Global Information Assurance Certification Paper

Defense-In-Depth Concept Solution
Applied to a Wireless
Windows XP Operating System (OS) Home Network
Charles J. Dumas
February 13, 2004

Introduction/Abstract

This document will attempt to offer knowledge and guidance in applying a defense-in-depth concept solution to a wireless Windows XP Operating System (O/S) baseline home network environment connected to the Internet via high-speed cable modem for typical family users. Typical family users include Dad, Mom and 3 school age children. The primary usage of the network will include Internet surfing, electronic mail otherwise known as e-mail, word processing and computer games. The home network will also be used for musical, video, and digital picture entertainment. This practical project will be in real time. Specifically, real time refers to while this paper is being written I will actually be purchasing the computer equipment, setting up the wireless network, and describing and applying each security layer otherwise referred to as defense-in-depth concept solution. Therefore, I will first cover computer equipment purchase, home network set-up and connectivity description design, and each defense-in-depth concept solution as it applies from system acquisition to operation. My defense-in-depth concept solution will include some knowledge of wireless security concerns and countermeasures, physical security, security plan development, firewall router combination technology deployment and configuration, consistent O/S patching, anti-virus software application, and file/folder encryption methods.

According to the world's leading resource for Internet trends and statistics NUA Internet Surveys, "the art of estimating how many are online throughout the world is an inexact one at best. Surveys abound, using all sorts of measurement parameters. However, from observing many of the published surveys over the last two years, here is an educated guess as to how many are online worldwide as of September 2002. And the number is 605.60 million." In my opinion the number of Internet users is astronomical—quickly soaring towards the billions. The total number of Internet users with malicious intent is co-related to the number of users on the Internet. As long as the number of Internet users keeps escalating so will the number of users with malicious intent. Vincent Wallace author of Personal Firewalls: Not Enough states, "With the proliferation of residential broadband more and more users are able to satisfy their craving for always-on Internet access. As the subscription to Digital Subscriber Line (DSL) and cable modem services grows, so does the

size of the playground for malicious users." Most subscribers are oblivious to the threats and vulnerabilities that accompany the 'always on' the Internet luxury. DSL and cable modem services have opened up yet another challenge for computer security professionals to combat. Even though there are a large number of people who are not proactive in protecting their computer resources there are many who know the threat of malicious users is real and so they are taking steps to protect themselves. Thus the concept defense-in-depth becomes more talked about and more likely to be applied in our effort to defend computer hosted information's confidentiality, integrity and availability. Defense-in-depth concept solutions are, by far, currently, the best computer network defense philosophies on the market.

What is Defense-In-Depth?

For starters let's take a brief look at what people are saying about these Information Technology (IT) 'buzz' words defense-in-depth. There are many computer security professionals out there talking about what defense-in-depth means and how to apply it. I have read many good definitions and explanations concerning defense-in-depth, but the one that perked my intellect came from Dr. Frederick B. Cohen. Even though most computer security professionals will agree there is nothing that can stop a determined, well-trained, and well-equipped malicious computer user from invading an Automated Information System (AIS). Only deterrence can be obtained in the cyberspace world we live in today. This is truly 'Bad News'. But, Dr. Cohen so eloquently said, "The good news is that the technique of defense-in-depth tends to provide ample redundancy to withstand new attack mechanisms well enough to study the attack and improve the bypassed mechanisms. This is a vital point because with such a mechanism, we are now in a proactive posture, where defenders are not 'chasing' attackers, but rather attackers are 'chasing' defenders." For example, if an intruder or malicious code makes its way through your router/firewall and gains access to your computer and your computer is properly patched and using updated anti-viral software, and proper file sharing and file encryption methods, the intruder will be faced with more defense mechanisms and the chance of deterrence and resources being protected is significantly increased. Now, Dr. Cohen's words were in support of layered anti-virus software applications. Never-the-less, defense-in-depth concept solutions can be applied to every level where a system can be accessed. Now that I have laid some foundation to my project let's move on to the computer system purchase.

Computer Purchase

Typical home users can purchase a decent computer system for as little as $599 or less. This purchase would typically include a computer processing unit (CPU), monitor and keyboard, possibly a printer and/or some other type of upgrade(s) depending on the company selected. Basic and advanced computer users may have different outlooks on the type of system required. For example, if you consider yourself an advanced computer user or if you plan to work with videos, music, and computer gaming, you may require a system with more memory and faster processing speed. The more you increase processing speed, memory, and hard drive space the more expensive the computer system will become. Anyhow, the time has come to purchase a new Personal Computer (PC)! So, what is the right PC for you? It is a very big decision—especially since the computer market is so competitive. Wait a second; PC purchasing won't be as bad as you think. DELL provides a neat web site and very competitive marketing pitches. The web site provides an informative look at PC buying and some marketing pitches that will surely raise an eyebrow. The web site will guide you through a methodical process and provide you with valuable information to help you with your selection. Your equipment selection will determine the potential and future upgrades of your system. Your system capabilities can range from a simple word processor to a system quickly processing videos, computer gaming, music and movies. "It's not as daunting a task as you may think. And once you've evaluated your needs, made your decision and purchased your new system, you can rest assured in the knowledge that you're getting the most from that PC and from your PC investment" (dell.com 2004). Yet and still there are many companies and many deals to choose from. In this day and age I consider the computer industry to be noting less than 'Booming'. I chose DELL. DELL's web page is designed to take you step by step through the process of purchasing either a stand-alone computer or components to build a small or large home Local Area Network (LAN). The web page will assist you in gathering a basic understanding of processors and memory, hard drive storage space capacity, monitor display, multimedia, Internet access, O/S and software packages, and peripheral devices. By visiting the web page you learn processing speed is measured in gigahertz (GHz), memory is measured in megabytes (MB), and storage capacity is measured in gigabytes (GB). Thus when you see these terms used for system description you will know what they mean and be able to speak intelligently about them and make an informed decision on what system is best for you. You will also learn about the different processor developers (Pentium and Celeron), different Random Access Memory (RAM) types (SDRAM, DDR SDRAM, and RDRAM), and different types of storage devices (Floppy Drives, CD-ROM, DVD, CD-RW, ZIP, USB port,

and Combination Drives). I spent a few hours studying the computer purchase section of the web page, and you know what, it was well worth the time invested. My network consists of the following:

2 PCs with various processors, memory, and storage space (Windows XP O/S) (Dell purchased)
2 monitors (Dell purchased)
2 Universal Serial Bus (USB) 1180 wireless adapters 820.11b technology (Dell purchased)
1 Wireless Router 820.11g technology (purchased at Best Buy D-Link DI-624)
1 HP printer (previously purchased)
1 additional PC (previously purchased)

NOTE: I did choose some upgrades to my monitors, processors, memory speed, and hard-drives. These upgrades significantly raised the cost of my computer systems. Please see the web page below for more detailed information.

Network Design

My network design consists of a cable modem Internet connection connected to the wireless router, 1 PC with a hard connection to the router, 2 PCs using 1180 wireless adapters connect to the Internet through the wireless router via wireless connection, and 1 printer connected to the PC that is directly connected to the router. The LAN was fairly simple to set up. All new components came with easy to follow instructions and pictures. DELL and Microsoft provide a host of avenues to obtain help in configuring your computers. I used Network Setup Wizard to get me started configuring my systems. The wizard provided a neat checklist and step-by-step procedures to get me under-way. To start the Network Setup Wizard, click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**. Under **Common Tasks**, click **Network Setup Wizard.** For the purpose of this paper I will not expound any further on setting up the network. Once my systems were all set up and properly connected it was time to deploy defense-in-depth layers. Before we began with the first defense layer (physical security), let's look at a quick overview of wireless security concerns and countermeasures.

Wireless Security Concerns and Countermeasures

Wireless technology is yet another component of Information Technology (IT) development that has quickly appealed to the consumer. Despite the fact that

wireless technology development caters mostly to convenience first and second to security concerns, it is becoming a more and more preferred way to build network infrastructures. Sadly, in my opinion wireless technologies developers are right on track with the 'convenience over security' development philosophy, because 'WE' as Americans are unwilling to compromise convenience and worry very little about vulnerabilities and risks—that is until something happens (911 terrorist attacks on World Trade Center). Despite this fact, system and software developers have recently done a much better job in balancing security with convenience. A layered security philosophy must be incorporated into information technology development in order for computer security countermeasures to be effective. According to an on-line article called Securing Your Wireless Network, "If your wireless LAN is located in a single family home, then you are probably more at risk from intruders coming in via your Internet connection than from folks gaining access to your LAN over the air. But if your LAN has some means of wireless connectivity, you've added another way to access your LAN that doesn't require getting past your router's firewall and doesn't even require physical access!" Defense-in-depth physical security and router/firewall configuration layers will be discussed later on to address physical and Internet connection malicious user access. An example of a malicious computer user accessing your home network over the air is called 'War driving'. According to a Microsoft on-line article called, Wireless Networks for the Home and Small Business, "War driving is the practice of driving around business or residential neighborhoods scanning for wireless network names. Someone driving around the vicinity of your wireless network might be able to see your wireless network name, but whether they will be able to do anything beyond viewing your wireless network name is determined by your use of wireless security." This point must not be overlooked as I mentioned earlier, wireless network infrastructures are more vulnerable at the Internet connection access point than from intruders gaining access to your LAN over the air. 'War driving' is just one security issue affecting wireless networks, but there are many others, as you will see and can explore below.

Below is a summary of security issues that exist with 802.11 (also known as Wi-Fi) extracted from a Microsoft on-line article called, Wireless 802.11 Security with Windows XP. This section is mostly informational. You can gain more detailed explanations and knowledge about these known published 802.11 security issues by visiting the web sites provided in my references. "Institute of Electrical and Electronic Engineers (IEEE) 802.11 is a set of industry standards for shared wireless local area network (WLAN) technologies, the most prevalent of which is IEEE 802.11b" ([1]Microsoft.com 2004). Current standards available are 802.11a, 802.11b, and 802.11g. More standards are in development as we speak. How much data, how fast the data is transmitted, upgraded security features, signal strength, and frequencies used are the differences in current standards. Wired Equivalent Privacy (WEP) encryption and 802.11b and 802.11g are the selected wireless technologies for this project. Since WEP, 802.11b (wireless network adapters) and 802.11g (router/firewall) are the

selected technologies we will focus mainly on them but not until later on in the Router Firewall section of the paper.

Wireless Security Issues

- No per-packet authentication mechanism to identify the packet source.
- 802.11 standards are vulnerable to disassociation attacks—forcing users off of the wireless network.
- No user identification and authentication.
- No central authentication, authorization, and accounting support.
- The RC4 stream cipher is vulnerable to known attacks described above.
- Some implementations derive WEP keys from passwords—also making passwords vulnerable.
- No support for extended authentication; for example: token cards; certificates/smart-cards; one-time passwords; biometrics; and so on.
- There are key management issues; for example, re-keying global keys, and no dynamic, per-station or session key management.

Below is a summary of some countermeasures extracted from an on-line article called, Securing Your Wireless Network, for the existing security issues. Again this section is mostly informational and you can gain more detailed explanations and knowledge how to apply these countermeasures, as they relate to your specific network, at the web sites provided in my references. What security countermeasure used to combat current 802.11 security issues will depend on your equipment capabilities. The countermeasures below ending with the word Deployed in parentheses apply to my network and will be described in the router/firewall section of this paper.

- Don't use TCP/IP for file and printer sharing
- Follow secure file-sharing practices
- Enable WEP encryption (Deployed)
- Use WEP for data and authentication (Deployed)
- Use non-obvious WEP keys and periodically change them (Deployed)
- Secure your wireless router/access point (Deployed)
- Disallow router/AP administration via wireless (Deployed)
- Use MAC address based Access and Association control (Deployed)
- Don't send the ESSID (Deployed)
- Don't accept "ANY" ESSID (Deployed)
- Use VPN

Physical Security (Layer)

On the front line, you can begin by physically protecting access to your computer system. Some computer security professionals might argue that physical security is not the first line of defense because with network connectivity, access can be obtained through system access points quicker and easier than through physical access. This is a valid argument because traditionally, prior to PC networking introduction, mainframe computer systems were stand-alone systems or only used point-to-point connections to pass information. For the purpose of this project I will stick with physical security being the first line of defense. The primary purpose of physical security should always be personnel safety and access control. For a home network physical security should only consist of protecting your computer system just as you would protect any other valuable items (i.e.; credit cards, money, jewelry, firearms etc;). Ensuring that you lock your residence should be all you need to do to physically protect your computers. Physical security requirements in more sensitive environments such as military facilities, government and intelligence agencies, and most financial institutions may require more stringent physical security measures, such as, armed guards, wired gates, physical entry access controls, and entry access badges or even biometrics. Sensitivity of the information to be protected compared to cost should be examined when applying the physical security defense layer. Just as it was mentioned earlier, we need to worry more about malicious users accessing our wireless home network from our Internet connection rather than, "War driving" or physically accessing our network. In order to remain in the scope of this project you only need concern yourself with locking your doors and being aware of your surrounding environment for physical security as a first line of defense.

Security Plan Development (Layer)

If effectively written and enforced, a security plan is definitely a part of any defense-in-depth layered computer security solution. Some computer security professionals might argue that a security plan is not necessary for home networks. I would argue that a security plan is a must for a home network simple because, according to Bowden, "A security plan establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of 'what' to do so that the 'how' can be identified and measured or evaluated". Bowden more simply said, "A security policy is nothing more than a strategy on protecting and maintaining availability to your network and its

resources". I would agree that you should keep the plan simple, brief, and directly related to physically securing your home network. Since you will be dealing mainly with family members living in your home there is no need to elaborate and go into great detail during plan development like you would, say for example a large corporate network. I consider my security plan development and deployment as my second layer of defense. For example, the policy should look something like this:

Security Plan for Dumas Home Network

Password Policy
--All network users must use passwords that include at least 8 alphanumeric characters
--Passwords will be changed every 90 days
--Password crack programs will be ran to check for weak passwords at least monthly
--Weak passwords will be corrected immediately

Administrative Responsibility
--System administrators will ensure all system default passwords are changed immediately
--Be involved with the assignment and maintenance of passwords
--Audit the system for intrusion and malicious activity through event logs
--Run Windows Management patch programs to ensure patches and hot fixes are current
--Scan systems for current patches and hot fixes
--Apply patches and hot fixes as necessary
--Ensure virus software is kept current

User Responsibility
--Know the home security policies
--Report any suspicious system symptoms to administrator

E-Mail Policy
--Don't open e-mails if you are not familiar with the sender
--Delete suspicious e-mails
--Notify system administrator if you have questions about e-mails

Internet Policy
--Parental control firewall methods will be used to block certain sites
--Internet time frames will be assigned to each user (especially children)
--Information will not be downloaded without approval from system administrator

Disaster Recovery

--Ensure system back ups are conducted at least weekly
--More sensitive data should be backed up before you sign off
--Consider lap top back-up systems for continued operation

Intrusion Detection
--Periodic audits will be conducted to ensure the security policy is effective and to assess how many would be Hackers have attempted to penetrate your system.
--Research and countermeasures will be deployed as necessary

Router Firewall Combination (Layer)

The router/firewall combination is my third defense-in-depth solution deployment and in my opinion probably the most important. The main reasons I think this layer is the most important are as follows:

(1) It is a revolving layer and gives the network administrator full control over configuration features. Thus allowing the administrator flexibility to make access from inside the network out to the Internet and vice versa more restricted. The ability to control firewall rules to allow or deny IP and port ranges is an excellent tool for securing the network.

(2) It provides several different security features like Network Address Translation (NAT), WEP, auditing features, and IP filtering to protect the LAN.

As I mentioned earlier depending on the wireless equipment standard you are using (i.e.; 802.11a, 802.11b, 802.11g) will determine what type of security features can be applied. Network configuration and O/S will also determine security features that can be used. Understanding your equipment capability is imperative to ensuring you apply the latest security features available. Again, for the purpose of this project I will stick to my router/firewall configuration deployment. My equipment standards support 802.11b and 80211.g. My computer wireless network adapters support the 802.11b standard and my router supports the 802.11g standard. Just like most computer software 802.11g is downward compatible but 802.11b is not upward compatible. Thus the 802.11g standard provides more security and administrative configuration options than the 802.11b standard may support. A future upgrade to my network from 802.11b network adapters to 802.11g adapters is already planned. For more information on the different wireless security options please visit the websites listed at the end of this paragraph. Let's shift gears and move into router/firewall combination set-up.
http://www.practicallynetworked.com/support/wireless_secure.htm
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoh

o.mspx

(Initial Set-Up)

I utilized the Set-Up Wizard to configure the router and it was fairly simple. In addition to the Set-Up Wizard configuration, I enabled and configured WEP, changed SSID name and disabled the broadcast feature, changed admin default password, and setup the feature to mail logs to my system administrator e-mail account for auditing purposes. I used the most secure method of WEP my system would support. Methods other than WEP for wireless authentication and encryption are available and should be explored. After I describe some router features I will explain the additional configuration features I just mentioned.

(Router)

The router/firewall combination technology is a neat and necessary peace of equipment to incorporate into your home wireless network infrastructure. I purchased the D-Link-624 router/firewall combination from Best Buy. Like the D-Link 624 most routers designed for small businesses and home networks provide somewhat adequate security features. The router portion of the equipment uses something called Network Address Translation (NAT) to masquerade all systems inside the network. In other words, all systems behind the router/firewall are invisible to any would be hackers on the Internet. NAT works by broadcasting one Internet Protocol (IP) address to the Internet. When an inside computer request connection with an outside computer the router records the inside computer's IP address and source port in the address translation table. The router uses a dynamically assigned IP address and a different source port in the outgoing traffic. When a response comes back from the outside computer the router compares the response to the stored information in the address table to determine what inside computer should receive the traffic. If everything checks out then the router allows the traffic through. This technology provides protection against external computers gaining access to your network without a previously established connection from an internal computer first. If outside computers being used by malicious users cannot get through the router without a connection initiated by one of the internal computers, we can safely say another layer of defense-in-depth is successfully deployed.

(Wired Equivalent Privacy)

WEP provides authentication and encryption to the wireless environment.

On-line article, Securing Your Wireless Network states, “802.11b’s WEP encryption has had a lot of bad press lately about its weakness. But a weak lock is better than no lock at all, so enable WEP encryption and use a non-obvious encryption key”. I enabled WEP and used the ‘shared key’ option. This configuration enables my system to both authenticate the client connecting and encrypt its data. I also incorporated a plan to change WEP keys periodically to significantly reduce malicious users from intercepting transmissions and determining the WEP key. This type of attack is possible but very unlikely because it requires interception of a large number of packets. On large busy networks this might only take a short time but on a home network one should consider this as a residual risk and worry more about attacks through the Internet connection. However, if a malicious user determines the WEP key, he or she can begin attacking your network. On-line article Wireless Networks for the Home and Small Business said, “Even if your WEP key is random, it is still subject to determination if a large amount of data encrypted with the same key is collected and analyzed. Therefore, it is highly recommended that you change WEP key to a new random sequence periodically, for example, every three months”. Just as I mentioned earlier there are other methods available that may offer increased security to your home network but may not be practical. For example, “IEEE 802.1x provides much stronger authentication than open system or shared key configurations. This recommended solution utilizes EAP-Transport Level Security (TLS) and digital certificates for authentication. This authentication infrastructure is appropriate for large businesses and enterprise organizations, but is not practical for the home or small business office” ([1]Microsoft.com 2004). Based on identified risk, vulnerability assessment, cost, and practicality, WEP and other replacements for WEP should satisfy most security needs at this level.

(Secure the Router and Use Additional Firewall Features)

Passwords are used to administer and configure the router. Immediately after installation I changed the default password and used a strong password (8 or more alphanumeric characters). I also disallowed remote administration privileges and configured MAC filters to only allow computers inside my network access to the network.

(Audit Log)

Computer system auditing is the process of gathering system activity information through event logs and assessing whether unauthorized activities have taken place or not. Events include but are not limited to, file and folder creation, modification, and deletion and access to local accounts and system services. All or some of these activities can be part of the auditing process. Auditing can be very detailed, require tedious

reviews and complete knowledge of system log output products. I kept my audit process plain and simple. I configured the router/firewall to log system activities, attacks, and notices. My configuration also includes logs being sent to my e-mail account. So whenever I want to review logs I simply ask the router to send them to my e-mail account through a simple click. I then access my e-mail account and review the logs at my leisure to determine and assess malicious activity.

Operating System Maintenance (Layer)

Ever since the development of computer Operating Systems (O/Ss) there has been a valiant effort to produce a product that will require less and less security and administrative Service Packs (SPs) and hot-fixes. This effort has created major points of contention between developing companies and computer security professionals arguing about whose product is the most secure on the market. Microsoft's Windows, Unix, Solaris, and Linux developers put forth a concerted effort and spend millions of dollars toward developing an OS they can say and demonstrate is truly secure and administratively sound. Because of all this, consistently patching and updating your O/S is yet another defense-in-depth layer that will help secure your system and must not be overlooked. I consider consistent OS patching as my fourth layer of defense. Again, Microsoft has developed a neat and easy way to keep your OS up-to-date and secure from most identified exploitable vulnerabilities. By no means is consistent OS patching an inclusive method and malicious computer users can still exploit vulnerabilities. Since my systems have a Windows XP OS baseline, I accomplished this defense-in-depth layer simply by visiting the Microsoft support center web page, reviewing and applying SPs and hot-fixes. My system already had SP1 applied but there was another Update Rollup available with an additional 22 hot-fixes. I also configured my system to automatically scan and update the OS as the patches and hot-fixes are released. Another tool I use on the web page gives the option of scanning my system and providing me with a list of critical updates and recommended but not critical fixes. The program is designed to identify and apply all critical fixes to your system but just in case something gets missed it will also list the critical fixes not already applied to the system. This tool gives me the option to decide what fixes to deploy on the system. Also, since I am employed by a government intelligence agency where computer security is a must, I am kept abreast with the current Information Assurance Vulnerability Alert (IAVA) status as well. This gives me a significant advantage for quickly gaining knowledge about hot-fixes regarding the most recent software and hardware vulnerabilities. Finally, I frequently visit the Microsoft web page to familiarize myself with known vulnerabilities and how malicious users can exploit these vulnerabilities.

Antiviral Software and Definition Updates

Confidentiality, Availability, and Integrity are the cornerstones of computer security. Unauthorized access to your information and impersonation or similar abuse of the system that can be traced back to and blamed on you (compromised confidentiality), denial of service and loss of data attacks (compromised availability), and altered inaccurate information (compromised integrity) are all very likely results obtained through virus infection. Virus infection can happen very easily and there are many methods of deploying viruses into a computer system or network—mainly e-mail and Internet downloads. Before I discuss how I deploy my fifth layer of defense, let me first give you some information on three virus types. First, "Viruses duplicate themselves in the file system through executable files" (networkmagazine.com 2004). Viruses also have the ability to install back doors that provide an open invitation and control of the system by the attacker. Finally, viruses can seize passwords and credit card numbers and basically just do bad things. Second, "Worms differ from viruses in that they spread across networks without piggybacking on an executable host file" (networkmagazine.com 2004). Mainly worms use e-mail attachments and shared files and folders to spread itself on a network. "A third category of malicious logic is the Trojan Horse, which disguises itself either as something useful—a network login window—or as something interesting—an online game or other form of entertainment" (networkmagazine.com 2004). The software, like a virus, can capture passwords to be retrieved later by a malicious user to regain access to a system. "Finally, some viruses and worms can install Trojan Horses on the computers they infect" (networkmagazine.com 2004). Even though all these malicious programs propagate themselves differently, can produce different symptoms on a computer system, and have names and identities of their own, most people refer to all of them as viruses. There is much literature available abroad about how viruses have caused major damage to our military's, corporate America's, small business', and plain everyday people's computer resources. Plainly put viruses wreak havoc and defense against them should not be taken lightly. Now that I have given you some basic information on what viruses are and how they can affect computer systems let's move into anti-virus deployment.

"Anti-virus software that automatically checks for newly discovered threats, periodically scans systems for those threats, and also watches in real time while new files are downloaded from the Internet or detached

from e-mail messages to make sure nothing unsafe gets through is invaluable" (networkmagazine.com 2004). There are many different anti-virus programs you can use to protect your system. I spent 20 years in the United States Air Force and I am currently employed with an intelligence agency called National Geospatial Intelligence Agency (NGA). Over this time period I have mostly seen McAfee and Norton anti-virus software products utilized. I consider consistent anti-virus software deployment as my fifth defense-in-depth layer. The fifth defense layer mechanism I used to protect my home network from viruses was fairly simple to implement. Since my computer already came with a free 90-day trial period from McAfee and my experience tells me that McAfee is a good anti-virus agent, I stuck with McAfee. The anti-virus software always runs in the background and notifies me when new virus definitions are available for download. Virus definitions are a list of recognized viruses contained within the anti-virus program and should be frequently updated. Viruses being introduced into the system will be detected, identified, eradicated and quarantined depending on virus definitions and how the anti-virus program is configured. These virus definition lists are updated as new viruses are identified. Thus the terminology virus definition updates derived. In addition to keeping my anti-virus software updated, I consistently visit the McAfee web site and other related web sites to maintain current knowledge on what viruses are out there and how they affect computer systems. Finally, "Up-to-date anti-virus software will significantly increase protection against known viruses, worms, and Trojan Horses that the anti-virus software developers have identified and neutered" (networkmagazine.com 2004).

Encryption File/Folder Process

If all else fails you can still possibly protect your information by effectively utilizing Windows XP NTFS file system. This is my sixth and final defense-in-depth security layer applied to my home network. One of the reasons I chose O/S Windows XP is because according to a Microsoft article Encrypt Your Data to Keep it Safe, "The NTFS file system available in Windows XP offers several security advantages not available in Windows 95, Windows 98 or Windows Me". Again these new file system security features offered with Windows XP provide yet another security layer to deter the malicious user. The Encrypting File System (EFS) security feature is one of the advantages offered through the NTFS file system. Access controls and permissions is another security feature and will be discussed later. EFS technology gives you the capability to protect your most sensitive information even if someone gains access to your network, steals your laptop or gains access to a disk you copied information to. EFS is multi layered with encryption features for security. When you encrypt files, "Each file has a unique file encryption key, which

must be used to decrypt the file's data. The key is also encrypted and available only to those who are authorized to see the data. Finally, EFS is integrated with the file system making it more difficult to attack, and easier for you to manage" ([4]Microsoft.com 2004). To initially deploy this security feature I created Folders on all systems and named them Platinum and Gold to identify system users' most sensitive information. My Folder naming convention will be revolving and change according to LAN expansion. I then encrypted the folders using the following steps:

To Encrypt a File or Folder

- Open Windows Explorer. (Click Start, point to All Programs, point to Accessories, and then click Windows Explorer.)
- Right-click the file or folder that you want to encrypt, and then click Properties.
- On General tab, click Advanced.
- Select Encrypt contents to secure data check box

After encrypting my folders they were ready for files.

NOTES: Files and folders that are compressed cannot be encrypted. If you choose to encrypt compressed files they will become uncompressed. System files also cannot be encrypted. When you encrypt a single file, you must decide whether to encrypt the folder that contains the file. If you choose to encrypt a folder, all files and subfolders that are added to the folder thereafter will be encrypted. If you encrypt a folder with existing subfolders and files, you must separately choose whether to encrypt existing files and subfolders.

To Decrypt a File or Folder

- Open Windows Explorer.
- Right-click the encrypted file or folder, and then click Properties.
- On the General tab, click Advanced.
- Clear the Encrypt contents to secure data check box.

The other file system management tool offered by Windows XP is access control. This feature also available through NTFS will further increase the security on your computer systems. With file/folder encryption and access controls in place your systems will be equipped with necessary security features to protect your information from the average malicious user. The object of the access control feature is to set permissions to define the type of access allowed or denied to a specific user or group. "For example, you can grant Read and Write permissions to an entire Finance group for the file payroll.dat. When you set up permissions, you specify the level of access for the group and users. For example, you can

let one user only read the contents of a file, let another user read and make changes to the file, and prevent all other users from accessing the file" ([4]Microsoft.com 2004). You can also use and apply some of the same techniques to printers and other peripherals. Since my network is brand new and not so many files/folders exist yet there were minimum permissions to be set. Most of my files exist eternally from my systems and will be slowly incorporated. I will be periodically auditing the network and instructing all users to put important files in the sub-directories I created.

Access controls coupled with encryption gives you a strong defense layer at this level. If a malicious user bypasses all your other defense layers and even bypasses your access control you still have the information encrypted and the malicious user won't be able to modify or see the information.

Conclusion

Let's recap all the information we discussed in this practical project. I covered computer equipment purchase, home network set-up and connectivity description, and each defense-in-depth concept solution as it applied from system acquisition to operation. My defense-in-depth concept solution included knowledge about wireless security concerns and applied countermeasures, physical security, security plan development and implementation, firewall router combination technology deployment and configuration, consistent O/S patching, anti-virus software application, and file/folder encryption methods. This defense-in-depth concept solution project is by no means inclusive. I will continue to build and upgrade the current defense-in-depth concept solution applied as I increase my knowledge about exploitable vulnerabilities and how to apply new and improved security countermeasures.

References

'NUA Internet Surveys'. (September 2002) URL: http://www.nua.ie/surveys/how_many_online/index.html (February 13, 2004).

Vincent Wallace. Personal Firewalls: Not Enough. (February 12, 2001). URL: http://www.itsolvers4u.com/security/Firewalls/personal_firewallsNotEnough.htm (January 27, 2004).

Dr. Frederick B. Cohen. Trends In Computer Virus Research. (1991) URL: http://all.net/books/integ/japan.html (January 27, 2004)

DELL USA Home & Office. Choosing Your Desktop Computer. No Date. URL:http://www1.us.dell.com/content/topics/segtopic.aspx/choosing_desktop?c=us&cs=19&l=en&s=dhs (February 10, 2004)

Practically Networked. Securing Your Wireless Network. No Date. URL: http://www.practicallynetworked.com/support/wireless_secure.htm (February 6, 2004)

Configuring Windows XP IEEE 802.11b Wireless Networks for the Home and Small Business. (November 2003). URL: [1]http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx (February 6, 2004)

White Paper. Wireless 802.11 Security with Windows XP. (August 12, 2003). URL: [2]http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/default.asp (February 2, 2004)

Chris Weber and Gary Bahadur. Wireless Networking Security. (No Date). URL: [3]http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wnsec.mspx

Joel S. Bowden. Security Policy What it is and Why—The Basics. (August 14, 2001) URL: http://www.sans.org/rr/catindex.php?cat_id=50 (February 6, 2004)

Steve Steinke. Coping with Home Network Security Threats. (January 7,

2002)
URL: http://www.networkmagazine.com/article/NMG20020106S0003
(February 6, 2004)

Encrypt Your Data to Keep It Safe. (August 24, 2001)
URL:
[4]http://www.microsoft.com/windowsxp/pro/using/howto/security/encryptdata.asp (March 2, 2004)

Mark Joseph Edwards. Keep Windows XP and SQL Server Secure. (October 22, 2003). URL:
http://www.winnetmag.com/Article/ArticleID/40599/40599.html (January 27, 2004)

Defense in Depth Benefits. (No Date).
URL:
http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html (February 2, 2004)

Home Network Security. (No Date).
URL: http://www.cert.org/tech_tips/home_networks.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event