card driver on my laptop using the CD that came with it. When I tried to change the configurations on the D-Link wireless card to match the wireless router, I was unsuccessful. The software would not allow me to change anything and the wireless card could not find the wireless signal. After calling the D-Link vendor for technical support I was told the latest Windows 2000 service packs would not work with the D-Link software. The vendor support technician had me try to de-install the card driver using the Windows software de-installation application. The de-install was unsuccessful and the message "access denied" was displayed on the screen. The de-install had deleted some of the files but not all of them. After this the CD could not reinstall the driver. The D-Link vendor support was not able to resolve the problem. At this point I had two options: rebuild my PC or use the Linksys Wireless Access Device.

I decided to use the Linksys wireless access point. The PC network configuration changes made earlier for the D-Link device did not need to be changed, they were the same for both devices. During the initial Linksys installation the default configurations on the wireless router were used so there would be fewer changes that could cause the problems and it would be easier for the tech support team to help. I did not change the SSID name, the Channel number, did not enable WEP encryption and did not disable the SSID broadcast. I decided to use the laptop's wireless receiver because it was already installed and should work despite the updates that were made to the Windows software. Next I set up the laptop wireless card to find the default Linksys wireless signal. I called the laptop vendor technical support to help get the wireless card working. They were very helpful and told me how to turn on the wireless card and change the card configuration. I set the network field (SSID) to "any" and it could find any wireless network signal that was available. The wireless card was successful in finding the wireless signal. Then I logged back into the Linksys wireless access point and changed the default Linksys SSID name, changed the channel number, turned off the SSID broadcast and turned on the WEP encryption. Then I went to the PC wireless card configuration and changed it to match the wireless router.

There were additional problems encountered during the installation of the wireless network. I could access the wireless network during the day, but in the evening when I tried to log onto the Internet I would receive the message that the IP address could not be found. I kept looking at my configuration settings to try to determine what was wrong. This happened several times before I realized that the cable Internet provider's bandwidth was being overloaded and I could not get a good enough signal to log on. To test that the access problem was not being caused by electronic noise I hooked the computer to the wireless access router via an Ethernet cable.

3 Testing the wireless environment security

After making so many changes to a computer and setting up a wireless high-speed connection to the Internet, tests should made to determine the security of the computer and network environment.

After loading new software and making configuration changes users need to ensure that existing files have not been replace with older versions. Additionally, they need to determine if the location of the wireless access device limited the outside range of the signal. The final test requires running a third party software tool that scans the new wireless network and reports on existing security vulnerabilities that were found.

3.1 Scan the PC

HFNetChkLT is a software tool that is used by many security analysts to scan systems to determine if any security patches are missing. It then allows the person performing the scan to update the patches and service packs. HFNetChkL was loaded onto the laptop, which also required the application Microsoft Data Access Components (MDAC) to be loaded. HFNetChkLT (www.shavlik.com) ran a scan against my PC. It reported my PC was missing seven patches. Two of the missing patches were for the new MDAC application that had just been installed with the HFNetChkLt download. MDAC was needed for HFNetChkLT to perform its scan.

The same Microsoft tool that was used earlier to scan the PC, before the wireless environment was set up, was used to scan the PC again. It found three critical updates were missing. It also found some other vulnerabilities that were less severe.

Both scanning tools found most of the same missing patches. The patches were installed.

3.2 Discover the range of the wireless access point

To test for my wireless signal I used my evaluation laptop with the wireless network card turned on. The wireless card software provided a link check function that showed what the data rate being used and if packets were being lost. I walked around the inside of my house and was able to access the wireless network from everywhere in the house. On the side of the house farthest away from the wireless access point, the data rate went down but the Internet connection did not go down and packets were not lost.

To determine how far the signal reached outside the house, I walked around the outside of my house with my laptop wireless card turned on. I found that I was able to walk all the way to the back of my yard, about 100 feet, before I lost the signal. At 50 feet from the back of the house, the signal data rate was greatly reduced and the line test program showed packets being lost. My driveway which is on the side of the house farthest away from the access point did not get a signal. In front of the house, I found the signal up to 100 feet from the house. The same held for the side of the house closest to the wireless access point.

When I tested for the distance of the signal, I used the wireless card with the configurations that matched the wireless access point. Next I changed the wireless PC network card configurations. I turned off encryption and set the SSID to "any". With these settings I was not able to access the wireless network.

3.3 Run the third party tools to try to sniff the wireless network and try to break in.

As a further test of the security of my wireless network I want to have a third party scan my network from the Internet. I selected a free third party scanner tool called QualysGuard located at URL http://qualys.com/. It is provided by Qualys Inc. The free scanner looks for the SANS/FBI top 20 vulnerabilities and then provides a report on the scan results.

To sniff a network from the outside requires the public IP address provided by the Internet Provider to the Wireless Access Point. To get the IP address requires logging onto the wireless router. For the Linksys router select the **Status** folder and the IP is listed on this page.

The scanner looked for the following vulnerabilities:

- NETBIOS - unprotected Windows Network Shares
- Anonymous Logon - NULL Sessions
- General Windows Authentication - Accounts with no or weak passwords
- Remote registry access

The results of my scan showed that my wireless network did not have any known security vulnerabilities.

In the results report I, was given the option to test my web browser for further vulnerabilities. As all Internet connections, wired and wireless, use the browser, I decided to run the test to determine if I had browser vulnerabilities. It tested for the following vulnerabilities:

- Cookie disclosure - "If the browser and firewalls are not secured a hacker could obtain cookies that are stored on your browser. With your personal information a hacker can pose as you to a web site." [13] My browser tested secure for this vulnerability.
- Clipboard reading -" the browser allows Web applications access to data copied on your clipboard. There is no vendor solution for this problem at this time. To

eliminate this vulnerability select **Internet Options** from **Tools.** Select the **Security tab.** Click on **Custom Level** and then select **Disable** under "Allow paste operating via script." [13] My browser had this vulnerability so I followed the instructions listed above to correct the problem.

- Program Execution - "tests if the browser allows the attacker to launch applications that are currently on the computer." [13] My browser would not let a program be launched by a hacker.'
- File execution -" tests if the attacker can open random files on the computer by tricking the browser into thinking it is safe to open." [13] My browser was found to be vulnerable to this attack. Patch MS02-047 needs to be installed.
- Web Page Spoofing -" This is an attacker impersonating a well-known web sites. The user may provide confidential information to the web site." [13] My browser tested safe from this vulnerability.
- Security Zone Spoofing -"An attacker puts malicious code into a URL that will open a window with the highest privileges." [13] My browser tested safe from this vulnerability.
- Hard Drive Access - "The attacker is able to read, write or edit data on my computer." [13] My browser tested safe from this vulnerability as Active scripting was disabled on my browser.

4 Conclusion: How secure is the new wireless environment

The final results of this test showed that my wireless signal is available to at least 100 feet outside of my home. This means that a hacker can sniff my signal. However my neighbors will not be able to access my signal, as they do not know the SSID name and the encryption keys that I have set up on my wireless access point.

The scans of the PC found some additional missing security patches. The vulnerabilities this created were not serious and the patches were installed to fix the problem. This shows that new vulnerabilities are discovered and patches are written to fix them almost every day. In addition, every time a new program is installed there is a potential of overwriting a file with an older version of the file that needs a patch that has already been installed. The third party scanner showed that most of the known security vulnerabilities had been fixed. For those that had not, instructions were provided to fix the problem. The vulnerabilities tested for effect both wired and wireless networks. To mitigate the risk of these vulnerabilities everyone should check for new patches and run third party scanning tools to find security vulnerabilities against their network on a regular basis.

In the home environment it is not possible to eliminate every risk that is created by being on the Internet via a wired or wireless network, but the homeowner can defend against some of these risks by securing his/her PC and wireless access point. If a homeowner makes the changes as outlined in this paper the home wireless network will be more secure from inadvertent access by their neighbors or recreational hackers, which are the most likely risk in a home environment. A serious hacker is more likely to try to hit a business where access to more computers and information is available. However, financial or personally sensitive information should not be loaded on a

computer that is used to access the Internet. That is information that I do not want to take any risk of someone getting without my permission. With this final risk mitigation factor I will continue to use the wireless network.

References

1. Alamgir, Nuruddin, "Insecurities of WEP and Securing the Wireless Networks", June 5, 2002, URL: http://www.giac.org/practical/nuruddin_alamgir_gsec.doc

2. Zone Alarm URL: http://www.zone-alarm-pro.com/

3. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*. November 2002

4. Linksys URL: http://www.linksys.com

5. D-Link URL: http://www.dlink.com

6. National Security Agency, *The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment*), Systems and Network Attack Center (SNAC), October 16, 2001, Version 1.0

7. Johnston, Michelle, **"**Homeland Security Starts at Home – Security for the Home Computer User" March 25, 2002, URL: http://www.sans.org/rr/homeoffice/homeland_sec.php

8. "Linksys Wireless Access Point Router with 4-Port User Guide",

9. "VPN and Wireless Security", URL: http://www.linksys.com/edu/vpnwireless.asp

10. Posluns, Jeffrey, **"**Wireless Communications Technologies: An Analysis Of Security Issues", April 26, 2001, URL**:** http://www.sans.org/rr/wireless/sec_issues.php

11. Mannion, Patrick, "Cipher attack delivers heavy blow to WLAN security", EE Times, http://www.eetimes.com/story/OEG20010803S008, dated August 6, 2001

12. AirSnort URL: http://airsnort.shmoo.com/

13. Qualys URL: http://qualys.com/

14. http://www.zdnet.com.au/reviews/software/security/story/0,2000023554,20269579-8,00.htm, ZD Net Australian Reviews

15. D-Link Tech Support: URL: http://support.dlink.com/faq/View.asp?prod_id=822

Last Updated: May 22nd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 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 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 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
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
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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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