Global Information Assurance Certification Paper

Hitchhiker's Guide to Securing the Mobile Worker

SANS GSEC
Practical Assignment
Version 1.4B

Shane Herman
4 October, 2004

1.0 ABSTRACT **3**

1.1 ENVIRONMENT OVERVIEW 3
1.2 SECURITY POLICY 4

2.0 NETWORK SECURITY **5**

2.1 FIREWALLS 5
2.1.1 Linksys Firewall (Tutorial) *6*
2.1.2 Windows XP SP2 Firewall (Tutorial) *8*
2.2 WIRELESS 10
2.2.1 Linksys Wireless Access Point (Tutorial) *11*
2.2.2 Windows XP Wireless Access (Tutorial) *14*
2.3 VIRTUAL PRIVATE NETWORKS 15
2.3.1 Microsoft Point to Point Tunneling Protocol (MS-PPTP) *15*
2.3.2 Microsoft VPN (Tutorial) *16*

3.0 HOST SECURITY **17**

3.1 PATCH MANAGEMENT 17
3.1.1 Windows Update Service *17*
3.1.2 Windows Update Service (Tutorial) *18*
3.2 HOST SECURITY CONFIGURATION 21
3.2.1 Passwords *21*
3.2.2 Windows XP Passwords (Tutorial) *22*
3.2.3 Windows XP Services *22*
3.2.4 Windows XP Services (Tutorial) *23*
3.2.5 Windows Encrypted File System *25*
3.2.6 Windows XP EFS (Tutorial) *25*
3.3 SECURITY APPLICATIONS 26
3.3.1 Antivirus and Spyware (Tutorial) *27*

4.0 CONCLUSION **28**

5.0 REFERENCES **29**

1.0 Abstract

As we move forward in the new millennium, broadband usage among business workers continues to increase. According to the 2002 Telework America Survey, thirty five percent of U.S. workers' broadband costs are paid by their employers **[1].** As broadband usage grows among the mobile workforce, so does security risk. This guide will provide security information targeted at the mobile worker and enable the reader to apply basic concepts to make the computing environment more secure. It is assumed the reader has an intermediate working knowledge of the Internet and security.

Basic security concepts covered in this guide will focus around network and host security. The reader will be lead through these concepts to setup a broadband firewall, secure a wireless network, discover virtual private networking, and secure Windows XP.

In addition, a basic security policy for systems used by the mobile worker will be applied. This will be a key component in implementing a defense in depth approach. The local security policy that will be established will ensure that information stored on the systems and network is properly protected.

1.1 Environment Overview

Mainstream software and hardware platforms have been chosen for the environment of this security guide. By choosing such mainstream choices for this environment, it is thought that the information contained within will apply to the majority of the mobile workforce.

- The hardware components that we will cover in this guide include:

Laptop	IBM Thinkpad T40
Firewall	Linksys Etherfast BEFSR41
Wireless Access Point	Linksys Wireless G

- The Software components that we will over in this guide include:

Operating System	Windows XP Service Pack 2
Antivirus	Norton Antivirus 2005
Anti-Spyware	Lavasoft Ad-Aware Personal SE
Firewall	Windows Firewall

- The basic layout of our environment's network is shown in the following network diagram.

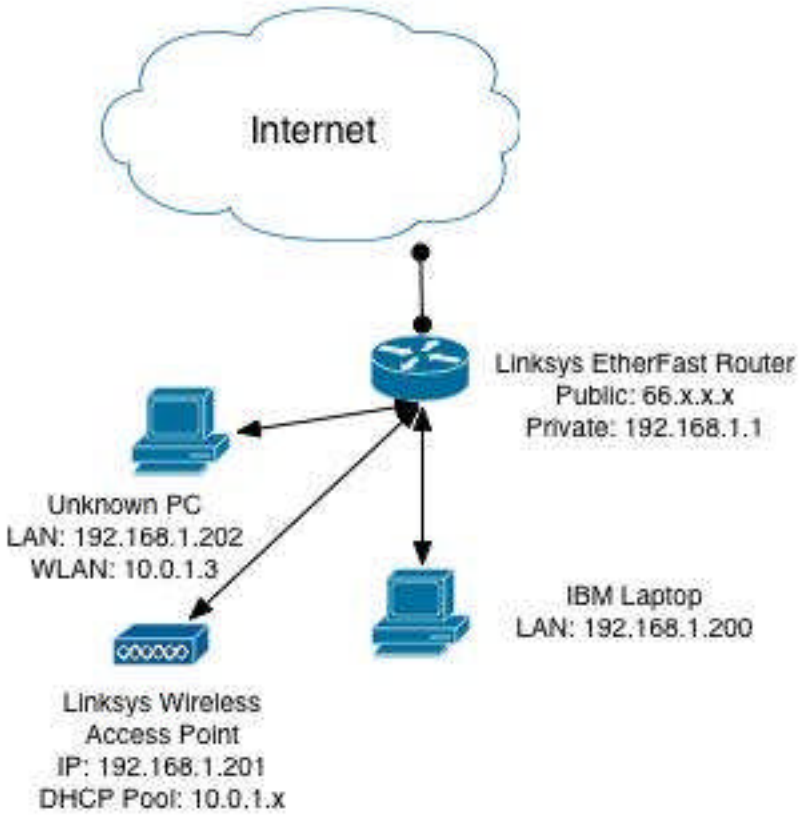

Diagram 1A

1.2 Security Policy

The development of a local security policy can clarify the objective and intended use of an environment for a mobile worker. It is important when developing a security policy to balance security and functionality. Having a single line security policy that states, "all systems should not have network connectivity" would be a secure policy, but not a very practical policy for the mobile worker.

Developing a security policy can be an involved process. There are many existing business and technical processes to consider when developing a security policy. Another aspect of developing a security policy is enforcement. A security policy is only as good as the ability to enforce the policy. In this single user hypothetical situation, however, enforcement is not a huge consideration. Instead the policy will act as a security foundation when changes are made to the environment.

Following are the major premises of our stated security policy:

- No external sources can initiate communication with any devices behind our firewall.
- The most secure authentication and encryption protocols should be used when accessing a wireless network.
- All systems should have strong passwords enabled.
- All personal documents and data need to be protected by encryption.
- Protection against viruses and spyware should be provided.

2.0 Network Security

Since we have assumed the underlying principle that the mobile worker's environment is at high risk of being compromised and the information at risk has a direct relationship to daily business of the mobile worker, the first area we will secure is the local network. This is important because it has direct access to the Internet.

In today's mobile worker environment, most workers use a form of broadband Internet. The most popular broadband implementations are Digital Subscriber Line (DSL) and Cable. DSL and Cable share a few security issues; the most common security issue is that the upstream Internet Service Provider (ISP) generally does not provide any type of filtering or firewall protection to the customer end-points.

We will implement a hardware- and software-based firewall that can immediately protect the mobile worker against hostile activity on the Internet. The most immediate vulnerabilities in Windows services are Windows Remote Access Services, Windows P2P File-sharing and SNMP. Firewalls can help restrict unauthorized access to all of these modalities. More information about these services can be found in the Top 20 SANS Vulnerabilities **[2]**. Finally, we will take into consideration our security policy as we implement network security.

2.1 Firewalls

Although there are several types of firewalls, only two types of firewalls will be covered at this time. First, we will cover a hardware-based firewall that uses Network Address Translation (NAT) **[3]**. By creating a private network, the NAT protocol allows a network with a single or limited Internet Protocol (IP) assignment the ability to connect an almost unlimited amount of devices. For example, with one public IP address assigned by an ISP, we can connect three devices with private addresses assigned by NAT. The three devices assigned private addresses have access to the Internet by proxy of the public IP address.

Besides enabling network growth, NAT also provides some basic security features. External sources on the public Internet usually (by default) cannot initiate communication to any devices behind a firewall implementing NAT. An external source can generally only communicate with the private network if communication is initiated there first. When this happens, the firewall dynamically assigns network ports that are

used to pass traffic from a private network and external sources. Another method to enable external sources to communicate with our private network is to enable port mapping. We will not configure this option, as it falls outside of our local security policy.

The second type of firewall we will examine is the personal firewall. The personal firewall is typically a software based firewall that is installed as an application or extension of the operating system. Most modern personal firewalls can filter incoming packets, log activity, and control application behavior. The personal firewall is a great first level of defense when a mobile system is connected to an untrustworthy network. As a mobile worker, you may be going to remote offices or connecting to public wireless networks. The personal firewall will provide a layer of defense to help protect against unauthorized users accessing unprotected file-shares or exploiting weaknesses in an operating system. Personal firewalls also provide a second layer of defense when using a trusted network, where traffic may bypass your hardware-based firewall.

2.1.1 Linksys Firewall (Tutorial)

The first security measure to implement is a hardware-based firewall. We will use the Linksys DSL Etherfast router to implement NAT. Our user was provided with one public IP address; we will assign this IP to the Linksys Wide Area Network (WAN) port. Behind our NAT firewall, we have two hosts and a wireless access point sharing one public Internet address.

In Diagram 1A, note the network layout, 66.x.x.x was the IP assigned by our ISP, and is assigned to the Linksys WAN port. The 192.168.1.xxx IP range is what we have assigned to our private Local Area Network (LAN). 192.168.1.1 is the internal LAN address assigned to the firewall as our LAN gateway.

All of these tasks can be accessed within the administration panel. For a more detailed explanation implementing changes to the Linksys, please refer to the online user guide **[4]**. In order to begin securing the Linksys, you will need to connect to the Linksys using Internet Explorer. Connect to the administration panel by going to the URL (http://192.168.1.1).

After logging in to your Linksys, make the following changes to make your Linksys more secure.

- **Change Password**

You will be prompted with a login and password to access the administration control panel. The default login and password is set to (username: admin password: admin). This is a very weak password and will need to be changed to a strong password. Please set the password field to a password that contains at least 8 characters and alphanumeric characters. You may reference section 3.2.1 in this document to learn more about choosing strong passwords.

- **Disable Remote Upgrade and Remote Administration**

Since you will be managing your firewall from the private LAN, there is no reason to enable remote upgrade and administration. While this limits some convience to administer your network from other networks, disabling these features will ensure unauthorized users on the Internet cannot upgrade or change the configuration of your firewall.

- **Upgrade Firmware**

The Linksys is an Internet-facing device protecting your LAN and can be subject to vulnerabilities. In order to prevent exploits to known vulnerabilities, it is good practice to keep your Linksys patched to the latest firmware. Currently, the latest firmware available for the Linksys BEFSR41 ver. 3, is Version 1.05.00. This upgrade corrects a critical DHCP vulnerability, which is described on the SecuriTeam website **[5].**

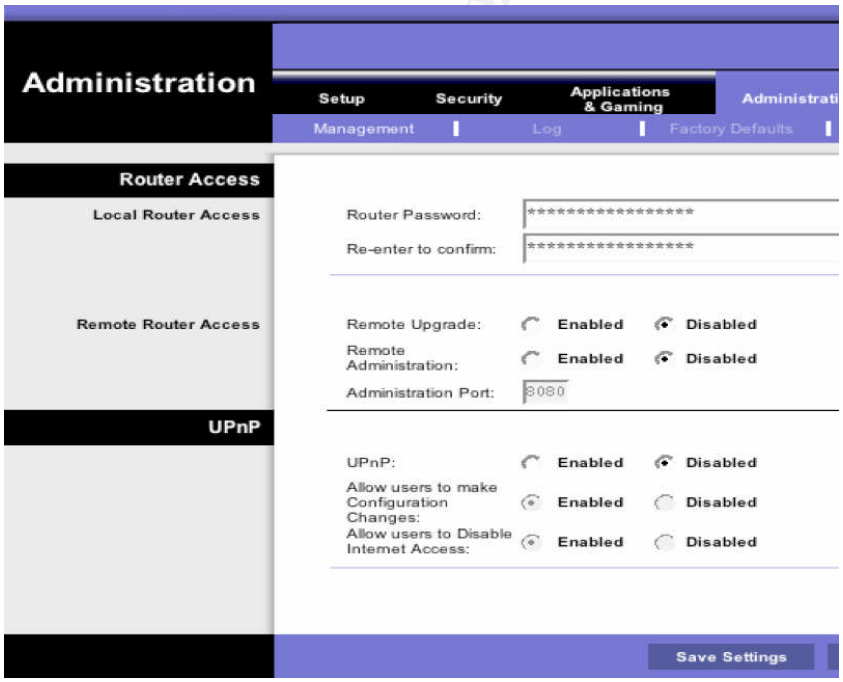

Diagram 1B

2.1.2 Windows XP SP2 Firewall (Tutorial)

The next security measure we will implement is a personal firewall. This one, in particular, is the new firewall built into Windows XP Service Pack 2. The personal firewall will restrict any external sources trying to reach the local Ethernet and built-in wireless access card. The following steps will configure the personal firewall to block all external sources to the laptop. By applying the personal firewall, we will also increase security when accessing public wireless networks. After configuration, no external sources should be able to communicate with our laptop while connected to a public wireless network.

- In order to launch and configure Windows Firewall from Windows XP SP2, go to: **Start -> Settings -> Control Panel -> Windows Firewall**

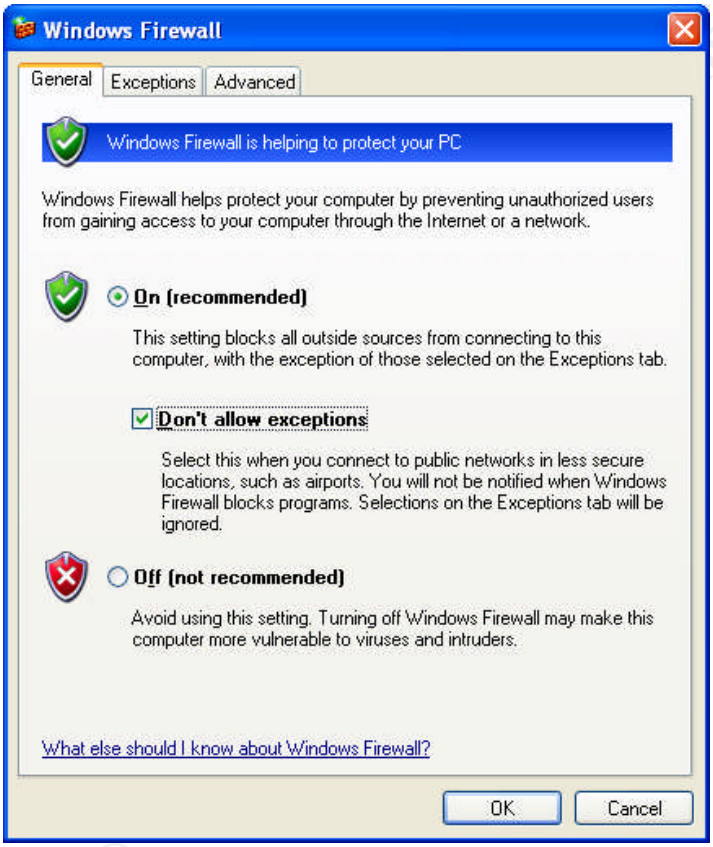

Diagram 2A

- Select the **"On"** and **"Don't allow exceptions"** options. This will enable the firewall and instruct it not to accept exception rules. This is the most secure setting, and will not allow external sources to connect to the laptop.

- The final step is to select the **"Advanced Tab"** and apply the firewall to the local Ethernet Connection and Wireless connection.

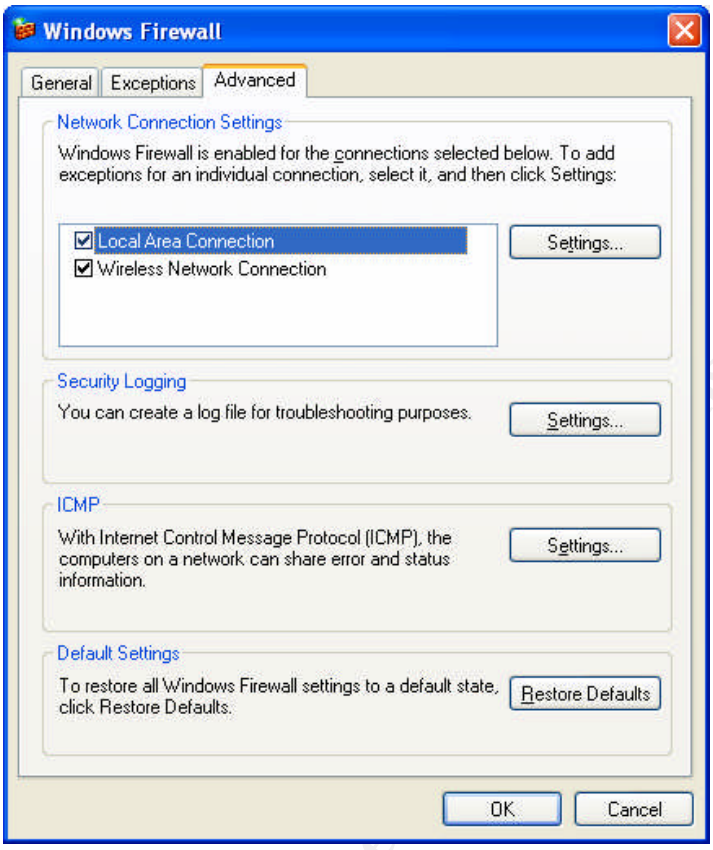

Diagram 2B

After going through the Linksys and Windows XP firewall tutorials, all devices in the LAN should have some type of firewall protection. This action should have also implemented the first statement from our security policy, which is "No external sources can initiate communication with any devices behind our firewall."

2.2 Wireless

One of the key forces for expansion in the mobile workforce is wireless network access. Wireless networks enable mobile workers to keep in touch with the enterprise from airports, hotels, restaurants and any location that has a wireless hotspot. Unfortunately this type of freedom has brought security issues to the forefront. According to Gartner **[6]**, "Ninety percent of mobile devices lack the protection necessary to ward off hackers, and the top security threat to mobile users is loss of a mobile device containing corporate data."

There are many methods to secure a wireless network. We will cover a few of the methods to help ensure your wireless access network is less prone to intrusion.

One of the key weaknesses in wireless security has been encryption and authentication. Users not employing encryption, or weak encryption algorithms, have been the primary culprits. No matter which encryption algorithm is available on an access point, you should enable the strongest option available. By not enabling encryption, wireless network access is clearly available and confidentiality is lost.

Wired Equivalent Privacy (WEP) was the first widely deployed wireless encryption algorithm. This algorithm is based on the RC4 algorithm and is typically available in 40 bit and 128 bit versions. The WEP algorithm has now been successfully attacked with many different approaches, including both active and passive attacks **[7]**. Because of the wide availability of tools to attack the WEP algorithm, many security experts are calling for all wireless networks to upgrade to a more secure algorithm.

One of the new wireless security standards is the WI-FI Protected Access (WPA) security standard **[15]**. The WPA standard addresses encryption and authentication for wireless networks. WPA leverages the Temporal Key Integrity Protocol (TKIP) for encryption and the Extensible Authentication Protocol (EAP) for authentication. While the combination of TKIP and EAP is not a silver bullet for wireless security, it does provide more security then WEP.

In order to make our wireless enabled host and wireless access point more secure, we will discuss enabling WPA to improve the encryption and authentication between these devices. In addition to enabling WPA, we will enable Media Access Control (MAC) address filtering, and disable the Service Set Identifier (SSID) broadcasting on the wireless access network.

2.2.1 Linksys Wireless Access Point (Tutorial)

Enabling WPA, MAC address filtering, and disabling SSID broadcasting will be the security measures used for the Linksys wireless access point. In Diagram 1A, you will notice that we have assigned the IP address 192.168.1.201 to the wireless access point. In order to implement the security measures, connect to the administration panel from the laptop using Internet Explorer. You may connect to the administration panel by going to the URL (http://192.168.1.201). For a more detailed explanation of how to implement changes to your Linksys, please refer to the online documentation **[16].**

After logging into the wireless access point, please make the following changes to make the wireless access point more secure.

- **Enable WPA**

We will implement WPA by using a pre-shared key and TKIP. In the wireless security menu, select "**WPA Pre-Shared Key"** for security mode and "**TKIP"** as the WPA algorithm. The final step is to choose a strong WPA Shared Key. We suggest you reference section 4.2.1 in this guide to choose a strong password as your key. Click "**Save Settings"** when done.

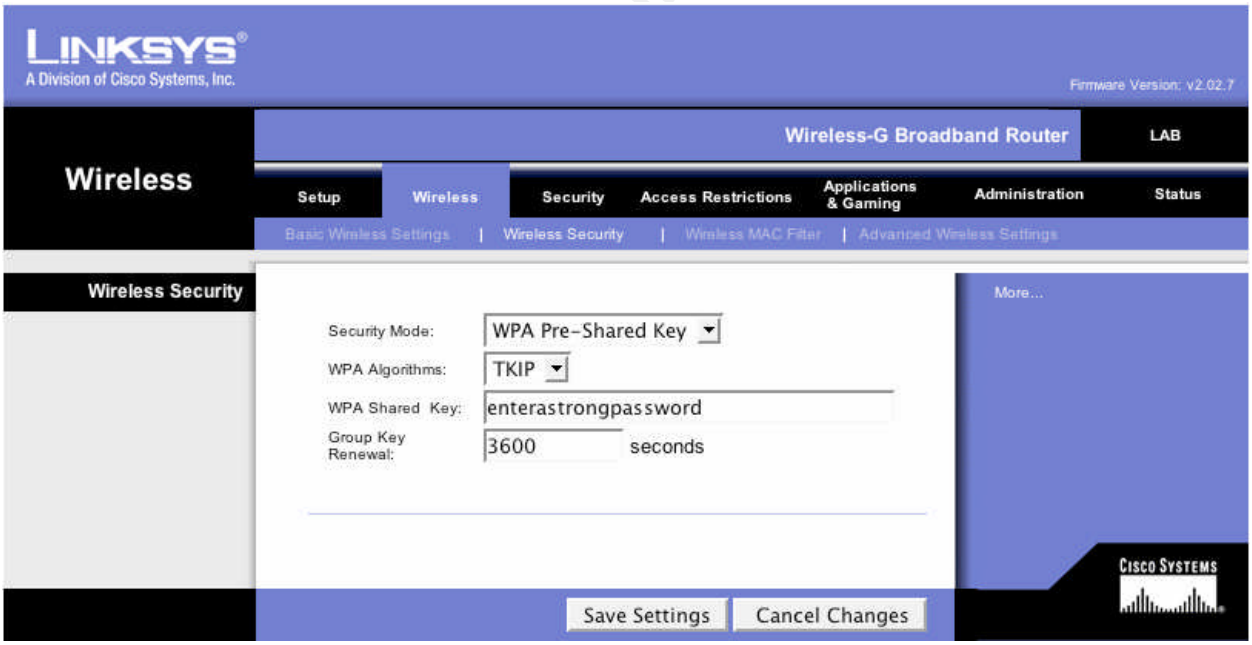

Diagram 3A

- **Rename and Disable SSID Broadcast**

In order for a wireless device to associate with a wireless access point, the SSID of the wireless access point of connectivity must be assigned. By default, most wireless access points publicly broadcast the SSID. Publicly broadcasting the SSID makes it easier for users to connect and use the wireless access point. Since we do not want other users sharing our wireless access point, renaming and disabling SSID broadcasting will make it a little more difficult to connect to our wireless access point. By default, the Linksys SSID is set to 'Linksys'. Since it is easy to guess a SSID, change your SSID to something not as easy to guess. Renaming and disabling the SSID is all done in the basic wireless settings menu. Rename the Wireless Network Name (SSID) and check the **"Disable"** option for Wireless SSID Broadcast. Click on "**Save Settings."**

Diagram 3B

- **Enable MAC Address Filtering**

The MAC address of a wireless access card is the unique hardware identifier for that network device. Since every wireless card has a unique MAC address, you can enable a range of valid MAC addresses that are able to access the wireless access point. The laptop is the only device that should have access to the wireless access point. In the Wireless MAC Filter menu, enable the **"Permit Only"** option and add the MAC address of the laptop by clicking on "**Edit MAC Filter List"**. When done, select "**Save Settings**."

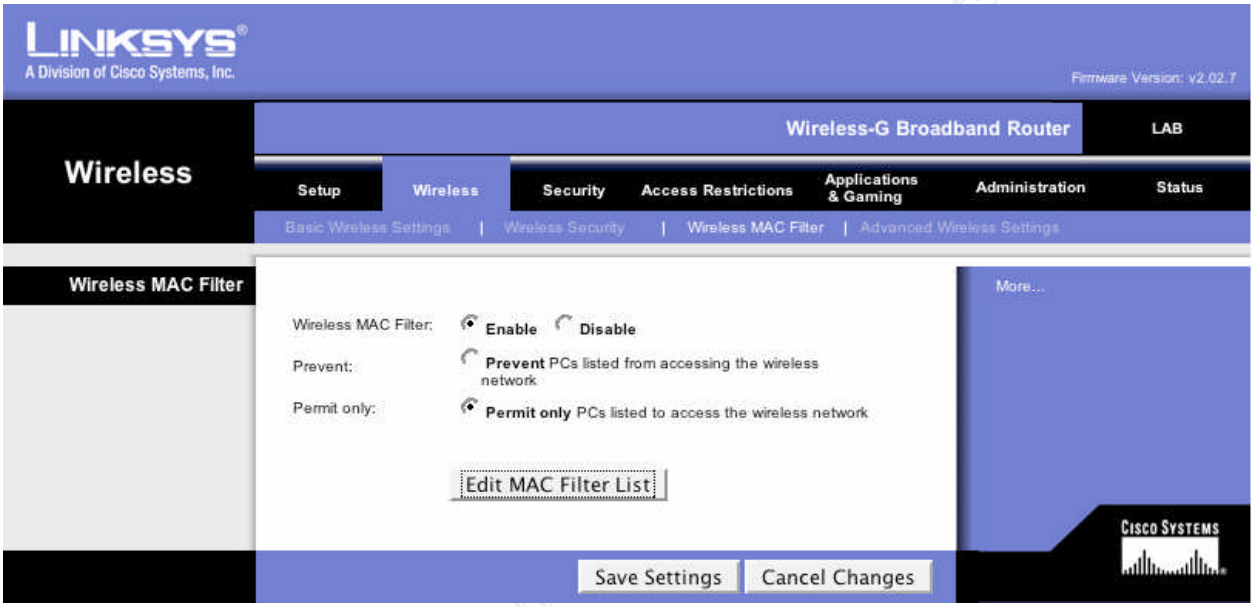

Diagram 3C

2.2.2 Windows XP Wireless Access (Tutorial)

In order for the wireless enabled laptop to connect to a wireless access point, we will need to configure the wireless network properties in Windows XP SP2 for WPA. The first step is to access wireless network properties by going to **START -> Settings -> Wireless Network Connections** and selecting **"Properties"**. Within **"Properties"** you will find **"Association"** settings. The first setting to change is the SSID. Set the Network name (SSID) to the name you chose in the previous tutorial. Next, choose a network authentication type. Since we want to use WPA, choose **"WPA-PSK"** as the network authentication type and **"TKIP"** as the data encryption type. Finally, enter the WPA pre-shared key you established on the wireless access point in the previous tutorial, and enter it into the network key field. After changing all the settings, select **"OK"**. The laptop should now be connected to the wireless network using WPA.

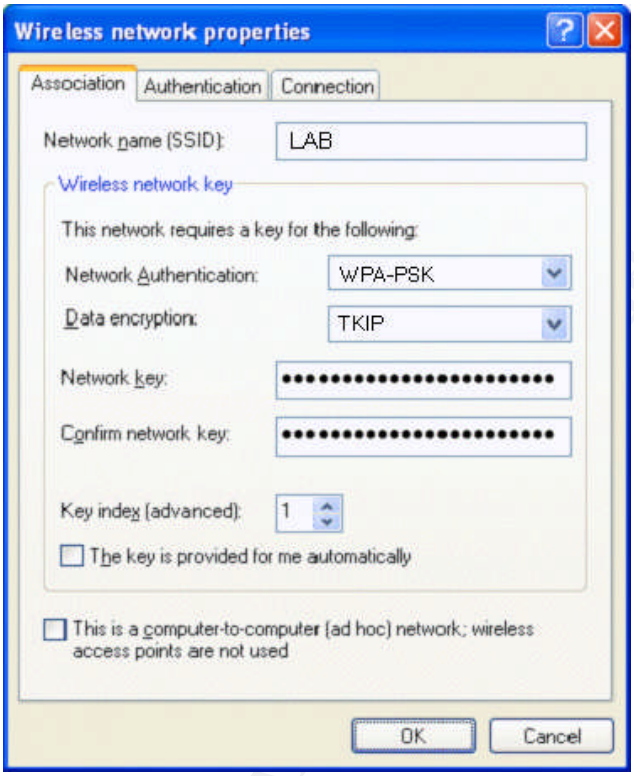

Diagram 3D

After going through the Windows and Linksys wireless tutorials, the wireless network created should be more secure. Defense in depth is the best approach to wireless security today. This tutorial should have helped to implement the second statement from our security policy, which is "Whenever accessing a wireless network, the most secure authentication and encryption protocols should be used."

2.3 Virtual Private Networks

Another technology that is driving the growth of the mobile work force is the Virtual Private Network (VPN). VPN technology (which can be hardware- or software-based) enables the mobile worker to create a virtual tunnel to a remote location and leverage corporate systems such as email. VPN technology has greatly reduced the cost of implementing remote office connectivity. For example, in the past, implementation of a secure connection between a Dallas and Houston office required a dedicated circuit. The approximate cost of this is $5,000 to $10,000 per month. VPN connectivity can now be implemented with an approximate cost of $100 to $500 per month. VPN is typically implemented over the public internet or a shared network. VPN's can be built with three basic components. The first component is the network connection between the client and server; this connection is also referred to as the tunnel. The next building block is authentication, which establishes the user of the connection. The last building block is encryption, which helps guarantee confidentiality. Most VPN implementations use all three building blocks. Authentication and encryption are options to make the tunnel more secure. We will discuss how to set up a basic VPN, and implement all three of these components. There are many types of VPN tunneling, authentication, and encryption implementations; we will cover the commonly used options available in Windows XP.

2.3.1 Microsoft Point to Point Tunneling Protocol (MS-PPTP)

"Out-of-the-box" Windows XP provides basic functionality for VPN connectivity. The most common way VPN connectivity is achieved in Windows XP is through the use of Microsoft Point-to-Point Tunneling Protocol (MS-PPTP). MS-PPTP establishes a virtual tunnel-over-IP and uses the Microsoft Point-to-Point Encryption (MPPE) protocol to encrypt data and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) for authentication. During setup, it is important that your MS-PPTP connection is configured with the most secure options available for authentication and encryption. There are a few options for authentication and encryption when using MS-PPTP. The most common Microsoft authentication protocols used are MS-CHAP and MS-CHAP Version 2. According to Microsoft, **[8].** "MS-CHAP provides a method of encrypted authentication and a challenge-response mechanism with a one way encryption on the response." Weaknesses in MS-CHAP, outlined by Bruce Schneier in his article "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", lead to the development of MS-CHAP Version 2. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data **[9]**. We suggest only enabling MS-CHAP version 2 when connecting to a remote VPN using MS-PPTP VPN technology. The Microsoft encryption protocol MPPE has 40 bit and 128 bit versions available. We suggest using only the 128-bit version of MPPE, also known as Microsoft Strong Encryption.

2.3.2 Microsoft VPN (Tutorial)

When setting up your Windows XP based-VPN through the network connection wizard, be sure to ask your VPN administrator which are the most secure options for your connection. When connecting to a MS-PPTP based VPN, we suggest that you enable maximum-strength data encryption MPPE 128 bit and Microsoft CHAP version 2 for authentication. The encryption and authentication options can be set in the **"Advanced Security Settings"** menu.

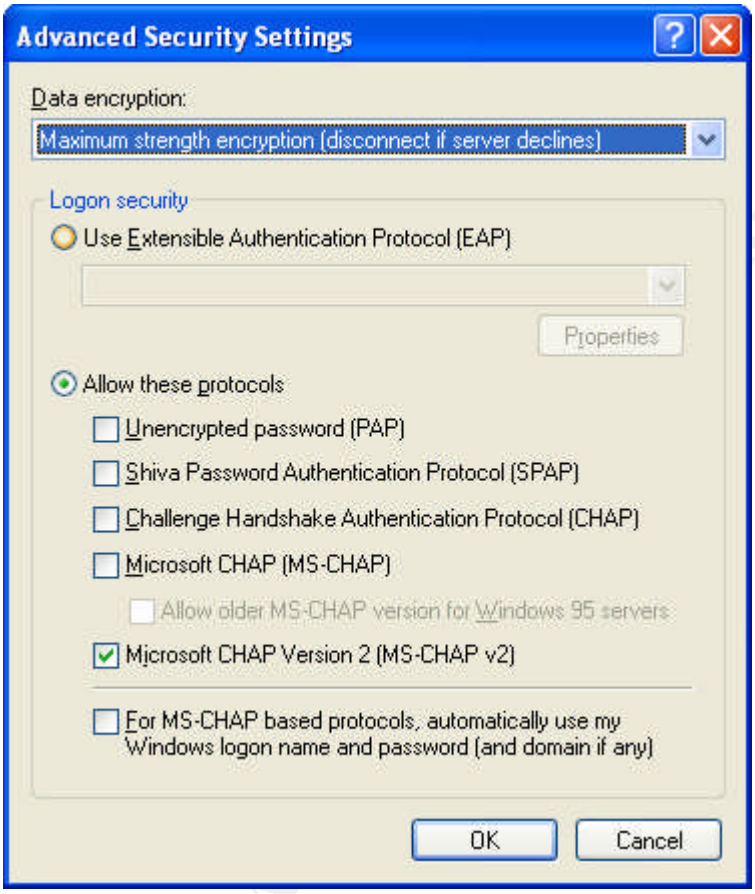

Diagram 4A

3.0 Host Security

One of the most important and expensive assets to protect is your laptop computer, which we will refer to as "the host." We will explore several different approaches to ensuring confidentiality, integrity, and availability of information on a laptop. Our guide assumes your host operating is system Windows XP. In this section, patch management, security configuration, and security applications will be the primary focus. In patch management, we will cover the Windows Update Service (WUS), and highlight other key aspects of application patch management. The security configuration section will focus on basic operating system and application configuration changes that will make the host more secure. As we round out host security, we will look at a few security applications such as virus scanners and spyware tools.

3.1 Patch Management

According to the CERT 2003 Annual Report **[10]**, the two most serious intrusion activities are the Sobig.F Worm and MS-SQL Server Worm. Both of these malicious internet worms leveraged software vulnerabilities in Microsoft software. The key to keeping a host secure is maintaining operating system and application software patches. Microsoft delivers Windows XP patches in an automated fashion by the Windows Update Service (WUS). In addition to operating system patches, Windows Update provides patches for applications such as Internet Explorer and Outlook Express. Patches are usually a fix to a known bug in the operating system or application code that allows for unexpected or malicious behavior to occur. For example, in June 2004, a critical exploit, "Download.ject" was released on the Internet. It leveraged known issues in Internet Explorer to load a backdoor program onto an unsuspecting user's PC **[11]**. Within a few weeks, Microsoft released Windows XP Service Pack 2, which contained several patches for Windows XP and Internet Explorer that fixed the Download.ject vulnerability. Typically, there are a handful of exploits for Windows XP reported each month. In order to maintain a host's security, it is critical consistently apply the latest patches. Because some security patches can break or constrain capabilities when applied, it is important to research and test patches before installing them to a host. In order to keep up with new Windows XP vulnerabilities, we suggest frequent visits to vulnerability reporting websites like SecurityFocus.org. SecurityFocus and other vulnerability websites usually cover the technical details of the exploits and vulnerabilities and also provide remedy information to fixing them.

3.1.1 Windows Update Service

Patch management for Windows XP and Microsoft Office has been made simple by the new version of Windows Update Service (WUS). The easiest and most secure setting for the Windows Update Service is the automatic download and installation of the updates to your host. This setting should work for most intermediate users who do not have such third party applications installed on their systems. WUS is very intelligent and has the capability of knowing what is installed on a system and which software

patches are required from Microsoft. The service also provides a reporting capability that reports which patches have been installed.

3.1.2 Windows Update Service (Tutorial)

This tutorial covers configuring the Windows Update Service for Automatic Updates and viewing the patch installation history.

- **Launch the Windows Update Service**
  The Windows Update Service will be launched from Internet Explorer and can be found by a shortcut in the **START** toolbar in Windows XP.

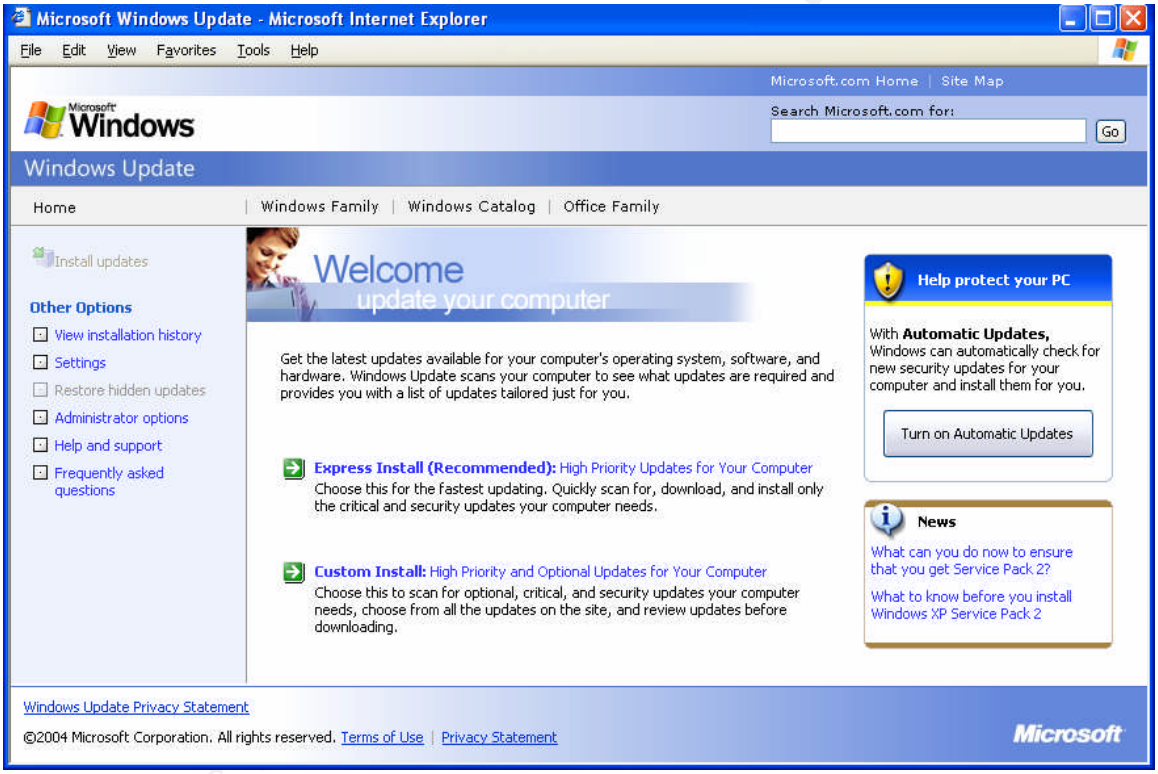

Diagram 5A

- **Enable Automatic Updates**
  In order to ensure the host automatically receives the critical Microsoft updates, enable the **"Automatic Update"** feature. Choosing "Turn on Automatic Updates" from the screen referenced in diagram 5A does this. Set up the service to check for updates every night at 3:00 AM. You should always leave your host powered on and connected to the Internet.

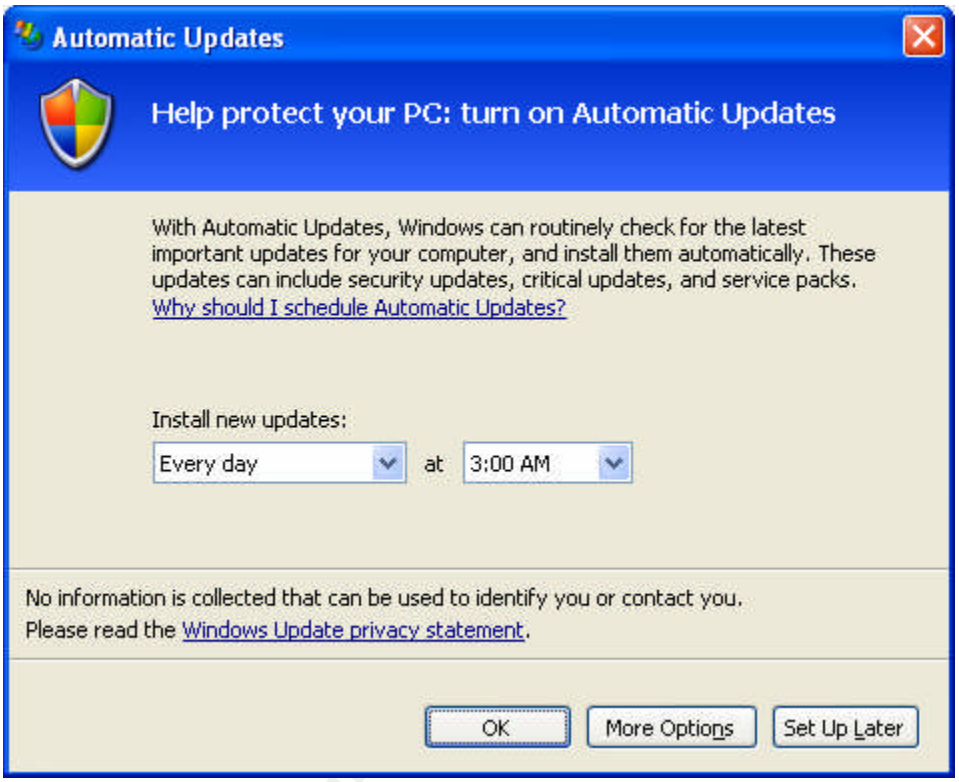

Diagram 5B

- **Patch Reporting**
  Viewing your patch history is important to make sure your Windows Update Service is working and to keep up with security updates that are being sent to your host. By choosing the **"View Installation History"** option you will show all the patches installed. If you click on a single patch name, you may view the details of a certain patch.

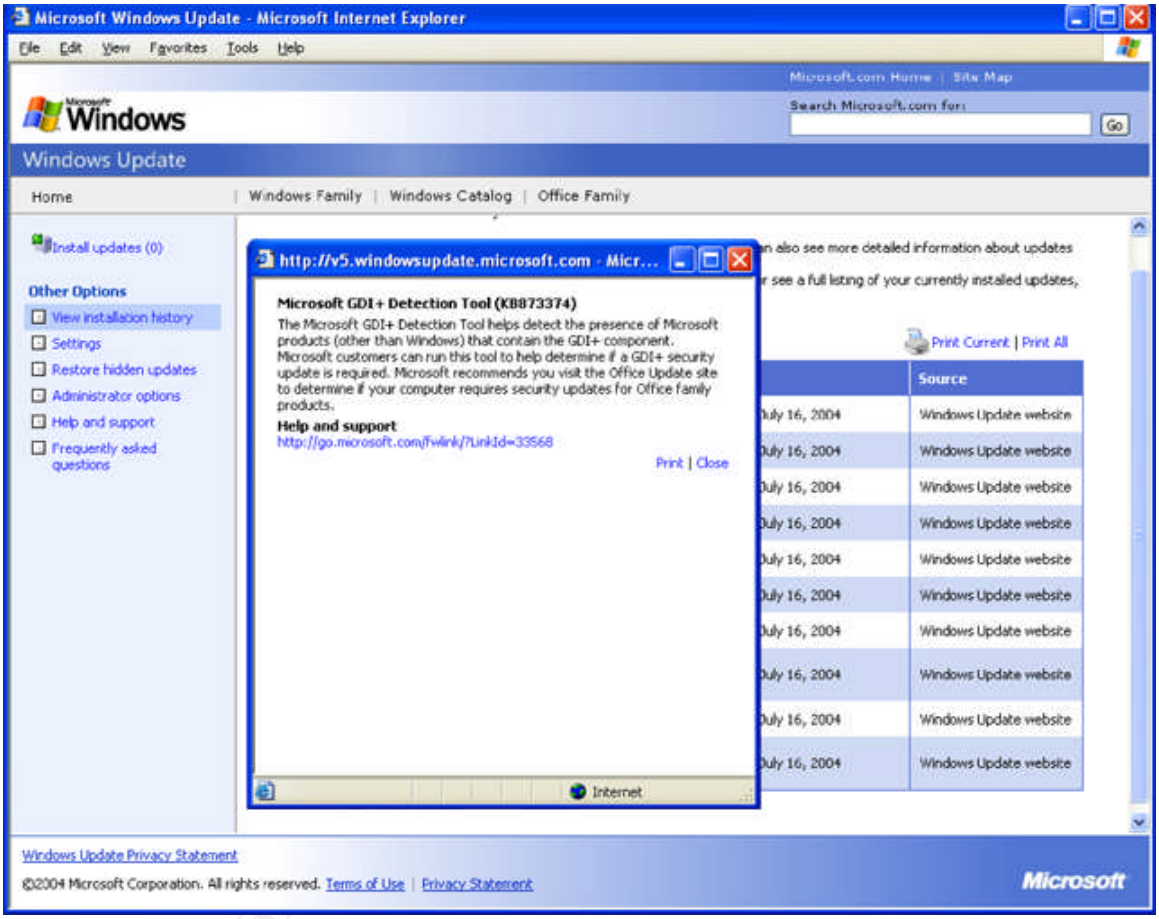

Diagram 5C

3.2 Host Security Configuration

Ensuring all the components of your operating system use the best security settings is essential in maintaining a deeper layer of host security. While there are many settings in Windows XP that can be configured to be more secure, our guide covers the top three issues that put your system at the highest risk. The lack of user account passwords and strong user account passwords is the first issue we will cover. Disabling unwanted Windows Services will be the next topic explored. Last, we will discuss enabling an encrypted file system to protect your personal documents and data.

3.2.1 Passwords

Mobile workers are often travelers or remote employees. Related activities make computers accessible to the outside world and more vulnerable to physical access to a computer. Passwords are one of the last safeguards in protecting a host and the data contained within. A common first mistake when setting up a host is not establishing a password for user accounts. A password should exist for every user account. In addition to setting up a password for every user account, a "strong" password should be selected for every account. There are different industry definitions for "strong" passwords and "weak" passwords. The Microsoft guide for establishing a strong password is a good reference.

The Microsoft guide refers to these common practices for establishing a strong password **[12].**

- A password that is 7 or 14 characters in length should be selected
- Passwords should contain characters from the following groups
    - Letters (uppercase and lowercase)
    - Numerals
    - Symbols (all characters not defined as letters or numerals)
- Passwords should contain one symbol character in the second or sixth position
- Passwords should be different then any prior passwords
- Passwords should not contain your name or username
- Passwords should not use any common words or names

Other then setting up a password for every user account and choosing a strong password, we suggest changing a password every 90 days, never sharing a password, and never leaving a written password on or near a computer.

3.2.2 Windows XP Passwords (Tutorial)

In this tutorial, we will cover the quickest way to configure a strong password in Windows XP. In order to change the password for a user account, the "NET USER" command can be used. By running the command **"NET USER [USERNAME] /random"**, Windows XP will generate a random 8 character password and assign that password to the user account. In our example below, the user administrator is assigned the password **"QbuTGA6l."**

Diagram 6A

After going through the Windows XP tutorial, the administrator account on the host will be assigned a stronger password. This tutorial also partially implements the third statement from our security policy which is, "All systems should have strong passwords enabled."

3.2.3 Windows XP Services

"Windows Services" are operating system processes that run in the background and process requests from a network or other applications. By default, Windows XP has almost all services enabled. While you may need many of the services, it is good security practice to disable all unnecessary services. A few services most people disable are the "alerter" and "remote registry" services. The "alerter" service allows users and computers to send administrative messages. While this is a useful feature, there have been exploits and denial of service attacks developed for this service. Microsoft apparently agrees that disabling this feature is good practice and has now by default disabled this setting in Windows XP Service Pack 2. The "remote registry" service allows remote hosts to edit your local registry settings. Since the local registry contains the heart of all security settings it is not good practice to allow remote hosts this access. To our knowledge this service is still enabled by default in Windows XP Service Pack 2. We suggest disabling if possible and reading about other windows services that can be disabled. Many resources are available on the Internet about this topic.

3.2.4 Windows XP Services (Tutorial)

For this tutorial, we suggest you research Windows XP services that may be disabled. Once you have decided which services to disable, do the following in the windows service management console.

- In order to launch the windows services management console, go to:
  START > Settings > Control Panel > Administrative Tools > Services

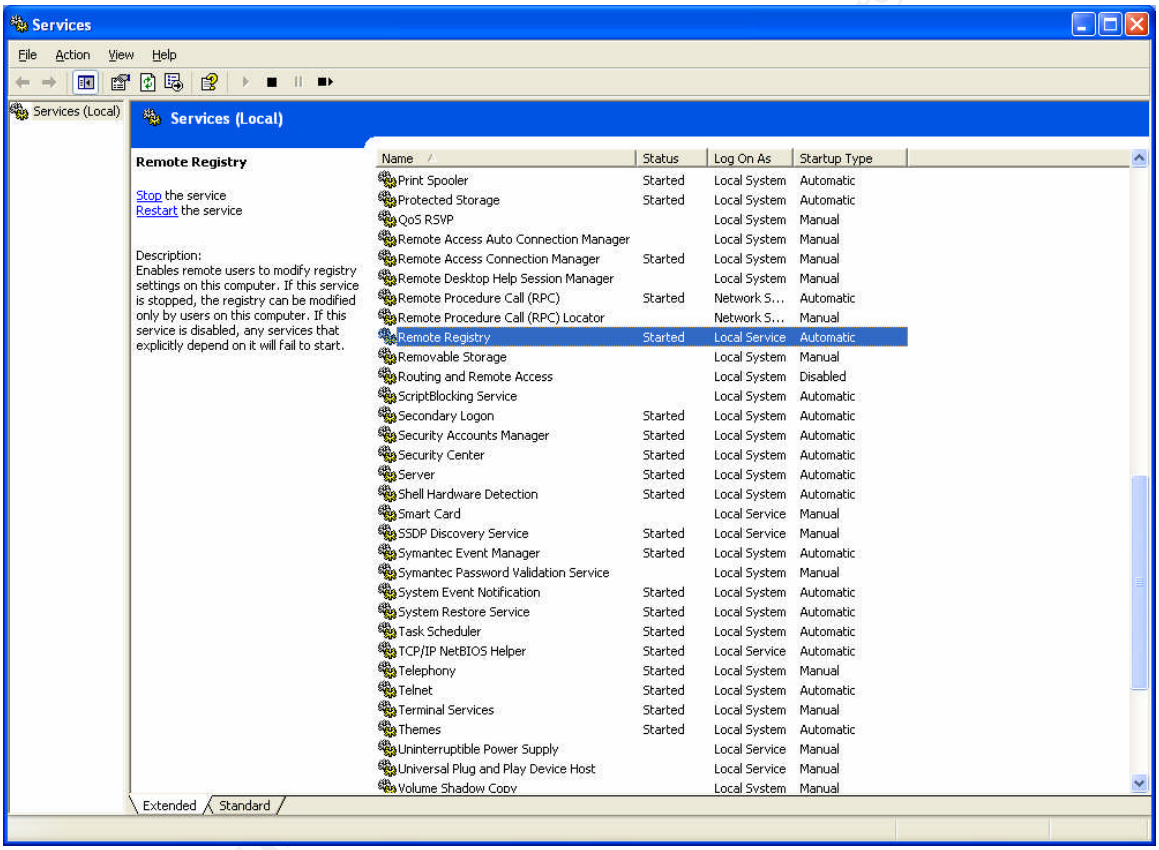

Diagram 7A

- You will enter the service configuration menu by right clicking on the **"Service Name"** and selecting **"Properties"**. In this menu select **"Disable**", click the **"Stop"** button and finally select **"Apply."** This will halt the service immediately, and disable the service from launching the next time your host is restarted.

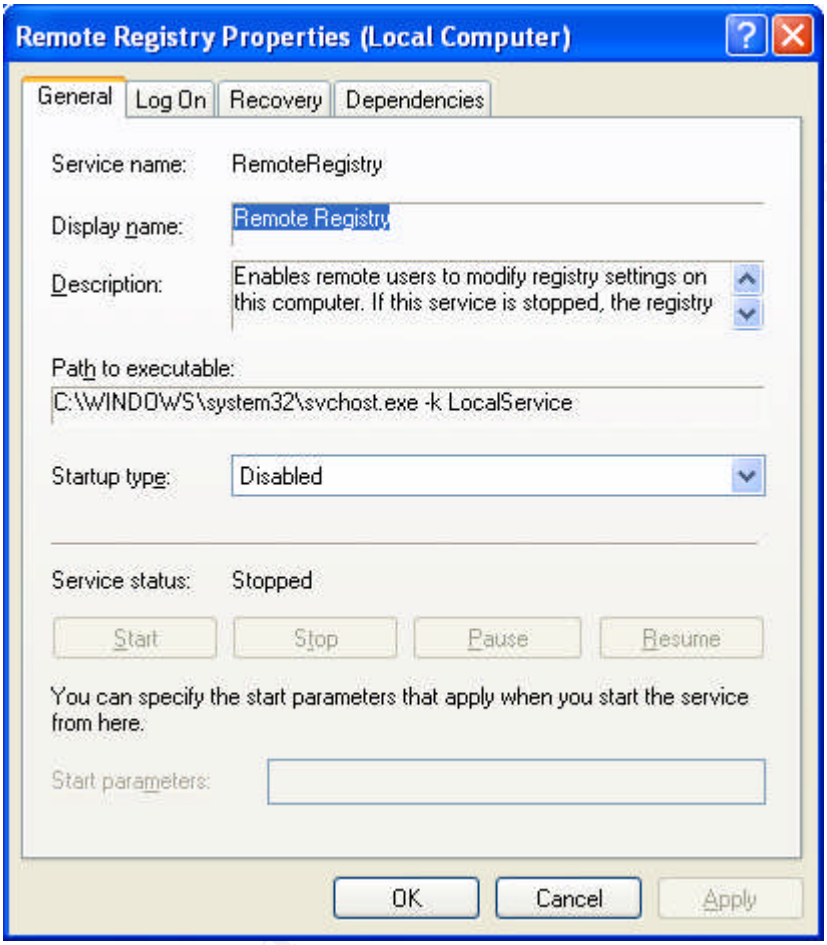

Diagram 7B

3.2.5 Windows Encrypted File System

If a host is ever stolen or accessed physically without your knowledge, it is simple for another user to bypass all security measures and copy documents and data from your machine. In order to provide another level of confidence that sensitive documents and data stored on your host will remain confidential it is a good idea to consider file encryption. In order to enable this functionality, Windows XP Encryption File System (EFS) should be implemented. EFS Provides DESX, 3DES and AES encryption that may be applied to any folder on your computer **[13]**. EFS uses a randomly generated File Encryption Key (FEK) to encrypt and decrypt data. The FEK is a symmetric encryption key and is encrypted with public and private key pairs the first time EFS is used. It is a good idea to back up the public and private EFS keys and store them in a safe location. The private and public key pairs can be used to recover data from your host if a user account password is lost.

3.2.6 Windows XP EFS (Tutorial)

This tutorial will cover enabling EFS to encrypt the **"My Documents**" folder**.** The **"My Documents"** folder on most Windows XP hosts is where personal documents and data are stored.

- In order to encrypt the **"My Documents"** folder with EFS, simple right click on the **"My Documents"** folder and select **"Properties"**. Next, select the **"Advanced Option"** in the **"Properties"** menu. In the **"Advanced Attributes"** menu, check the **"Encrypt contents to secure data option"** and then click **"OK."** This will immediately encrypt the **"My Documents"** folder with the default EFS encryption.

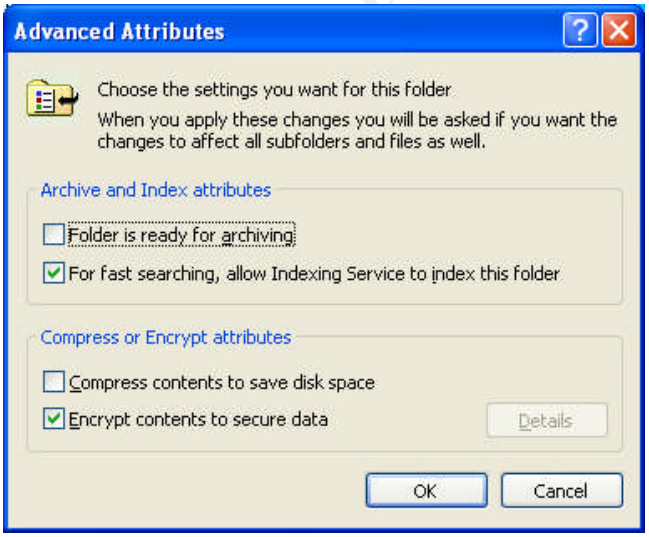

Diagram 7C

- After completing the Windows XP EFS tutorial, personal data on the host should be more secure. This tutorial should have helped implement the fourth statement from the security policy, which is **"**All personal documents and data need to be protected by encryption."

3.3 Security Applications

As security threats such as viruses, worms, and spyware multiply over time, new software applications are developed to prevent such threats from infecting the host operating system. Generally viruses and worms are malicious code that is developed with the intention to alter the behavior of a host without your knowledge. A virus is a stand-alone program that infects a host file and requires some interaction to replicate. A worm may not always infect a host file, and has the advanced capability of self-replication across a network. In the past few years' worms have become more common and advanced in their capabilities **[14]**.

Even though we have implemented a software and hardware firewall in this guide, the host is still susceptible to viruses and worms. Antivirus applications are the answer to detecting and removing viruses and worms from a host. Today, antivirus applications usually have two operating modes. The first operating mode is "real-time" detection. Real-time detection allows an antivirus application to detect a worm or virus as a user checks email or surfs the web. The capability of real-time virus- and worm-detection is an essential tool you need to make sure your host is not being compromised.

The second operating mode of antivirus application is "manual mode." In manual mode, the antivirus application will manually scan all the files and configuration data on your host and detect any viruses or worms that may have not been detected in the real-time mode. The manual scanning process is time consuming and should only be run every few days, as long as real-time mode is enabled.

The other key element to an antivirus application is the virus definition file. The definition file contains all the virus descriptions and information necessary to detect and remove new viruses and worms. Usually new definitions are released every few days to handle all new developing threats. It is important your antivirus application is kept up to date with the latest definitions; otherwise the antivirus application is rendered useless.

Spyware is another fast-growing threat on the Internet. Spyware's general intent is to track and collect personal information about a user and their Internet activity. Spyware is typically loaded onto a host from a malicious website or email. Spyware usually comes in the form of a small program or malicious browser cookie. Once spyware is loaded in a host, it will usually report back to an advertising or malicious server with your activity and personal information. While it is always good to set the highest security settings on your web browser and email application to help prevent spyware from infecting your system, you should also install an anti-spyware application.

Anti-spyware applications usually have a "real-time" and "manual operating" mode like the antivirus applications discussed above. If available, we recommend running the anti-

spyware application in both modes. Anti-spyware applications will detect and remove different forms of spyware. Anti-spyware applications also use a definition file which informs the application of new types of spyware. It is important that you keep your anit-spyware definition file up to date as well. New security applications like Norton Antvirus 2005 are starting to detect and remove spyware. Until the antivirus application vendors have a more robust spyware detection capability, we suggest using separate applications.

3.3.1 Antivirus and Spyware (Tutorial)

In this tutorial, we will cover the basic setup and overview of Norton Antivirus 2005 and Ad-Aware SE.

- **Symantec Norton Antivirus 2005**

Symantec Norton Antivirus 2005 is the latest antivirus software from Symantec. Symantec is one of the industry leaders in antivirus software. After installing Norton Antivirus, make sure to enable the following options, **Auto-Protect**, **Email, and Automatic LiveUpdate**. Symantec requires you to renew your antivirus definition subscription service once a year. As discussed earlier, keeping your virus definitions up to date is critical. For further support in configuring Norton Antivirus, we suggest visiting their online support site.

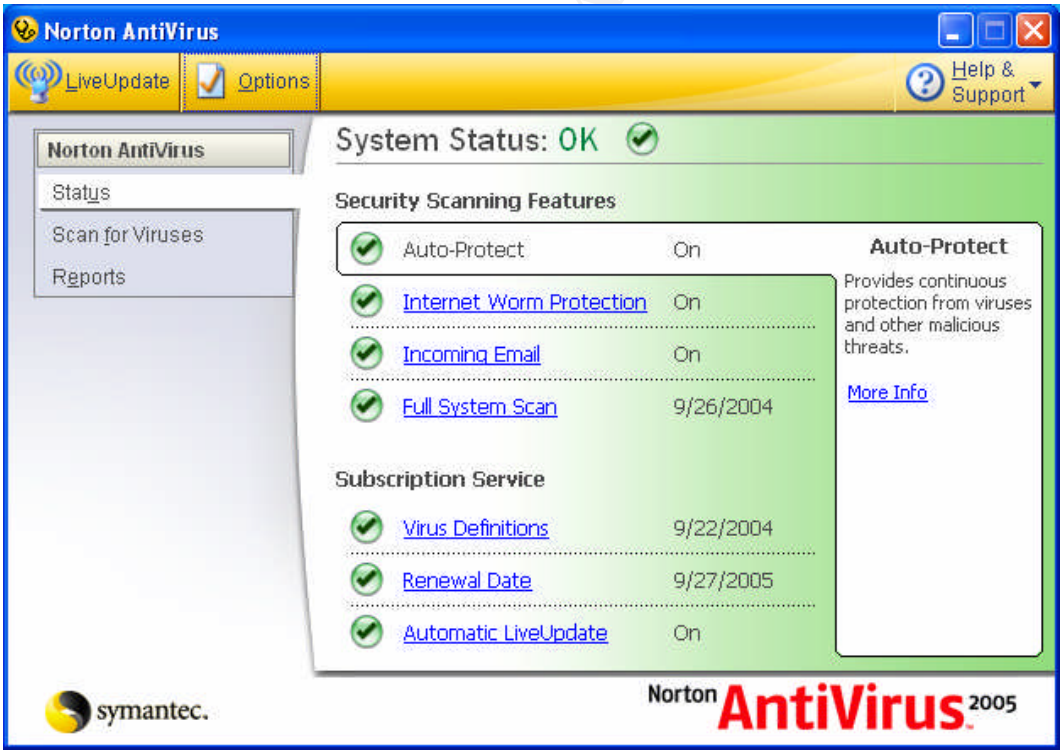

Diagram 8A

- **Lavasoft Ad-Aware SE**

Lavasoft Ad-Aware SE is a widely used spyware detection and removal tool. The SE personal edition of Ad-Aware is freely available on Lavasoft's website, http://www.lavasoft.de. After installing Ad-Aware, we suggest updating the definition file and running a deep system scan. After running a deep system scan, you will be shown a list of all the traces of spyware found on your host. In order to remove the spyware, simply select all the spyware occurrences' you wish to remove and click the **"Next"** button.

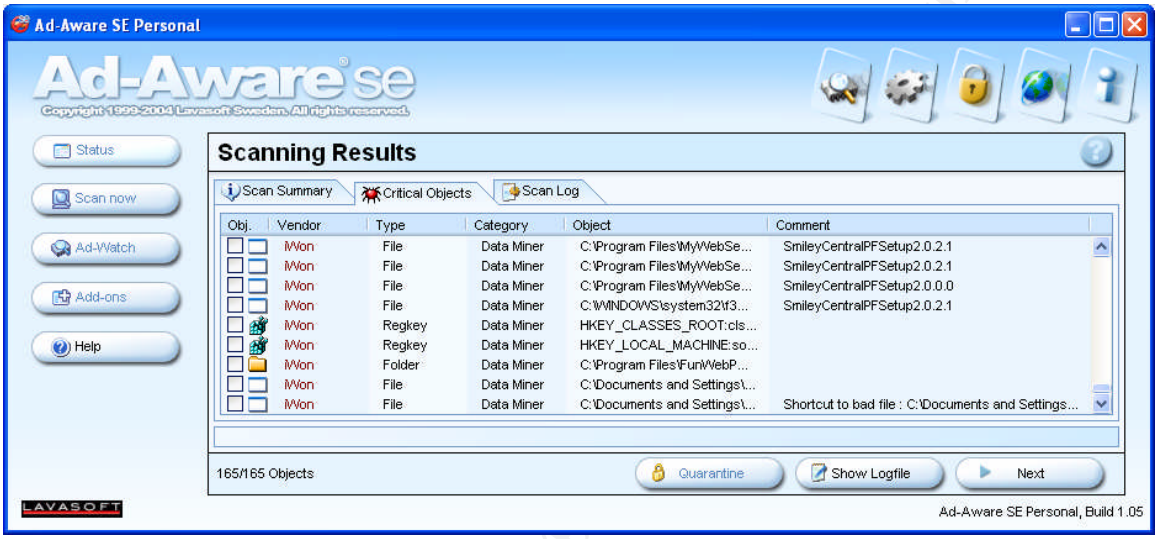

Diagram 8B

After completing the security applications tutorial, data on the host should be more secure from viruses and spyware. This tutorial should have helped to implement the fifth statement from the security policy which is, **"**Protection against viruses and spyware should be provided."

4.0 Conclusion

Defense in depth is the key to maintaining security for the mobile worker. A security foundation is established when a comprehensive security policy is implemented. The mobile worker should continually review their policy and always keep security in mind whenever making a change to an environment. This guide only covered the basics of network and host security. Firewalls, patch management and antivirus software are the basic essential components every mobile worker needs. Maintaining these components will ensure a basic level of security within the mobile worker's environment. Security education is a crucial element in keeping the mobile worker secure. New threats are being developed everyday and mobile workers must continually educate themselves about new security threats and solutions for mitigating risk from exposure to these threats.

5.0 References

[1] Pratt, Joanne H. “Teleworking Comes of Age with Broadband.” Telework America Survey 2002. April, 2003. http://www.telecommute.org/pdf/TWA2003_Executive_Summary.pdf

[2] SANS. The Twenty Most Critical Internet Security Vulnerabilities. October, 2003. http://www.sans.org/top20/

[3] Srisuresh and Holdrege. RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations. August, 1999. http://www.faqs.org/rfcs/rfc2663.html

[4] Linksys. Etherfast Cable/DSL Router User Guide. ftp://ftp.linksys.com/pdf/befsr41V3_ug.pdf

[5] Hart, Jon. Linksys BOOTP Memory Leak. May, 2004. http://www.securiteam.com/exploits/5DP0A20CVC.html

[6] Gartner. “Mobile Users Careless With Wireless Security.” E-Week. March, 2004. http://www.findarticles.com/p/articles/mi_zdewk/is_200403/ai_ziff123118

[7] Borisov, Goldberg and Wagner. Security of the WEP algorithm. 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[8] Microsoft Corportation. Local and Remote Network Connections. 2001. http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/prork/prcg_cnd_qwpl.asp

[9] Schneier, Bruce. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). 1999. http://www.schneier.com/paper-pptpv2.html

[10] CERT Coordination Center. 2003 Annual Report. April, 2004. http://www.cert.org/annual_rpts/cert_rpt_03.html

[11] Microsoft Corporation. What You Should Know About Download.Ject. July, 2004. http://www.microsoft.com/security/incident/download_ject.mspx

[12] Microsoft Corporation. Creating Strong Passwords. 2004. http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_password_tips.mspx

[13] Microsoft Corporation. “EFS Files Appear Corrupted When You Open Them”. Knowledge Base Article 329741. December, 2003. http://support.microsoft.com/default.aspx?scid=kb;en-us;329741

[14] Symantec Corporation. What is the difference between viruses, worms, and Trojans? February, 2004. http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106

[15] Ellison, Craig. “Wireless Security: WPA Step by Step,. October 2004.” PC Magazine. http://www.pcmag.com/article2/0,1759,1277020,00.asp

[16] Linksys. Linkys Wirleless-G: Quick Installation. 2004. ftp://ftp.linksys.com/qinstalls/wkpc54g_qi.pdf