2004

Evaluating the Usability and Security of Wireless Networks

George E. Danilovics III

Evaluating the Usability and Security of Wireless Networks

By

George Edward Danilovics III

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

October 8, 2004

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: George Edward Danilovics III

Thesis Title: Testing the Security and Usability of Wireless Networks in Business Data Communications

Thesis Committee

Name	Signature	Date
Prof. Bruce Hartpence Chair		10-24-04
Prof. Sharon Mason Committee Member		11-16-04
Evelyn Rozanski, Ph.D Committee Member		10-24-04

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Information Technology

Evaluating the Usability and Security of Wireless Networks

I, George Edward Danilovics III, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: 12/08/2004 Signature of Author:

Table of Contents

Table of Figures

I. Introduction

Determining security measures for a wireless network is no different than determining a strategy for traditional wired networks. Network administrators survey the possible exploitations that a hacker could use and than determine which measures would protect from such attacks. A network administrator must weight the risk associated with the attack against the costs of protecting against the attack.

Many articles have recently been published about both the perils and promise of wireless networks. Increased worker productivity, ubiquitous network access, and instant gratification are just a few of the benefits employees can utilize with a wireless network. These articles also discuss many of the vulnerabilities of wireless networks, with topics ranging from AirSnort to WEP cracking.

In order for wireless networks to be effective in business those that deploy them must determine the expectations of the wireless network and then take into account the risks associated with that type of network deployment. Vendors in the software and hardware industry have filled the market with proprietary products that can allow the deployment of wireless networks. This paper will not explore the many proprietary solutions on the market. While these networks will function using a specific vendor's product they do not remain accessible by another manufacturer. A wired network allows different operating systems, different network card adapters, and different network connectivity hardware to communicate and so should a wireless network.

The primary goal of a network is to get data from one point to another, and a secure network ensures that the data transmitted does not get intercepted en route. An important feature of a secure network is that only authorized devices or people could gain access to receive and transmit data. Wired networks use switches to limit a packet's exposure on the network and eavesdropping is difficult, but not impossible, through wiretaps. A packet on a wireless network travels out in all directions as far as the sending device is capable of transmitting.

Security must also be weighed against usability. A highly secure network could require fourteen random character user passwords and biometric identification. While this network would be secure it would not be useful to many people and would probably be overkill for most business applications. A wide open, truly plug and play network would allow anyone access to anything. Employees can access all the data they need for their job, but attackers would also enjoy this unfettered access. Network administrators have to keep the usability of the network in mind when devising security measures to counter the risks to the network.

This paper will explore the some of the risks that accompany the use of wireless networks. Six different scenarios will be presented. The first will be a wireless network with no security measures in place. The second scenario will introduce security measures controlled by the network hardware. The third scenario will use security designed specifically for wireless networks. The fourth scenario will use only security measures offered through operating systems. A fifth scenario will employ a third party to control

security of the network. And a final sixth scenario will use all three: operating system, network, and third party security measures. Each scenario will also check vulnerabilities to network clients, servers, and to the packets being transmitted. Following manufacturer instructions the security measures will be implemented by computer literate testers that have no specific wireless security training. The same group will also rate the end user accessibility of the network. At the end of this paper network administrators will have an understanding of the risks associated with wireless networks and the costs of implementing security measures to reduce those risks.

Wireless technology has developed rapidly during the time this paper was being written. This paper was written using the technologies available during the summer of 2003. Advanced security measures such as WPA and 802.1x are not included in the body of this paper but are briefly described in the Appendix. Methods of breaking into wireless networks have also matured along with security. This paper looks at exploits that were commonly available during the summer of 2003.

II. Wireless Network Attacks Explained

Wireless networks by default are insecure. The same network features that allow users to roam from room to room and not lose connectivity allow hackers access to that same network. Wireless network attacks attempt to view the data being transmitted over the air and gain access to the wired network and its resources.

The first step in hacking a network is reconnaissance. Wireless networks freely give out their system service identifiers (SSIDs). In order for a client to connect to an access point the client must know the SSID of that access point. By default access points broadcast their SSID into the air so that clients can determine which access points are within range that they can connect to (Linksys 12). Linksys, for example, sets the default SSID for all their networking hardware – access points and client adapters – to 'linksys'. This practice allows a network administrator to simply plug in and turn on any Linksys device and they will automatically be able to communicate with each other. In addition to being broadcast by the access point, every wireless packet contains the SSID in plain text (Wi-Fi Planet).

Netstumbler is a free tool available for network administrators to test the strength of their access point signals. This tool also doubles as a first strike weapon that allows hackers to find the SSIDs of access points. As shown in Figure 1, Netstumbler lists the access point's MAC address, the broadcasted SSID as well as determining if Wired Equivalent Privacy, WEP, encryption is used for communication.

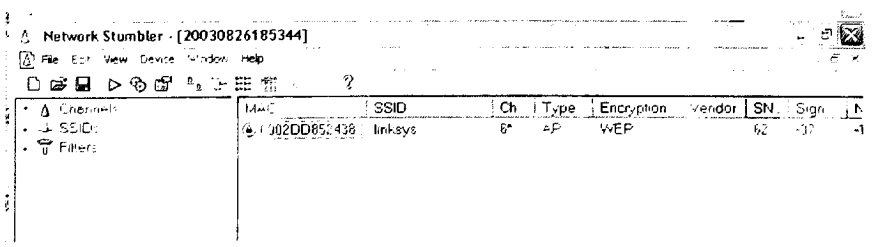

Figure 1 Netstumbler locating access points

Once a hacker has the SSID used for communication the next step would likely be the capturing of packets. Ethereal is another free tool that can aid administrators in

diagnosing network problems and also give hackers an eye on what is being transmitted through the air. If no encryption is used Ethereal can view everything in the packets: including usernames and passwords. This is not an exclusive vulnerability to wireless networks however. A telnet username and password can just as easily be picked up on a wired network if no encryption methods are used. Figure 2 shows a decoded TCP stream from an Ethereal capture. The capture was of a telnet session from the wireless client to a server running a telnet service. The login name 'administrator' and password 'rochester' are clearly visible.

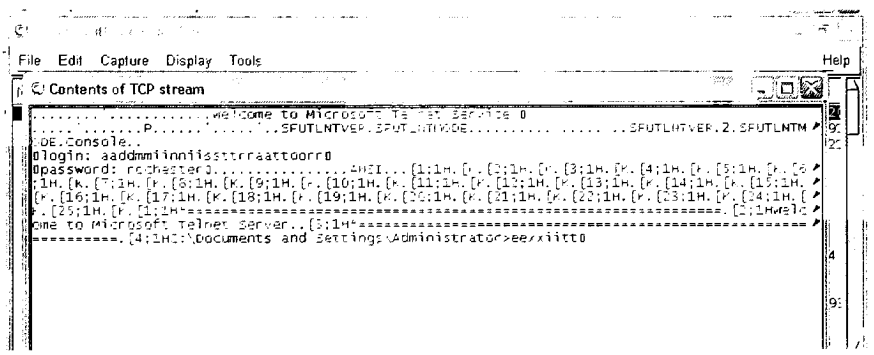

Figure 2 Decoded unencrypted telnet session

If the wireless packets are encrypted by Wired Equivalent Privacy, a very basic encryption algorithm, a casual hacker might be deterred. Access points that use WEP are identified by Netstumbler. WEP encrypted packets in Ethereal show up as a myriad of LLC packets. A capture of a WEP encrypted data stream is shown in Figure 3. Although a few research papers have been published about the breaking of the WEP key algorithm, the actual decryption of packets has not been easy to replicate.

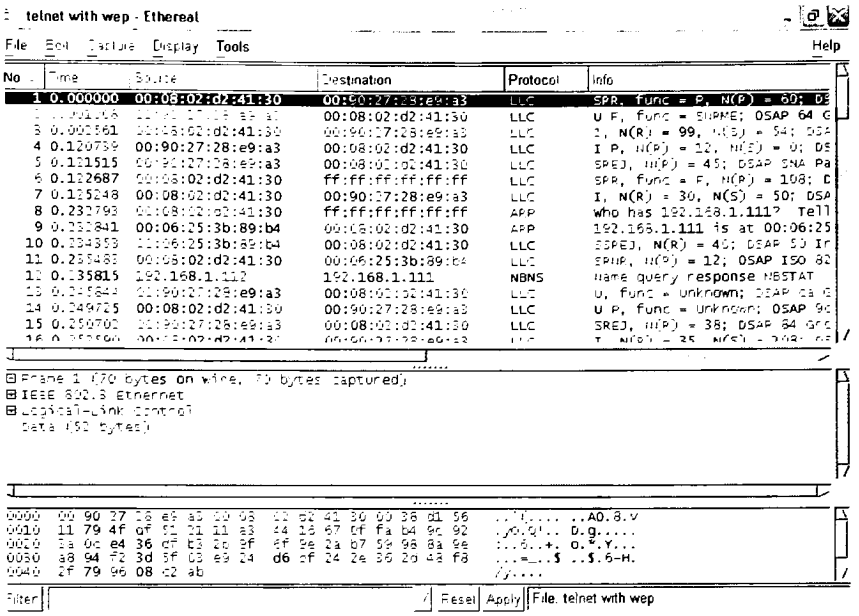

Figure 3 WEP encrypted telnet session

Using a passphrase of 'hello' and a 64-bit encryption option generated the four keys on the Linksys wireless router. The key value is then entered into the wireless client to gain access to the network. Multiple repetitive ping requests were sent from the wireless client to a wired network host. Then, on a separate wireless client that did not have the WEP key value packets were captured into Ethereal. Airsnort, one of the free tools that claims the ability to break the WEP key algorithm, recommends capturing 5 million packets for a sample size for cracking. Once the Ethereal capture hit 5 million packets the capture file was loaded into Airsnort. The program identified the MAC addresses of the hosts, but after running 72 hours the program was unable to reveal the WEP key used. An independent study done by Rochester Institute of Technology students Collins and Reznik also experienced difficulties in using Airsnort to break WEP (Collins and Reznik 7). Fluher, Martin, and Shamir published a detailed analysis of the

RC4 algorithm that is used in WEP encryption. Their paper outlines the technical workings of the algorithm and how a program could, if it had enough packet samples, break the WEP encryption and view the encoded data. No media announcements have been made about a breach in WEP that resulted in a hacker breaking into a wireless network. This should not lead administrators into a false sense of security. The Fluher report gives the technical details to beat WEP that only need better implementations than WEPCrack or AirSnort.

Another basic level of defense is MAC filtering on the access point. This filter is a simple list of hosts that are granted or denied access through the access point. By capturing packets a hacker can see which MAC addresses are allowed to communicate through the access point (SyDisTyKMoFo). Once that host has left the network, the hacker can assume that MAC address using a MAC address masking tool and gain access past the MAC filter on the access point. If the hacker were to assume the MAC address while the host is still communicating a denial of service attack would take place. Figure 4 is a screenshot from SMAC showing how the simple interface allows the spoofing of MAC addresses. Hosts on the local wireless network communicate via MAC addresses and a segment having duplicate MAC addresses would prohibit reliable data transmission.

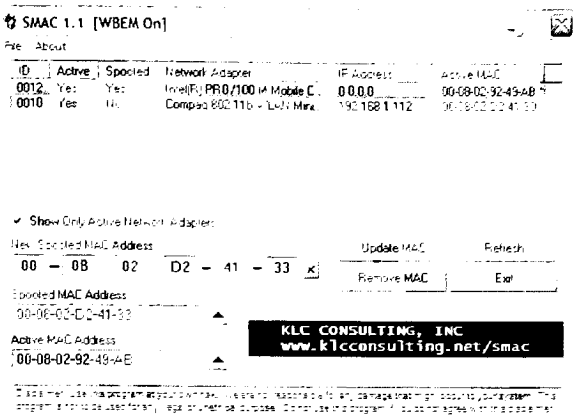

Figure 4 SMAC MAC address spoofing

The final type of attack wireless hackers can attempt is a man-in-the-middle attack. In this type of attack the hacker positions himself in the middle of the transmission stream, reading packets from one host and forwarding them on to the next (Fleck and Dimov). Ettercap is another freely available tool on the Internet that allows the forging of network packets. Local Area Network communication between hosts is based on MAC addresses. Ettercap allows the creation of ARP replies with forged IP to MAC address pairings (Ettercap). In the test network, the default gateway on the network is 192.168.1.1 with a MAC address of 00:06:25:A3:E6:F2 as shown in Figure 5.

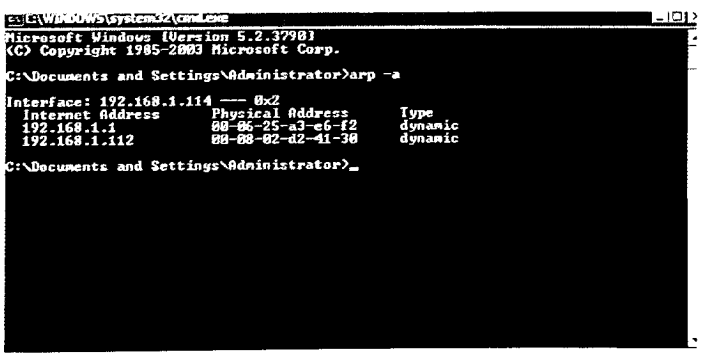

Figure 5 ARP cache on host before ARP poison attack

After using Ettercap to send a forged ARP Reply to the host any communication that the host would send to the gateway will be directed through the rogue machine. More advanced software would be needed to read incoming packets and reassemble them to be sent out on the wire and avoid detection by the hosts, but this quick and easy attack could disrupt network communications until discovered. Notice the spoofed MAC address for 192.168.1.1 now listed in Figure 6.

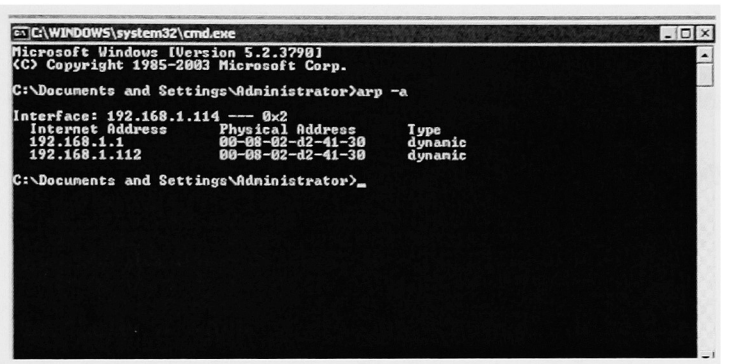

Figure 6 ARP cache on host after ARP poison attack

III. Layers of Protection

The first layer of protection involves the MAC address of the wireless hosts. Access points can have MAC filter lists that permit or deny communication based on the MAC address of the host. This basic level of protection will only stop casual hackers and would be sufficient only for home office networks. Public hot spots could only use this method effectively if the access point allowed dynamic assignment of valid MAC addresses. Corporate environments could use this layer of protection as long as the list of hosts does not change frequently: having to manually add and remove hosts for a lookup table would be a tedious and time consuming job for a network administrator. MAC

filtering should not be relied on as the sole method of defense due to the ease of MAC address spoofing demonstrated in the previous section. MAC filters should only be used in smaller static networks and not used as the only method of protection.

The next method of protection is the encryption of the data transmission. Wired Equivalency Protocol (WEP) uses a shared key to encrypt the data. WEP defines the use of a shared key to encrypt data, but does not define key management. WEP allows both a 128-bit key or a 64-bit key for encryption. The access point and all wireless hosts must use the same key in order to communicate, but unfortunately the same method that breaks the 64-bit key also works on breaking the 128-bit key (Vaughan-Nichols). This is because each packet is encrypted with the same RC4 cipher. Made up of a 24-bit initialization vector and the WEP key, this key is either 40-bit or 104-bit which is why documentation commonly lists the keys as 64-bit or 128-bit. Each key contains the initialization vector in plain text: the Achilles heel for WEP. Each key contains a 24-bit initialization vector with 16,777,216 possible combinations regardless of the key length (Vaughan-Nichols). Because it is possible to break WEP, other encryption methods should be used such as VPN or SSL. Using WEP is still better than no security at all.

The next approach combines authorization with encryption. Virtual Private Networks have been widely used on the Internet to allow home workers to connect to their office networks. The remote computer presents user credentials, usually a smart card or username-password combination, to a remote access server. That server then compares the credentials to an authentication database to determine if access is

authorized. The data stream is then encrypted between the client and VPN server (Webopedia). The VPN server routes traffic between the wireless client and the internal network. VPN solutions are attractive because many networks already have a VPN server handling connections from the Internet that can also accept connections from wireless hosts. The VPN solution, however, is also not a completely secure solution. Rogue access points can still infiltrate a network and allow a hacker to view traffic as it passes through. The reason for this breach is because the access point is not validated in any way – only the client's identity is tested. The traffic exposed through a rogue access point will be encrypted and this solution may be secure for most transmission needs, but the risk of a rogue access point is present in the solution.

The next sections will explore six different wireless networking solutions. Each solution will outline the steps taken by a network administrator to setup the solution and steps needed by the end user to get onto the network to gain access to a server on the wired network. The sections will also contain explanations of the problems encountered.

IV. Testing Wireless Network Topologies

Six scenarios were presented to five computer literate people to attempt configuration. The years of computer experience and personal aptitude rating are shown below in Figure 7. The testers were asked how long they have been using a Windows environment, to rate their own computer aptitude, and finally their profession. As expected a range of aptitudes was present for testing.

	Yes of Experience	Aptitude	Profession
Tester 1	8	Advanced	IT College Student
Tester 2	7	Advanced	IT College Student
Tester 3	8	Intermediate	Architect
Tester 4	8	Intermediate	Business College Student
Tester 5	5	Basic	Coffee shop Barista

Figure 7 Tester Computer Experience

The testers were given the Linksys Wireless-G user guide to configure the Linksys device and Windows Help for configuring the server and wireless client. At the beginning of each scenario the environment was set back to a default configuration. This configuration includes:

Linksys wireless router restored to factory defaults

Windows XP client without any VPN or WEP settings configured

Windows 2003 Server running Virtual Private Network and Internet Authentication Server services

Once the environment was reset to the default configuration the testers were given steps to complete in order to administratively secure the network and then to perform an end user task.

The first task in each scenario was to configure the Linksys wireless router with the appropriate security: none, MAC filtering, WEP, VPN, RADIUS support, and all combined. The second task involved getting a Windows XP client onto the now configured wireless network and accessing a file share on the server. Performing these tasks tests the clarity of the documentation as well as the usability of the web interface. If the documentation is inaccurate or the web interface is not usable, then those attempting to secure wireless networks would be at a disadvantage.

Testers were also asked questions during the process and asked to verbalize their thought process. The first question was if the Linksys would support the security measures in the scenario. The second question asks if the Linksys documentation provides any warnings along with the configuration. The documentation should reflect the capabilities of the hardware and not provide false senses of security. Testers were also asked if any feedback was presented to them when accessing the wireless network to give them information on the security of that network. The tasks and questions are listed in Appendix G.

IV-1. Scenario 1: Default Wireless Network

A default wireless network is extremely insecure and should never be used for data communications. Nothing has been changed in the wired or wireless network. There is no authorization of clients wanting access to the wired network and there is no authorization of the access points. By default the access point sends out a beacon of the SSID that can be discovered by Netstumbler as shown earlier in this paper. Data is not encrypted and the transmissions which could include usernames and passwords is easily captured.

This is the default configuration for the other tests. There was no administrative setup for the testers to perform. All five testers were able to successfully map a drive to the server from the wireless client.

IV-2. Scenario 2: MAC Filtering Only

Setting the access point to only allow specified MAC addresses is a simple first step administrators can take to allow only specified hosts to communicate with the access point. Allowed clients are entered into a lookup table on the access point and hosts wanting to communicate are compared to the list. There is no data encryption with this method so data transmissions are again susceptible to eavesdroppers. This setup is also susceptible to MAC cloning that would allow a hacker to see which MAC addresses are allowed to communicate and then assume one of those MAC address to communicate with.

Setup for MAC filtering is done on the access point only and requires no modifications to wireless hosts. An administrator logging into the Linksys access point configuration page is not automatically presented with the ability to filter based on MAC addresses. The first page displayed is in Figure 8. The Advanced tab leads to the page to configure MAC filtering.

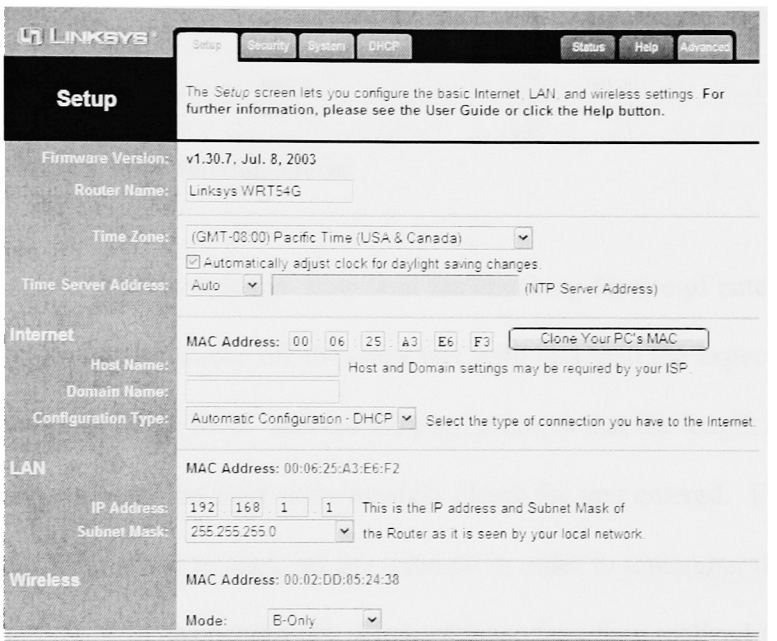

Figure 8 Linksys setup screen

The administrator is then presented with a window to enter up to 40 different MAC addresses. There are two problems with this entry page. The first is that at the top the page says to enter MAC addresses in xxxxxxxxxx format. However, after the Apply button is pressed, the MAC addresses auto format into xx:xx:xx:xx:xx:xx – shown in Figure 9. The difference in what is shown as the input mask and the end formatting could cause confusion.

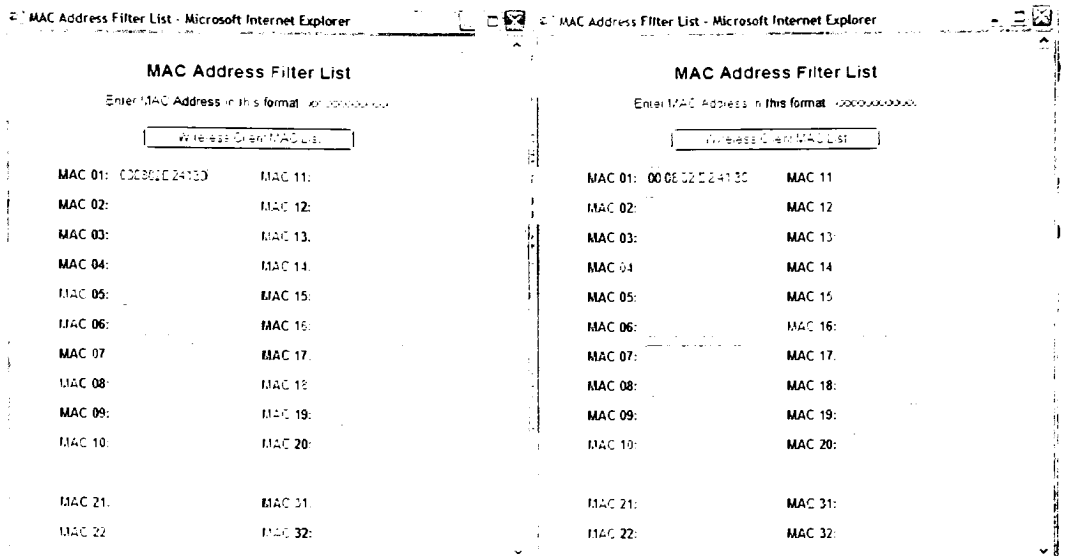

Figure 9 MAC filtering screens

The next design flaw is in the checking feature of entered MAC addresses. If the administrator clicks off the entry box with less than the expected twelve characters when entering in the MAC address the page prompts that the length is not correct. While this is a good idea, the page unfortunately clears the text entered. Four of the five people used for testing had to click off the window in order to remember the rest of the MAC address to type it in (Appendix G). Each of those four then realized they had to move the MAC filter window to the side so that they could see the MAC address of the machine they needed to add. In order to improve this entry page the check for MAC address size should be performed when the Apply button is pressed.

IV-3. Scenario 3: Wireless Network with WEP Only

WEP encryption for wireless networks should only be used for small or home office networks. The keys must manually be typed into wireless clients that want to gain

access to the access point. Although no cases of WEP being cracked have made the mass media, reports across the Internet speak to the vulnerability of the hashing code used to encrypt the data, and free tools are available online that claim to be able to break WEP transmissions (Delio).

Administrative setup for WEP first requires the entering of a passphrase on the access point which is converted into four keys that are used for WEP encryption. The wireless hosts need to know one of the keys in order to connect to the access point.

The Linksys documentation does state that using WEP encryption is highly recommended (Linksys 24). The documentation also states that using WEP can decrease transmission speeds and that a higher key bit encryption results in a slower throughput. Appendix A compares the different security measures and the transmission capacity between a wireless host and one on the wired network. The first step on the access point is not easy to find because the WEP settings are on the first page but require scrolling to the bottom of the page to find the option (Appendix G). Notice in Figure 10 that the user can not see the option to configure WEP settings.

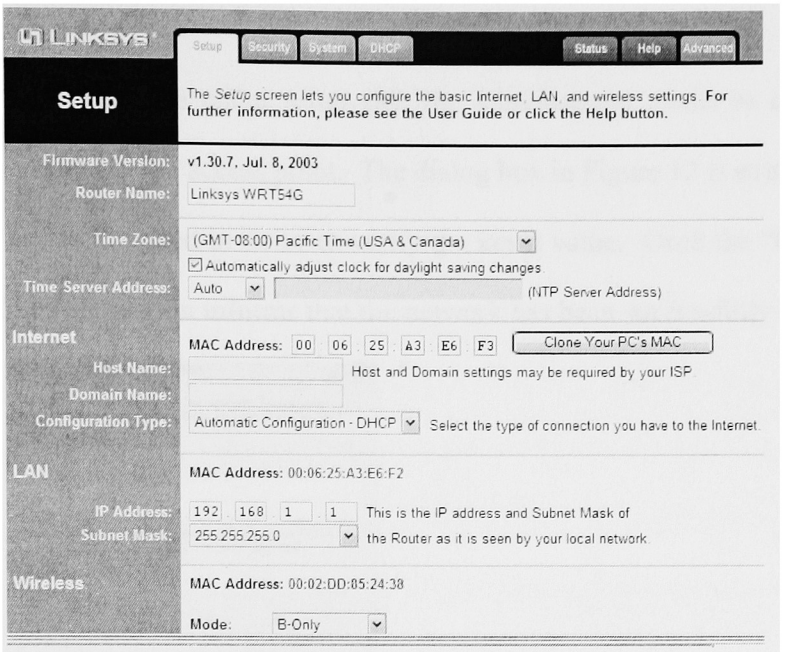

Figure 10 Cutoff setup screen

The WEP settings screen in Figure 11 is straight-forward except for figuring out how to exit after generating the keys. All five testers clicked "Apply" first after generating the keys. Two clicked "Cancel" to exit the screen, the other three clicked the X for the window to close it (Appendix G). To make this screen more user friendly the window should have an "OK" or "Close" button to use when finished entering in the WEP settings.

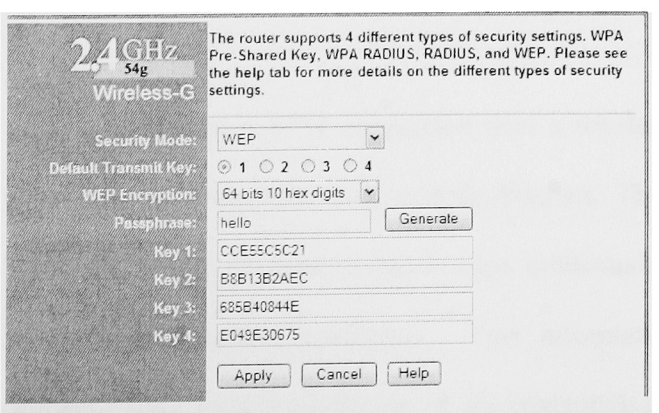

Figure 11 WEP screen with no clear exit

On the client setup side the administrator needs to enter in the key to use to connect to the access point. The dialog box in Figure 12 is straight forward asking for the key to be typed in twice to verify the key's value. Once the "Connect" button is pressed pop-up balloon informs that the network has been successfully connected.

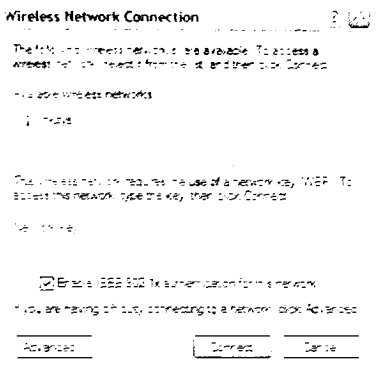

Figure 12 Windows XP prompting for WEP key

IV-4. Scenario 4: Wireless Network with VPN Only

Virtual Private Networks provide the quickest security approach for authorizing wireless clients and encrypting data. Wireless networks that use VPN as a security mechanism are potentially exposed to man-in-the middle attacks by rogue access points.

Setting up a VPN connection over a wireless network is the same as creating a connection that would be used over the Internet. The client enters in the IP address of the VPN server and presents authentication credentials in the form of a smart ID card or username-password combination. This information is sent to the VPN server for authentication and authorization. If the credentials are valid and there are no restrictions

on the account the VPN server acts as a remote access server encrypting data between itself and the wireless host and allows the wireless host access to the internal network.

The wireless access point may need to be configured to allow the unmodified passage of VPN traffic between the wireless and wired networks. The Linksys router by default allows VPN traffic to pass through, although only one person found the section in the Linksys documentation stating that VPN pass-through is enabled by default. All five testers were able to quickly find the section in the web configuration to enable VPN pass-through (Appendix G). There was no mention in the Linksys documentation about using a VPN tunnel to secure the wireless network.

None of the five testers had problems setting up the VPN connection. Four of the testers have created VPN connections before and the fifth was quickly guided through the setup armed with only a VPN server IP address and account credentials to use when logging in.

IV-5. Scenario 5: Wireless Network with RADIUS

Remote Authentication Dial-In User Service is an open standard used to authenticate remote users to the local network. RADIUS includes authentication, authorization and accounting all of which are controlled at a central location. The advantage of RADIUS authentication is that the process can include a wide variety of authentication methods to a centralized user database (Backman). The advantage of

using RADIUS for authorization over MAC filters is that a remote access policy can be centrally controlled. A large corporation with multiple access points would require adding all wireless hosts to the MAC filter lists. Using RADIUS would only require configuring the access points to defer authorization to a RADIUS server. The RADIUS server checks the remote access policy which could allow account access based on group memberships or even time of day. RADIUS also offers accounting to measure how long users were connected and report this to a central repository. While none of the five testers had configured Microsoft's Internet Authentication Server before, they all easily walked through the configuration of an IAS client to accept requests from the access point.

Setting up the Microsoft IAS for wireless use is no different than any other remote access use. The IP address of the client, the access point's address, and a shared secret that is used by the client and IAS server to encrypt communications during authentication and authorization are entered into IAS.

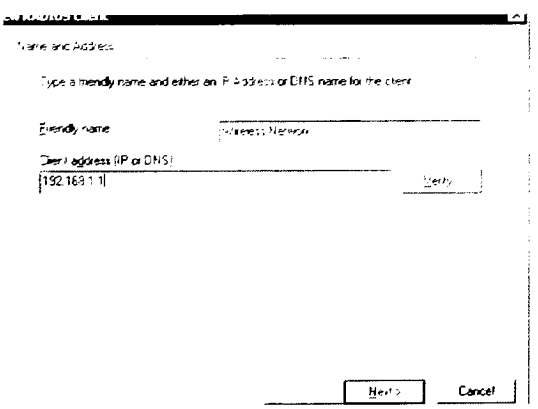

Figure 13 IAS setup screen

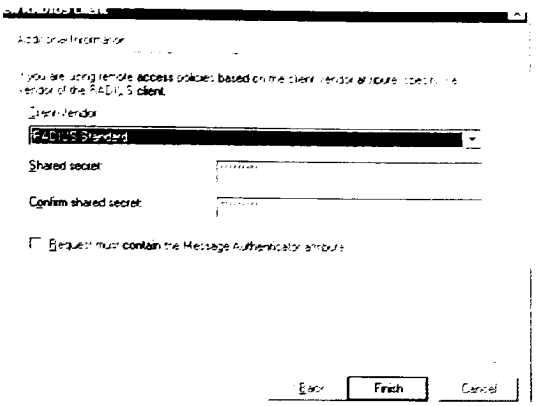

Figure 14 IAS shared secret

Unfortunately the Linksys documentation contains no reference to the hardware supporting RADIUS. The testers required assistance in finding RADIUS in the Linksys web configuration page (Appendix G). Having been told that the access point does support RADIUS, and because the five testers saw RADIUS as an option in the wireless security section, the testers were able to find the option to enable this configuration. The Linksys configuration shown in Figure 15 allows different RADIUS authentications to be combined with WEP encryption. Without any further documentation all five testers were unable to continue. No testers were able to get the wireless host to communicate through the access point to gain access to the wired network (Appendix G).

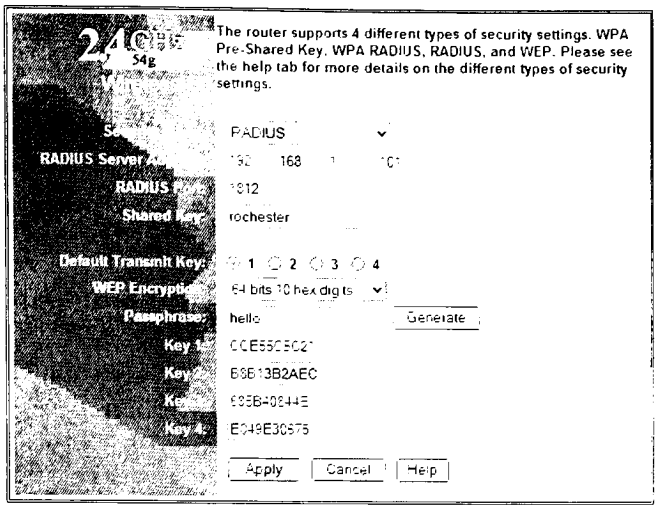

Figure 15 RADIUS on Linksys including WEP

IV-6. Scenario 6: All Security Measures in Place

This final scenario put all methods of security into place. This scenario will use MAC filtering despite the requirement of having to enter in static MAC addresses. The original plan was in fact to use RADIUS for authorization and not MAC filtering, but the change was made because all five testers failed to get RADIUS to work in the previous test. A VPN tunnel will then be created to a server on the wired network. This measure provides use authentication and authorization as well as encryption of data while on the wireless network.

Again the testers had no problems repeating steps for the previous scenarios. They quickly got into the web configuration to enable MAC filtering to only allow their host access. Nobody this time around had a MAC address entry issue with the interface deleting partial entries – refer to problem description in section IV-2. And the testers had no problem creating the VPN connection again. All five testers completed the configurations without any issues (Appendix G).

V. Setup Documentation Review

The Linksys documentation gets mixed marks in aiding administrators in setting up wireless security. The paper documentation had clear steps that a standard network administrator could follow. The documentation does not explain the risks that wireless networks are exposed to. During the setup the documentation highly recommends changing the router's administrator password (Linksys 20). There is no recommendation to use the MAC filter settings on the Linksys access point. In the Q&A section the documentation is very misleading. When asked "Will the information be intercepted while it is being transmitted through the air?" the documentation answers "WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control (Linksys 82)." In a separate appendix, Linksys does give some security recommendations. These include changing the default SSID, using WEP encryption, and enabling MAC address filtering (Linksys 87). Having a side-bar notation during the configuration section stating that this is a recommended practice would have been a helpful tip to someone going through the configuration pages during a setup. The documentation also fails in not mentioning how to configure WPA or the RADIUS options.

Microsoft has made configuring the steps for wireless security as simple as fill in the blank. The administrator is isolated from the lower intricacies of security

management. Unfortunately the only documentation Microsoft has published outlines configuring 802.1X and WPA scenarios. There was no mention about using a VPN connection to secure wireless networks. The security documents do list the vulnerabilities with WEP and the solutions to the problems as addressed by either by 802.1X or WPA.

VI. Administrative Setup Review

Administrative setup is an important part of network configuration and security. If a network administrator is not aware of the risks with a network configuration he can not determine whether or not to address them. Documentation plays a part in the configuration but the higher cost is in maintenance of the system.

The first scenario with no security measures in place requires no administrative configuration. The network is as easy to set up as it is for hackers to break into. This setup is strongly discouraged.

MAC filters in the second scenario provide a basic level of defense. In static networks or networks with a few access points MAC filters only require an initial entry of MAC addresses. If the network has a high turnover of wireless hosts, keeping the MAC filters up to date would be a high administrative overhead. Also, if there are many access points to configure keeping them up to date could be tedious. MAC filters can

also be bypassed by MAC spoofing software and should be combined with other security measures.

WEP encryption in the third should be used for the sole reason that some encryption is better than none at all. Administrators first have to enable WEP on the access point and generate the keys to be used. To aid end users administrators should enter the WEP keys into the wireless hosts. The job of changing WEP keys is a manual process. The administrator needs to change the access point's keys and then either change the hosts manually or have the end users perform the task. The frequency of changing keys is dependent on the security desired. Highly secure networks may want keys changed daily – resulting in a potentially unusable network for end users. Again, this is the challenge facing administrators in balancing security risks and usability. Stronger encryption methods such as VPN or SSL should be used for corporate networks but if resources prohibit either of these, then WEP encryption will thwart casual hackers and is better than no encryption at all.

VPN connections in the fourth scenario adds another server into the mix of hardware systems for an administrator to maintain. If the company has an existing remote access server accepting VPN connections over the Internet, this same server can also service the wireless network. Administratively this could mean no additional configurations. However, this could put added demand on server resources depending on how many wireless clients would be connecting in addition to regular loads from the

Internet. Administrators also could encounter training issues in getting end users used to making VPN connections to get on the network.

Unfortunately the lack of documentation failed to allow testing of the RADIUS scenario. The administrative setup did entail more configurations on the access point and the installation of a RADIUS server. Since WEP keys were still used, maintenance of the keys would be an administrative overhead similar to using WEP alone. Authentication and authorization is handled by the RADIUS server and compared to a corporate directory service such as Active Director or NDS. Keeping accounts centralized does minimize the maintenance required by administrators.

The final configuration adds some flexibility for administrators. MAC filters are used in this configuration and as such this scenario is only low maintenance for networks with low host turnover. WEP keys were again used to keep casual hackers at bay. Fortunately the addition of a VPN connection provides more security to pick up where MAC filters and WEP leave off. VPN adds authorization of a username building on the MAC filters on the access point. VPN also adds a stronger encryption scheme than WEP. Because of the encryption offered by VPN the WEP keys could be changed less frequently.

VII. End User Usability

An important part in rolling out security practices is balancing them with end user usability. End users of a wireless computer network should not have a substantially more

difficult time getting onto the network than their wired network coworkers. If wireless networks become unusable because of complex steps required to gain access, then the gains of mobility and productivity that the wireless networks tout will be negated. Unfortunately for network administrators the most usable networks are the least secure – and the most secure networks are the least usable. The tightrope that administrators walk is finding the balance between security and usability. Fortunately with wireless networks the most complex parts of security are handled by the administrator and not the end user. The less than adequate Linksys documentation and unintuitive web configuration for the access point are never seen by the end user. Instead, the users are padded by Microsoft's Windows XP operating system.

In the first scenario, there was clearly no security and the highest usability. Users simply needed to turn on their wireless device. Windows shows any access points that it is able to get a beacon signal from. The user is presented with a list of access points and even a warning that the access is not using WEP and that communications between the wireless host and the access point are not secure. None of the testers had problems connecting to the default wireless network (Appendix G). The available networks and security warning are shown in Figure 16 below.

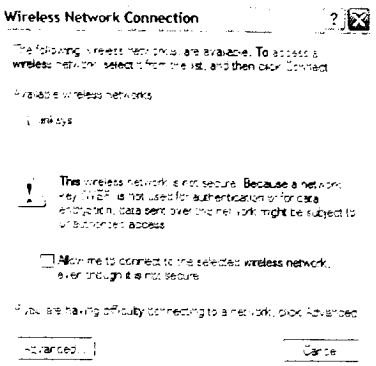

Figure 16 Connecting to insecure access point

The second scenario again has little effect on the end user but does add a small degree of security. MAC filtering is an administrative action that puts an access list on the access point stating which MAC addresses are allowed to connect. End users must inform the network administrator so their MAC address can be added to the access point. In this scenario no WEP was used so the end user was again presented with a dialog box stating that communications on this wireless network are not secure. There is no change in what the end user sees when using MAC filtering.

The third scenario introduces a possible configuration step for the end user. WEP encryption in a wireless network requires the access point and wireless host to have a shared key to encrypt messages with. The network administrator enters the keys on the access point. Most administrators would then manually enter the keys into the host so the host has them when attempting to connect to a WEP enabled wireless network. Windows again is there to assist end users that do not have the WEP keys already entered. When Windows attempts to connect to a WEP enabled network a dialog box, Figure 17, is presented stating that a WEP key is needed to communicate with the access point. The end user types in the key and is then connected if the key is correct. None of the testers

had a problem figuring out how to enter in the WEP key required to connect to the wireless network (Appendix G).

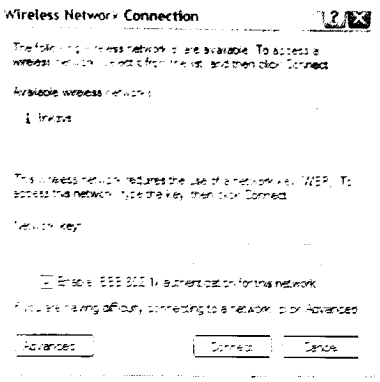

Figure 17 Windows XP asking for WEP key

The fourth scenario adds an end user step required to gain access to the network but also adds the second highest security. Corporate road warriors are now familiar with VPN technology that they use to communicate with company servers behind the firewalls. The user is first presented with a dialog box to connect to the discovered network. A WEP key is needed for WEP enabled networks or the user is prompted before connecting to an insecure network. Once connected to the access point the user would then have to connect to the VPN server. A username and password are required for authentication and authorization and should be compared to the company's user account database. This would allow a single sign on for both VPN access and access to other corporate resources. Single sign-on eliminates the needs for users to remember multiple account usernames and passwords and increases usability. Users familiar with using VPN connections had no learning curve in using a VPN for wireless networks (Appendix G). Other users could need training in establishing the connection before attempting to access resources.

Due to the inability for the testers to configure the fifth scenario no hosts were able to get onto the network. In theory the end user would need the WEP key used by the access point. The user would also have to supply credentials that the access point would pass to the RADIUS server for validation. If the credentials are valid then access is granted and no further action is required by the end user.

The last scenario combines three levels of security. The end user has to ensure that the administrator has their MAC address to add to the MAC filter on the access point. Windows then presents the user with an available network and prompts for a WEP key to gain access. After supplying the correct key the user must make a VPN connection to gain access to the wired network. This scenario provides the highest level of security of all the scenarios presented. To make this scenario most usable for end users, an administrator should enter the WEP keys into the wireless host when it is setup and also use single sign on for the VPN connection. The five testers had no problems performing the tasks the end user would have to go through (Appendix G). The combination of WEP encryption, MAC filtering, and VPN security only resulted in a net increase for the end user in having to create the VPN connection. Having only one additional step should be acceptable for administrators and end users in order to obtain a highly secure network.

VIII. Debunking the Myths

Mathew Gast, author of *802.11 Wireless Networks: The Definitive Guide* lists seven security issues in wireless networks that would deter network administrators from deploying wireless solutions. His security issues are listed below along with explanation and how the issue is not a security concern or how the solution above that uses all security levels by combining RADIUS and VPN eliminates the security concern.

Problem #1 Easy Access

Wireless LANs are by their nature easy to locate. Access points send out beacon frames announcing their presence and communication between wireless devices is sent out in the open air encrypted or not. Gast does list steps to fix this problem in using WEP keys to allow access to that wireless ether, putting access points outside the firewall, and requiring VPN for secure access (Gast).

Problem #2 Rogue Access Points

Gast states that any user can purchase wireless gear, plug it into the network, and therefore allow outside hackers a path into the network. The solution to this problem is in securing the wired network. Wired hosts should be authenticated before they are given access to the wired network. This would prevent a rogue access point from being plugged into the network.

Problem #3 Unauthorized Use of Service

By default access points are wide open, allowing anyone with a wireless adapter to gain access. To solve this problem, network administrators can use WEP as a basic level of defense and use VPN to secure communications even further.

Problem #4 Service and Performance Constraints

Wireless LANS can have garbage packets sent into the air or other outside interference generated to degrade the limited band of airwaves used for transmission. Nobody can stop someone from sending stuff out into the air, but as Gast points out, network monitoring using the SNMP protocol can alert administrators when a link becomes saturated.

Problem #5 MAC Spoofing and Session Hijacking

All 802 networks, both wired and wireless, do not authenticate frames by default. The frames have a source and destination addresses but there is no verification that the host in the frame was the host that sent the frame. The only solution to this, as Gast points out, is using a frame-based and user-based authentication which is provided in the upcoming 802.1X standard.

Problem #6 Traffic Analysis and Eavesdropping

Gast brings light to the open nature of wireless communications. All traffic is sent out on the air and needs to be encrypted to ensure that unwanted people do not intercept the data. He recommends that companies use WEP at minimum to encrypt data. He even states that some new vendor releases of WEP automatically use dynamic key

changing to thwart attacks that worked against the original WEP implementation (Gast). A final recommendation is to use a higher level encryption method for sensitive data, such as a VPN connection, IPSec, or SSL.

Problem #7 Higher Level Attacks

Wireless networks are sometimes incorrectly placed directly connected to the trusted internal network. Anyone gaining access to the wireless network automatically gains access to the trusted wired network. The solution to this problem is in placing the wireless access point outside the trusted network. Doing this treats wireless traffic as suspect, like any traffic coming in from the Internet. The traffic passes through a firewall and other security checkpoints before getting to the secure wired network.

IX. Conclusion

Network administrators are asked to provide solutions to their company that increase productivity and lower costs. Wireless networks allow users to roam from office to conference room without losing connectivity to the network. Installation costs for wireless networks are also less than wired counterparts. However, installation costs and productivity are not the only measures that can be used to justify a wireless network.

Wireless networks by their nature are not secure. The medium used for transmitting data is the open air which is accessible by anything within the transmission range of an

antenna. Network administrators need to understand the risks associated with wireless networks before they are added to wired networks.

Since most administrators are not wireless or security experts they have to rely on the documentation provided by vendors in making their decisions and implementing solutions. The documentation provided by Linksys in this project only provided basic information about protection methods such as MAC filters and WEP encryption. It did not mention any of the vulnerabilities that a wireless network would be exposed to. The Microsoft documentation did explain the risks with wireless networks, especially WEP cracking, and offered a solution in using RADIUS authentication and VPN connections. Problems with the configuration were experienced by all skill levels. The Linksys configuration page contained some poorly designed sections. These areas were identified before testing as potential problems and the testers further validated that even by following provided documentation that problems existed with the interface. The documentation also failed to provide any warnings about configurations and their security risks.

Administrators must also contend with the usability of the wireless network. MAC filters, WEP keys, and VPN credentials all need to be maintained once the network is in production. If maintenance becomes too cumbersome the administrator could stop performing some duties and the security of the network could be compromised. Likewise, if the network is unusable for end users they may stop using the network or find ways to circumvent the security measures.

This paper looked at the different risks that wireless networks are exposed to and also at the various steps administrators can take to secure their wireless networks. The end goal was to create recommendations that would allow a secure network to exist that was easy for an administrator to maintain and did not prohibit the average end user for gaining access. With that in mind the following security recommendations are being made:

1. Change the default SSID on the access point but leave the beacon enabled. The SSID is broadcasted by the access point to announce its presence to anyone within its transmission range. This is a valuable tool for administrators wanting to troubleshoot connectivity problems. Wireless hosts must have the same SSID as the access point in order to communicate with it. The SSID is sent in every wireless packet, is not encrypted, and should never be used as a layer of defense (Wi-Fi Planet). Because the SSID is not a security layer having it enabled provides more administrative troubleshooting assistance than help to a would be hacker.
2. Enable MAC filters on small networks or networks with low host turnover. MAC filters provide a basic level of protection that would only stop a casual hacker. Determined hackers would have tools at their disposal to get past this security measure. Because of this MAC filters should not be the only line of defense.
3. Enable WEP encryption. Some encryption is better than none, and this is still the case with WEP. Small networks that use MAC filtering and WEP have reduced their chances of being hacked than those with no security in place. If resources

permit, more security layers should be implemented to compliment MAC filtering and WEP.

4. A VPN connection provides the best method for securing wireless access to a wired network. VPN technology is trusted to protect data across the entire Internet and it performs exactly the same way over wireless networks. User accounts are centrally controlled and access can also be configured based on time of day or other criteria.
5. The access point should be placed outside the corporate network. Any traffic coming in from the access point should be viewed as untrusted; similar to any traffic coming in from the Internet. A firewall should limit traffic coming in from the access point and only trusted VPN communications should be allowed to pass to the corporate network.

Administrators need to realize that no network is completely secure. A hole or exploit will be found for every security step that is put into place. Wireless networks can be used as a valuable resource for companies wishing to provide mobility to their employees. It is the job of a network administrator to find those holes, mitigate those risks, and to do so without compromising usability.

Appendix A Speed Comparison of Topologies

A major concern about wireless networks is the actual performance of the network. Wired networks commonly run 100Mbps to the desktops and even gigabit connections are becoming common for power users. 802.11b as stated in the standard runs at 11Mbps with a fallback to 5.5Mbps, 2Mbps, or 1Mbps based on distance from the access point and interference (PCWebopedia.com). A valid concern is that adding layers of security will further decrease transmission speeds over a medium that is already slower than wired networks. Performance Test, a benchmark application suite from PassMark Software was used to test transmission speeds. A connection point was installed on a wired server and another on a wireless host. The chart below summarizes the security topologies tested and average kilobits per second transmitted over a two minute timeframe. The wireless host was located one floor below and about 50 feet away from the access point. Windows showed the connection at 5.5Mbps.

Security Measures in Place	Average Kilobits per Second
No Security Measures	3,537
64 bit WEP	3,118
128 bit WEP	3,445
VPN	2,786
WEP and VPN	2,772

Figure 18 Speed Comparison

As expected, the overhead for the VPN connection would result in a slower speed.

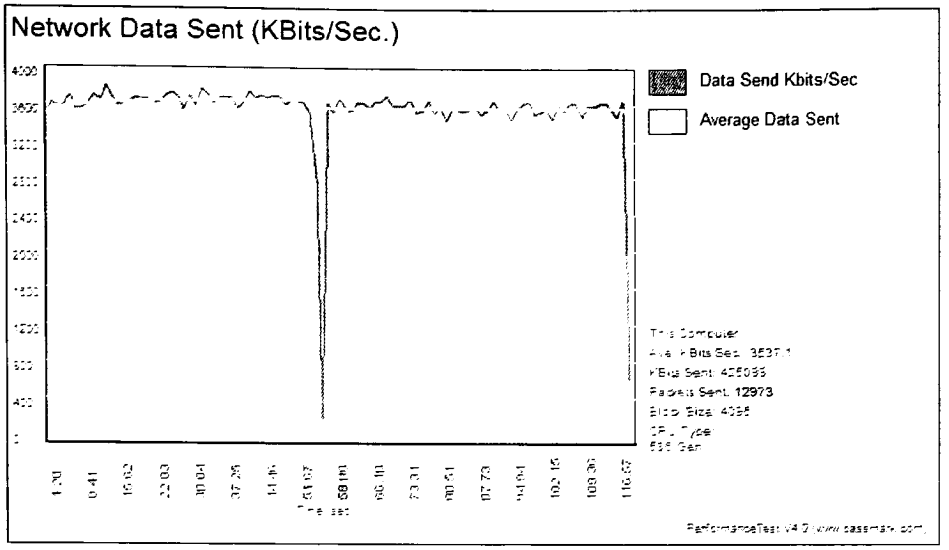

Figure 19 Transmission test without security measures

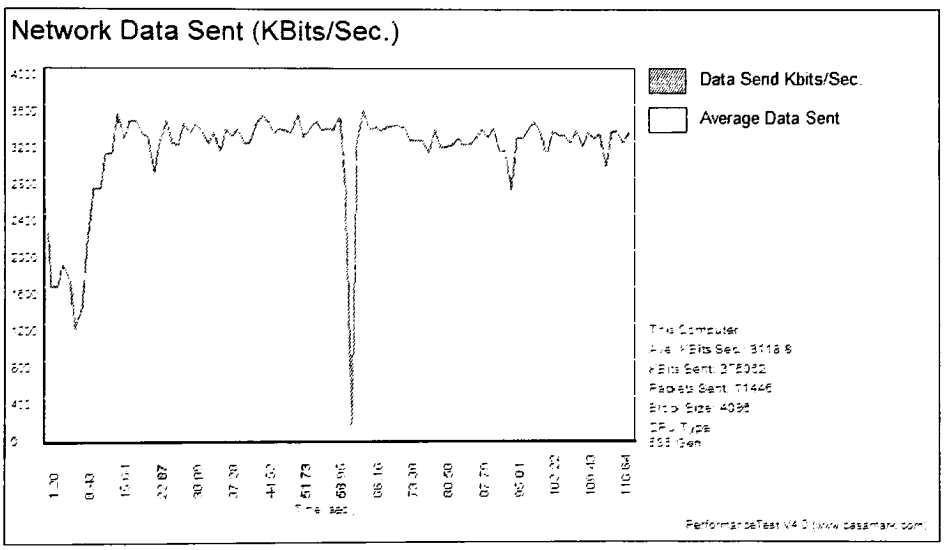

Figure 20 Transmission test with 64-bit WEP

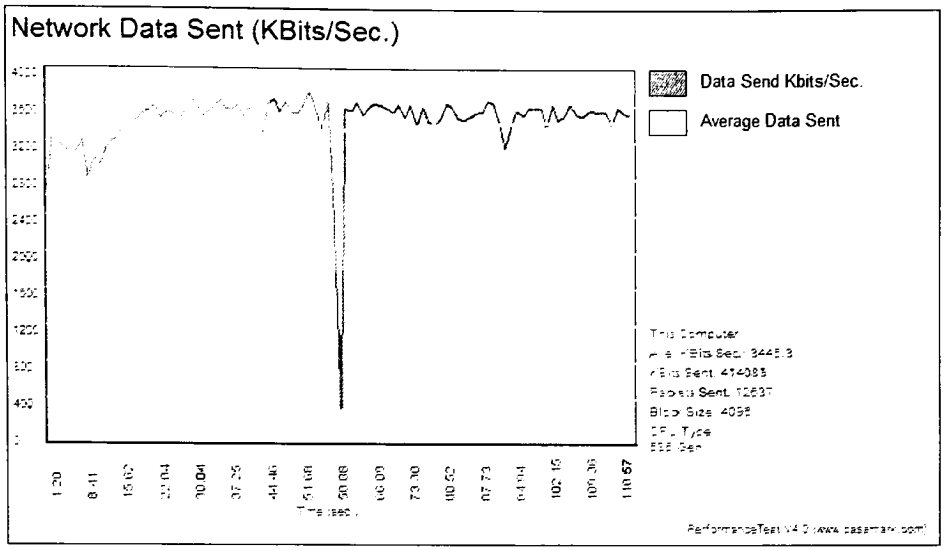

Figure 21 Transmission test with 128-bit WEP

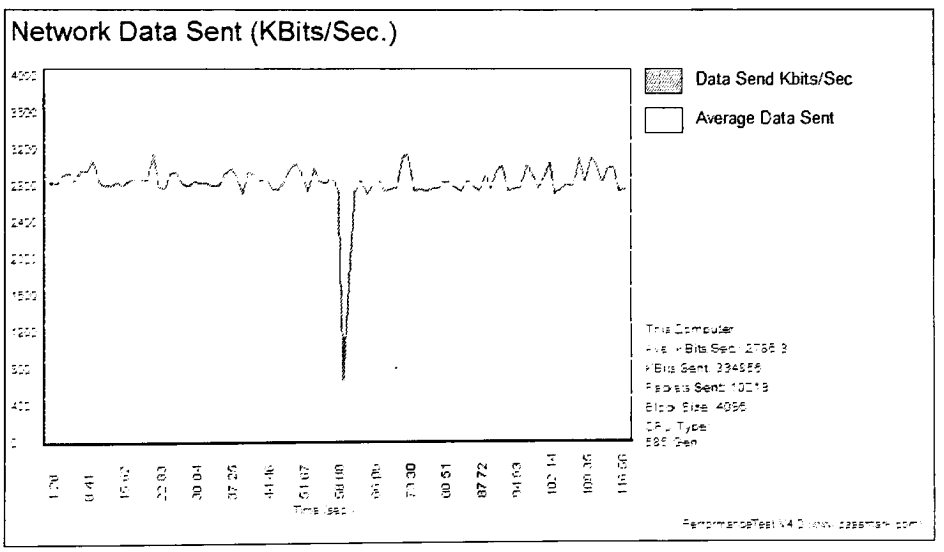

Figure 22 Transmission test with VPN

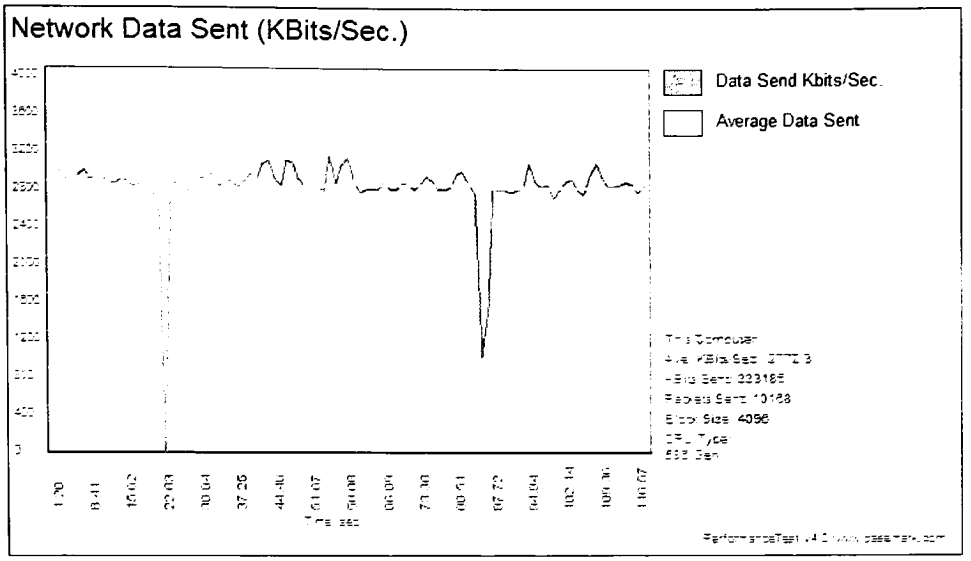

Figure 23 Transmission with WEP and VPN

Appendix B 802.1x Security

802.1X enables "authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless networks (Aboba)." 802.1X contains three major players. The supplicant is the entity wishing to be authenticated to gain access. In a wireless network these are the wireless hosts. The authenticator is the link between the supplicant and the trusted network. The authenticator passes credentials between the supplicant and the authentication server using Extensible Authentication Protocol. The authentication server compares credentials from the authenticator and supplicant to determine the identity of both and to grant or deny access. RADIUS support is an option in the 802.1X as the authentication server but working drafts have started as this is the expected route to be taking by administrators (Congdon et al).

802.1X involves a series of communications between the supplicant, authenticator, and authentication server. The supplicant, the wireless host, sends an EAP-start message to the authenticator, the access point, to gain access. The authenticator sends an EAP-request identity packet back. The supplicant responds with an EAP-response packet which the authenticator forwards to the authentication server (RADIUS) to determine if the supplicant is allowed access. The authentication server validates the supplicants credentials and returns an accept or reject message to the authenticator. The authenticator relays the accept or reject to the supplicant. If the message is an accept the authenticator also opens a trusted port that the supplicant can use to access the wired network. If the message is a reject the supplicant is asked to send its credentials again (Geier).

802.1X is not the end all solution for securing 802 networks. 802.1X networks are still vulnerable to session hijacking and man-in-the-middle attacks. "The hacker waits for someone to successfully finish the authentication process. Then you as the attacker send a disassociate message, forging it to make it look like it came from the AP. The client thinks they have been kicked off, but the AP thinks the client is still out there. As long as WEP is not involved you can start using that connection up until the next time out, usually about 60 minutes" states Professor William Arbaugh who first reported this breach (Schwartz).

Appendix C Wireless Protected Access

Wi-Fi Protected Access began as an interim replacement for the potentially vulnerable WEP encryption scheme. WPA is a software upgrade to operating systems and device firmware to provide better security until the 802.11i standard is ratified (Grimm). Wi-Fi had two goals when being developed. The first was to improve on the breakable encryption mechanism used by WEP. The second was to introduce user authentication which previously had to be performed by another layer of security such as a VPN connection. WPA uses Temporal Key Integrity Protocol to encrypt data. TPKI includes per-packet key mixing, a message integrity check, initialization vector, and a re-keying mechanism that eliminates the vulnerabilities present in WEP (Grimm). WPA uses 802.1X and Extensible Authentication Protocol to validate both the user and access point's identities before allowing data transmissions. WPA in a home office setting can also use a manually entered shared key, similar to WEP, but WPA uses TPKI for encryption instead of WEP.

Appendix D 802.11i

802.11i is an upcoming standard being developed by the IEEE Taskgroup I. Components of the 802.11i standard have already been finalized and released for use. 802.1X uses port-based authentication, Temporal Key Integrity Protocol, and key management, and is a part of the final 802.11i standard. 802.11i will be backwards compatible with network devices running WPA (Dell Computer Corporation).

Improvements in 802.11i over current security offerings include creating new keys at the start of each session (Lawson). Packet integrity checks ensure that packets being sent are a part of the same data stream (Lawson). Robust Security Network (RSN) uses dynamic negotiation of authentication and encryption algorithms between wireless hosts (Cohen and O'hara). This allows wireless networks to start with the standard Temporal Key Integrity Protocol, and later, when standards are adopted, to upgrade to Advanced Encryption Standard (AES) which is a part of 802.11i. Network Fusion authors Alan Cohen and Bob O'hara created the figure below to explain Temporal Key Integrity within 802.11i.

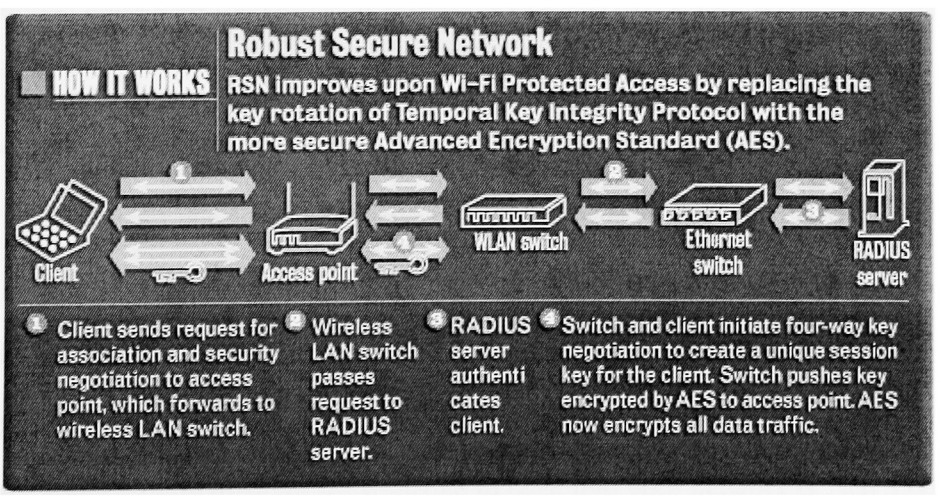

Figure 24 802.11 using AES

Appendix E New Linksys Documentation

The acquisition of Linksys by Cisco and the advancement of security initiatives explain the security focused revision of the Linksys access point documentation. The first improvement is in the explanation of the wireless security options. WPA pre-shared key, WPA radius, radius, and WEP options have the requested configuration fields explained (Cisco 28). The big addition to the documentation is a new appendix dedicated to wireless security. The documentation does a great job in explaining how a wireless network works by comparing devices on a wireless network to everyday cell phones and cordless phones that also broadcast their signals (Cisco 52).

The documentation even goes into brief explanations of four different attacks against wireless networks. Passive attacks are defined as attacks where the hacker just views data transmitted over the air (Cisco 53). Unencrypted data is easily viewed and even WEP keys can be captured defeating this method of security. Jamming attacks entail putting garbage waves into the air (Cisco 53). Jamming could be intentional or unintentional since many common household appliances use the 2.4 GHz frequency. The next attack is an active attack. In an active attack the hacker has gained access to the wireless network and has gained access to resources on the wireless and wired networks (Cisco 54). Man-in-the-middle attacks position a hacker in between wireless hosts and access points. The hacker accepts data from one and forwards it on to the other while viewing the contents in transit (Cisco 54). The documentation includes a message that is the rule for network security: "No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network (Cisco 55)."

The documentation then outlines measures that can be taken to secure the wireless network. Positioning access points so that signals do not stray far from the physical building and using hard to guess administrator passwords are two of the "Common Sense" security practices (Cisco 55). They recommend disabling the SSID but warn that SSIDs are not a security measure and should not be used as a way to protect a wireless network (Cisco 56). Enabling MAC filtering on the access point is also recommended as well as placing the access point outside the corporate firewall to treat wireless traffic the same as untrusted Internet traffic (Cisco 56). WEP keys "only provide enough security to make a hacker's job more difficult (Cisco 57)." Using multiple WEP keys and more advanced dynamic WEP keys makes the breaking of WEP more difficult. Wi-Fi Protected Access is only defined as the latest and best standard available for wireless networks. Unfortunately the documentation does not go further and explain how WPA eliminates the security problems of WEP.

Appendix F Summary Findings

Scenario 1: Default Wireless Network

- Only one person found the best practice in the Linksys documentation to change the default SSID and enable WEP.

Scenario 2: MAC Filtering Only

- Four testers went to look in the Linksys index for MAC filtering but there was no mention of MAC filtering.
- Three of the five went to the Wireless area of the Linksys config page – only two made the correct Advanced tab selection.
- Four of the five had problems entering MAC addresses due to the config page performing a length check when clicking off the entry box.

Scenario 3: Wireless Network with WEP Only

- Two testers went to the Linksys index but did not find any mention of WEP.
- Two testers tried the Security tab first while two others tried to the Advanced tab first in the Linksys config page.
- Only one tester on the first attempt scrolled down on the main page to find the WEP settings.
- The WEP key entry page also did not have an OK or Done button to allow testers to leave the screen.

Scenario 4: Wireless Network with VPN Only

- Four testers said the Linksys supports VPN. One questioned if VPN is the same as VPN pass-through.

Scenario 5: Wireless Network with RADIUS

- The Linksys documentation had no mention of RADIUS support, but the config page contains options for RADIUS.
- None of the testers completed this scenario.

Scenario 6: All Security Measures in Place

- No additional issues than those found above

Appendix G Testing Tasks and Questions

Scenario 1: Default Wireless Network

Are there any warnings or dangers in the Linksys documentation about this configuration?

All five testers were correct in the documentation not warning about a default, no WEP and no filtering configuration.

Are there any recommended 'best practices' in the Linksys documentation?

One person found the note to change the default SSID and to enable WEP.

Are there any warnings or dangers in the Windows documentation about this configuration?

All five testers said found that not using WEP for encryption was not recommended.

Are there any recommended 'best practices' in the Windows documentation?

All five said using WEP.

Using the documentation provided by Linksys & Microsoft get the wireless Windows XP computer to map a drive to \\controller\share. Talk out loud during this process verbalizing any questions or assumptions you are taking.

All five were able to turn on the Windows XP client and connect to the network share. All five saw the Windows XP notice that the network was unsecured and were able to connect without a problem.

Scenario 2: MAC Filtering Only

Is the Linksys access point capable of support MAC filtering?

All five correctly said yes.

Are there any warnings or dangers in the Linksys documentation about this configuration?

All five were correct in the Linksys documentation not containing any warnings about using MAC filtering only.

Using the documentation provided by Linksys configure the access point to filter wireless MAC addresses so that only your Windows XP computer can gain access to the wired network. Talk out loud during this process verbalizing any questions or assumptions you are taking to set this up.

Four of the five testers immediately flipped to the back of the Linksys documentation to look for an index. There was no index so they went back to the table of contents.

Three of the five went onto the Wireless section of the configuration before making it to the Advanced tab. Entering in the MAC addresses presented a problem for four of the five testers. The four started typing in the MAC address but had to click back to the command prompt to get the rest of the MAC address. When they did this the entry page alerted them that the MAC address was the incorrect length and then deleted all the text entered.

After you configure the access point from the Windows XP computer map a drive to \\controller\share Talk out loud during this process verbalizing any questions or assumptions you are taking while doing this user task.

All five turned on the Windows XP client and were able to map the drive. Again the warning appeared about the unsecured network, after checking the warning they were all able to map the drive.

Scenario 3: Wireless Network with WEP Only

Is the Linksys access point capable of supporting WEP encryption?

All five were correct with yes.

Are there any warnings or dangers in the Linksys documentation about this configuration?

All five were correct in the Linksys documentation not containing any warnings about using WEP only.

Three people found the notice that using WEP could decrease speed.

Is the Windows XP operating system capable of supporting WEP encryption?

All five were correct with yes.

Are there any warning or dangers in the Windows documentation about this configuration?

All five were correct with no.

Using the documentation provided by Linksys and Microsoft configure the access point and Windows XP computer to use WEP encryption. Use the pass phrase hello to generate your key. Talk out loud during this process verbalizing any questions or assumptions you are taking to set this up.

All five were correct with no. Two people looked through the Linksys documentation and found the WEP area but could not figure out what to do next. They went to the configuration webpage. Three of the testers went directly to the webpage and bypassed the documentation. Two clicked the Security tab first, two went to Advanced and looked around there first. Only one person scrolled down to find the WEP section on the first attempt. After getting to the WEP key screen all five were able to generate the keys. All of them also hesitated on how to exit this screen since there was no OK or DONE button. Two clicked Cancel, three clicked the upper right X.

After you configure the access point and Windows XP computer map a drive to \\controller\share Talk out loud during this process verbalizing any questions or assumptions you are taking while during this user task.

All five testers were able to see the WEP enabled network. Four typed in the key correctly on the first attempt. One person needed to enter the key in twice. All five then mapped the drive without a problem.

Scenario 4: Wireless Network with VPN Only

Is the Linksys access point capable of supporting a VPN tunnel?

The two more technically savvy testers said yes. Two of the intermediate users said yes. The third basic user hesitated with yes assuming that VPN pass-through was the same as a VPN tunnel.

Are there any warnings or dangers in the Linksys documentation about this configuration?

All five were correct in the Linksys documentation not containing any warnings about using VPN only.

Is the Windows XP operating system capable of creating a VPN tunnel?

All five were correct in saying yes.

Are there any warning or dangers in the Windows documentation about this configuration?

All five said no. The Windows documentation contains no warnings about using just a VPN tunnel.

The server CONTROLLER with IP address 192.168.1.114 is set up as a VPN server for hosts on the Internet. Using the documentation provided by Linksys and Microsoft configure the access point and Windows XP computer to make a VPN connection to CONTROLLER. Talk out loud during this process verbalizing any questions or assumptions you are taking to set this up.

From the previous uses with the web configuration utility all five clicked on the Security tab to double check VPN was allowed.

One of the five never used VPN before and was able to follow Windows Help after searching for VPN. The other four went right into Control Panel and set up the connection.

After you configure the access point and Windows XP computer connect the VPN connection and then map a drive to \\controller\share Talk out loud during this process verbalizing any questions or assumptions you are taking while during this user task.

All five connected to the unsecured wireless network. All five then connected the VPN and mapped the drive.

Scenario 5: Wireless Network with RADIUS

Is the Linksys access point capable of supporting RADIUS authorization?

All five said no. The Linksys documentation does not contain any reference to RADIUS.

Are there any warnings or dangers in the Linksys documentation about this configuration?

All five said no. The Linksys documentation does not contain any reference to RADIUS.

Is the Windows XP operating system capable of supporting RADIUS authorization?

All five said yes and found the configuration tab in Windows.

Are there any warning or dangers in the Windows documentation about this configuration?

All five were correct with no. Two noted that RADIUS is more secure than WEP.

Using the documentation provided by Linksys and Microsoft configure the access point, Windows XP computer, and CONTROLLER to use 802.1x authentication. IAS has not been configured on

CONTROLLER yet. Use the secret secret for the 802.1x key. Talk out loud during this process verbalizing any questions or assumptions you are taking to set this up.

This test was skipped by 4 of the 5 testers since no documentation was provided by Linksys. One of the technically savvy testers tried to configure RADIUS by guessing settings on the Linksys web configuration pages but was not able to get it to work.

After you configure the access point, Windows XP computer and CONTROLLER map a drive to \\controller\share Talk out loud during this process verbalizing any questions or assumptions you are taking while during this user task.

This test was skipped by all five testers since no documentation was provided by Linksys.

Scenario 6: All Security Measures in Place

Using the documentation provided by Linksys and Microsoft configure the access point, Windows XP computer, and CONTROLLER to use MAC filtering to allow only your Windows XP computer access, create a VPN connection and configure 802.1x authentication. Use the secret secret for the 802.1x key. Talk out loud during this process verbalizing any questions or assumptions you are taking to set this up.

This test was modified to use MAC filtering, VPN, and WEP since 802.1x did not work. All five testers were able to get to the correct screens on the Linksys web configuration on the first attempt. Nobody clicked off the MAC filter list when entering the MAC address into the field. The VPN connection was also created without a problem on the Windows XP client.

After you configure the access point, Windows XP computer and CONTROLLER, connect the VPN connection and map a drive to \\controller\share Talk out loud during this process verbalizing any questions or assumptions you are taking while during this user task.

All five were able to enter in the WEP key to connect to the network. All five were able to connect the VPN and then map the drive.

Works Referenced

Aboba, Bernard. "A Diagnostic Model for IEEE 802.1X" Network Working Group. Internet: http://www.drizzle.com/~aboba/IEEE/diag.txt 2 March 2000.

Backman, Dan. "Guarding the Flank with RADIUS & TACACS." Network Computing. Internet: http://www.networkcomputing.com/902/902ws13.html September 2002.

Cisco. "2.5GHz Wireless-G Broadband Router User Guide." Linksys a Division of Cisco Systems. 2003.

Cohen, Alan and O'hara, Bob. "802.11i shores up wireless security." Network World Fusion. Internet: http://www.nwfusion.com/news/tech/2003/0526techupdate.html 26 May 2003.

Collins, Jennie and Reznik, Gleb. "Wireless Layered Security." Rochester Institute of Technology. Unpublished Independent Study. 21 May 2003.

Congdon, Paul. Aboba, Bernard. Smith, Andrew. Zorn, Glen. Roese, John. "IEEE 802.1X RADIUS Usage Guidelines." Internet: http://www.drizzle.com/~aboba/IEEE/draft-congdon-radius-8021x-23.txt 17 February 2003.

Delio, Michelle. "Wireless Networks in Big Trouble." Wired News. Internet: http://www.wired.com/news/wireless/0,1382,46187,00.html 20 August 2001.

Dell Computer Corporation. "Wireless Security in 802.11 (Wi-Fi) Networks." Dell Computer Corporation. Internet: http://www.dell.com/downloads/global/vectors/wireless_security.pdf January 2003.

Fleck, Bob and Dimov, Jordan. "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired the network." Cigital, Inc. Internet: http://www.cigitallabs.com/resources/papers/download/arppoison.pdf October 2001.

Fluhrer, Scott. Martin, Itsik. Shamir, Adi. "Weakness in the Key Scheduling Algorithm of RC4." http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf August 2001.

Gast, Matthew. "Seven Security Problems of 802.11 Wireless." O'Reilly Network. Internet: http://www.oreillynet.com/lpt/a/2404 24 May 2002.

Geier, Jim. "802.1X Offers Authentication and Key Management." 802.11 Planet Internet: http://www.80211-planet.com/tutorials/print.php/1041171 7 May 2002.

Grimm, Brian. "Wi-Fi Protected Access." Wi-Fi Alliance. Interent: http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf 31 October 2002.

Lawson, Stephen. "Wi-Fi Gets a Security Boost." PC World. Internet: http://www.pcworld.com/news/article/0,aid,109482,00.asp 24 February 2003.

Linksys. "Wireless-G Broadband Router User Guide." 2002.

PCWebopedia.com. "802.11" Internet: http://www.pcwebopedia.com/TERM/8/802_11.html 25 June 2003.

Schwartz, Ephraim. "Researchers crack new wireless security spec." InfoWorld. Internet: http://www.infoworld.com/article/02/02/14/020214hnwifispec_1.html 14 February 2002.

SyDisTyKMoFo. "Wireless Attacks Explained." Internet: http://www.astalavista.com/library/wlan/wlansecurity.htm June 2003.

Vaughan-Nichols, Steven J. "Making the Most from WEP." Wi-Fi Planet. Internet: http://www.wi-fiplanet.com/tutorials/article.php/2106281 6 March 2003.

Webopedia. "VPN." Internet: http://www.webopedia.com/TERM/V/VPN.html 10 April 2003.

Wi-Fi Planet. "SSID" Internet: http://wi-fiplanet.webopedia.com/TERM/S/SSID.html 21 August 2003.

Software Used

Airsnort Alpha http://airsnort.shmoo.com/

Ethereal 0.9.14 http://www.ethereal.com/

Ettercap 0.6.b http://ettercap.sourceforge.net/

Passmark Performance Test 4 http://www.passmark.com/

Microsoft Windows XP Tablet PC Edition http://www.microsoft.com/windowsxp

Microsoft Windows XP Professional http://www.microsoft.com/windowsxp

Microsoft Windows Server 2003 http://www.microsoft.com/windowsserver2003

Netstumbler 0.3.30 http://www.netstumbler.com/

SMAC 1.1 http://www.klcconsulting.net/smac/