Global Information Assurance Certification Paper

Securing Personal and Home Communications

Thomas E. Fowler
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1
29 February 2004

Table of Contents

Introduction

This document is focused on providing a process of reviewing the security of personal communications and applying this information to the instruments we use on a daily basis. There is an enormous amount of knowledge related to securing corporate information available. This documentation is directed at using similar processes learned and used within a corporate environment and applying them to our personal lives. Whether the equipment is hardwired or portable, being aware of their inherent security weaknesses will no doubt enlighten our need for safeguarding our personal communications.

Limitations exist in making information 100 percent secure. While these limitations are built-in the technology itself, updating or modifying hardware, equipment configurations, and our social responses to personal information are within our ability to make them more secure. Many sources are free; others can require additional financial expenditures, depending on the level of personal security one wishes to achieve.

Applying security as the strategy to help shield our personal communications will strengthen our ability to guard this information. I will first review some differences between hardwired and wireless computer systems including programs that should be installed to allow these systems to become more secure. Then I will look at our voice communication systems. I will end with reviewing other vulnerabilities such as social engineering and how our responses can enhance security. This paper is designed to guide and enlighten nonprofessionals in securing areas where information is exchanged.

Securing Personal Communications

There are many common issues between communication points, which hardwired and wireless systems share. The commonality will be based on the location of the software or hardware placed on a network and their functionality. The home and each personal mobile device used in communicating information have their own set of individual vulnerabilities.

To accomplish securing information evaluate each device, service, and location on an individual basis. Defining and building a layered perimeter can be as simple as being aware of others within earshot. Below are services and activities that are in common use today. Each of which will be surmised as to their ability to enhance security.

Hardwired Systems

Hardwired systems are classified as having private physical connectivity by keeping the communication traffic within the confines of the cabling and associated hardware. This type of systems is also called a Local Area Network (LAN). There are several ways to connect hardware together. The most common is called Ethernet and is defined and described in the Institute of Electrical and Electronics Engineers 802.3-2002 standard

IEEE[1]. Figure 1 below shows how a typical system could be configured
All connections are physically joined together with the exception of the connection to the Internet cloud. The only way to access this network would be from the internet cloud or

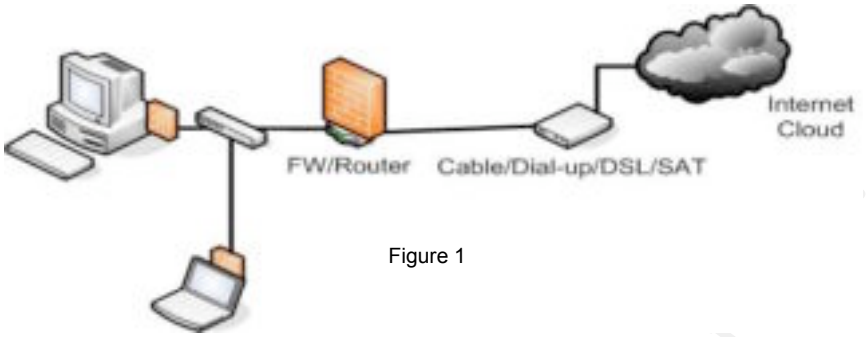

Figure 1

physically being at this location. There are several ways to secure this hardwired system. The implementation of firewalls, antivirus, and others, as they make a system more secure, are essential, easy to implement, and will be covered later in this paper. For a more detailed and in-depth application to securing a home PC review the following papers from the SANS Reading Room – Home & Small Office[2]; Shauna Munson's Defense in Depth and the Home User[3] and Thomas Harbour's Defence in Depth on the Home Front[4]. Next, I will review a wireless system. This type of system is more vulnerable and needs more care when security is implemented.

Wireless Systems

Wireless Local Area Network (WLAN) is a technology used to connect hardwired computers and mobile devices together. Wired networks send traffic over a dedicated line that is physically private while wireless devices broadcast their traffic over shared airwaves. This broadcasted traffic, from and Wireless Access Point (WAP), and the additional interference from other wireless devices sharing the frequency range of 2.4 GHz and 5.8 GHz, such as cordless phones, wireless laptops, and cameras, add to the need for security.

Being aware of ones own surroundings becomes important in assuring that proper steps can be taken in securing information and property. As we become mobile and use wireless equipment for personal and business use we need to be aware of the vulnerabilities while traveling. Traveling and using mobile equipment to log and communicate information is at high risk from theft and eavesdropping and extra care should be taken when using portable equipment. Visit the SANS InfoSec Reading Room – Travel Security[5] section for more detailed articles. Focus on Thomas Palmer's Basic Travel Security Revisited[6] paper where he tackles the steps and processes one should follow to ensure the security of using mobile devices, like laptops, while traveling.

Wireless systems are a prime target for uninvited guests and are installed similar to figure 2.

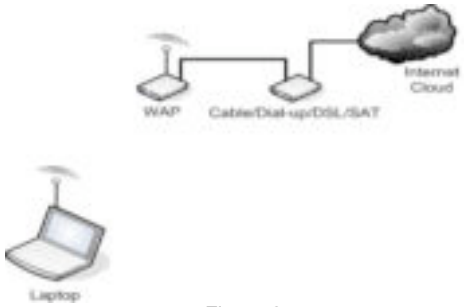

Figure 2

Wireless LANs allow for more mobility and flexibility by allowing users to stay connected and communicate to the network. Users can roam from one room or location to another without the need to plug a cable into a jack in the wall. While this provides enormous flexibility there can be potential vulnerabilities. Think of a neighboring teenager getting access to your internet connection downloading illegal music at your expense while he or she remains anonymous and your network is identified as the offending party. Unauthorized access via a wireless access point can be achieved easily if proper measures are not taken to protect oneself from this activity.

The IEEE houses several standards and specifications for deploying wireless local area networks. The 802.11 Wireless[7] standard specifications use a few techniques for achieving some protection in wireless networks that are defined below.

- The Service Set Identifier (SSID) is a common key that identifies a specific wireless network. Users must be configured with the correct service set identifier in order to access their respective wireless local area network. This confidential key should be shared only with those having legitimate need to access the network. In order to secure the service set identifier the broadcasting of the service set identifier should be disabled in the configuration of the device and the service set identifier should be changed periodically.
- The Media Access Control (MAC) setting is used to filter out non-specified device addresses and to restrict access to computers that are on a specific list you authenticated and created. If you do not add a device to the list access is not granted.
- The Wired Equivalent Privacy (WEP) in an encryption algorithm that protects data streams between the end-user devices and the WAP.

For a more in-depth knowledge of this standard review SANS InfoSec Reading Room-Wireless Access and read Stanley Wong's The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards[8].

Placing the wireless network on an Un-Trusted segment, as seen in figure 3 below, is recommended because if an intruder were to compromise your wireless access point they would be unable to reach your Trusted Network.

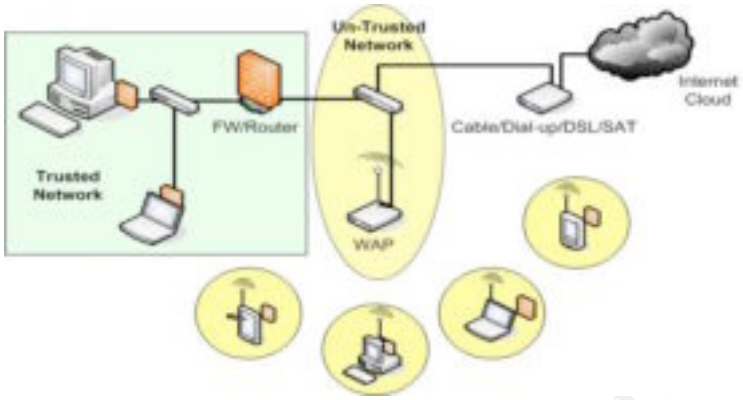

Figure 3

There are other settings and configurations available each dependant on the product vendor. Along with looking at changes to configurations, being aware of how someone is able to find out about your network is also important. Next, we will look at a process called Wardriving[9] to gain just such information.

Tactics such as Wardriving can reveal your network to others. Wardriving or Warwalking is a process in which an individual uses a wireless device such as a laptop or Personal Digital Assistant (PDA) while driving or walking around with these devices. This equipment is usually set in passive or promiscuous mode looking for any wireless network nearby, hopefully unsecured. Wardriving or Warwalking requires no elaborate software or hardware to achieve gaining information. Using a global positioning satellite receiver in combination with the wireless device and some software, anyone is able to map a major metropolitan area or neighborhood (figure 4) while documenting and mapping wireless networks both secured and unsecured.

Figure 4

In order to discourage and protect your wireless system disable the broadcasting of the network and change the SSID regularly. Doing so will discourage intruders and hopefully direct them to someone else's network. For more detailed information on securing wireless systems review articles on the Internet or in the SANS InfoSec Reading Room - Wireless Access[10]. Once a network has been found it is only a matter of time before the systems is documented and displayed for all to see. This process is called Warchalking[11].

Warchalking is a method of marking a series of symbols on sidewalks, walls, curbs, or anywhere visible, to the public, to indicate nearby wireless access points. If your wireless network is Warchalked, and you do not realize it, your network is at risk. The information about how to access your network is now visible for all to see. Below, in figure 6, is a sample of how networks could be documented and an example of what the symbols look like;

This symbol (figure 5) identifies the node is open and shows the SSID and the bandwidth shown.

Figure 5

Figure 6

This symbol (figure 7) identifies a closed node with the SSID displayed.

Figure 7

This symbol (figure 8) identifies the network as a WEP node with the SSID, access contact, and bandwidth exposed.

Figure 8

Conducting a proper site survey is essential when setting up a wireless network. For instance, placing the access point close to an outside wall would extend the broadcast range further outside your home perimeter allowing a greater risk in unauthorized access onto your network. Both hardwire and wireless systems use services such as e-mail and the World Wide Web (WWW). The following information will highlight some security issues for e-mail and Web services.

E-mail

E-mail is now used and widely available almost instantly. There are several methods used to access e-mail such as by home computer, wireless devices like cellular phones, PDA's, and text pagers. E-mail is usually sent in the clear, which can be sniffed by hackers and read by administrators at internet service provider sites. Encrypting the messages ensure data confidentiality and using digital signatures will provide non-repudiation of content and integrity in your correspondences.

Another way to enhance e-mail security is by not responding to any messages that require you to provide private information. The thawte[12] Web site will provide you with a personal e-mail certificate that will allow you to provide a digital signature and encryption to personal e-mails, best of all this service free. Since e-mail is so popular a new threat and source of aggravations is on the rise. This threat is known as spam.

Spam

Spam is unsolicited and or unwanted e-mail. Besides flooding the in-box with unwanted advertisements spam can also be used to collect personal and private information. E-mails can also be engineered to solicit phony requests for you to yield this information. Treat this as spam and a potential risk, do not reply.

If you are sent an e-mail from some service or source that you do not know or cannot validate and the message contains a link that instructs you to "click here to unsubscribe" do not do so. These messages are often sinister redirects to sites with Trojans, viruses, worms, pornography, and or tools for the spammers to verify that your address is valid. Unsubscribing will not remove you from the list.

If possible, on your e-mail system, create a blacklist or block this sender in your mail filters from further solicitation. The WWW is vast, ungoverned and sometimes unforgiving. Being able to secure communications that contain private information is important and should be viewed as essential when transmitting personal information or transactions online.

Web

Accessing the Web to purchase products or services is common practice today. Purchasing items or services from the Web can be unsecured. Be sure never to put credit card information or other personal information, such as user identification or passwords, in a site that does not first direct you to a secure socket connection. This would look like figure 9 and figure 10, a closed lock indicating the page is secured.

Figure 9

Explorer and other applications like Yahoo![13] (figure 10) often request you to remember your passwords on the screen or site. Never select the option to remember the password or user ID.

Figure 10

Some web sites will upload cookies to track your browsing activities.
A cookie is a unique identifier that a web server places on your computer which attaches a tracking identification number that can be used to retrieve your personal records from their databases. Others will alter settings in your computer or install software commonly referred to as ad-ware or spy-ware and can be used for a number of annoying, menacing, or vicious reasons. Use programs such as Ad-aware 6[14], a purchased software utility, or Spybot Search & Destroy[15], a free software utility, to

remove ad-ware and spy-ware to combat this issue. The idea here is that there are an abundant amount of tools available that can be used to help secure information.

Tools

There are vast services available that will allow remote scanning of a system for vulnerabilities to intrusion and exploits. Tools are very useful in determining that security configurations are setup properly and are typically defined as Host-Based or Network-Based. One such product is called ShieldsUp![16].

ShieldsUp! provide a free service that will allow you to scan for file sharing and open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports.

> It is likely that no one has told you that your own personal computer may now be functioning as an Internet Server with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet! (Gibson)[17].

TCP/UDP ports are used for a variety of services, such as http://standards.ieee.org/getieee802/802.11.html Web pages use port 80 and e-mail uses port 25, in order to communicate on. Services are assigned ports ranging from 0 to 65535. Having file sharing and open ports for services that are not used or needed is a huge security risk as malicious users will use and exploit them.

Using tools regularly will assist in identifying your systems security weaknesses. Tools provide guidance on what enhancements could be made to help limit ones exposure. Many such tools or services also provide step-by-step tutorials to assist with modifying and implementing configurations to close exploits and vulnerabilities. Antivirus software is one such tool.

Antivirus

The use of an antivirus program is essential. It protects email, instant messages, and other files by automatically removing viruses, worms, and Trojan horses.

- A virus is a program, which has the ability to replicate, i.e. copy itself to other computers or disks without being asked to do so by the user, and it requires that its host program be activated to make the virus effective. A virus does not have to do any damage to be called a virus it simply just has to attempt to copy itself.

- A worm is a computer program that replicates itself and is self-propagating. Worms as opposed to viruses can run independently and are meant to multiply in network environments.

- A Trojan horse is a computer program that has a useful function, but which also contains additional hidden sometimes-malicious functions. These hidden

functions may secretly exploit the system's security by making a blind copy of a sensitive file for the creator of the Trojan horse to view. They are often designed to install a tool that may then be used to circumvent the system's security for direct access.

Antivirus products are continually enhanced with features such as detecting certain non-virus threats as spy-ware and keystroke loggers. Antivirus programs should be on all equipment processing information. The greatest vulnerability is not having an antivirus program in place and not keeping up to date with patch releases. Several products are free for home use. Selecting a vendor that has a good reputation and constantly updates their definitions would be a wise decision. Firewalls are also an important service to implement. They are usually placed and defined as the initial wall of defense for securing resources.

Firewall

If you have a high-speed cable, DSL, or satellite connection, and you are not using a firewall, your computer is wide open to anyone on that network. Firewalls are critical in reducing the risk of vulnerability. Theses products come in many forms and range from hardware to software. A firewall is a system that enforces access between two networks. The firewall can be thought of as one set of rules created to block traffic and another set of rules to permit traffic. The most important thing to understand about a firewall is that it is designed to control access in and out of the network.

Theoretically, there are two types of firewalls, Network-Based and Application or Host-Based. Network layer firewalls have become increasingly more sophisticated and easier to use. This type of firewall typically resides at a point in the network where all communication traffic is routed and is commonly on a stand alone hardware device with its own proprietary software. Application or Host-Based firewalls are usually software based and reside on the device it is protecting.

Adding firewalls between network segments and to individual network devices will help secure intrusion into the network. Examples of software firewalls are Zonealarm[18], BlackICE[19], McAfee Firewall[20], and Norton Internet Security[21]. Common examples of hardware-based firewalls are Siemans[22], Linksys[23], and Netgear[24] systems geared for home or small office environments. Most, if not all, can be purchased at the local retail store such as BestBuy[25] and CompUSA[26] or at an online retailer.

A common error made by many is that if they are using a firewall they are automatically secure. This is not necessarily true because all security holes, big and small, can be exploited. Be aware that if devices and technologies like firewalls or routers are configured incorrectly, the network can be compromised. Placing firewalls in multiple locations and within multiple devices on the network will augment the ability to secure them. The more layers defined the stronger your security perimeter. As you can see in figure 11 below the hardware firewall/router is placed in front of the connection to the

internet. This is the first and most important wall of defense for the network, and can be defined as a Trusted Network. Adding software firewalls on each device respectively will create an additional layer of protection to your information. Each layer would protect different aspects of intrusion.

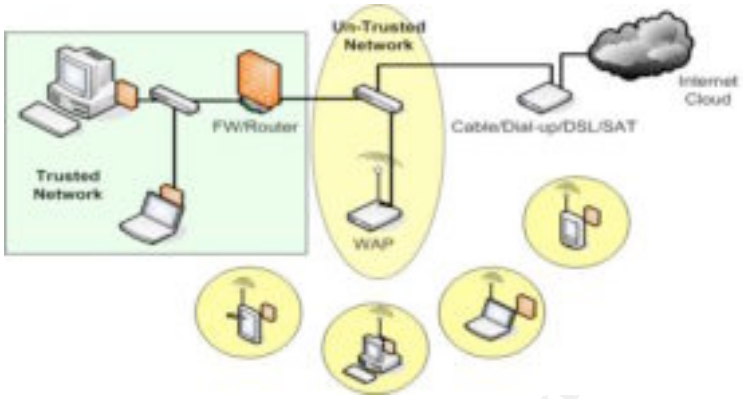

Figure 11

Any device added to an Un-Trusted network segment is more vulnerable, as the layers of protection are reduced, increasing the risk of exploitation. Hardware based firewalls can easily be configured incorrectly leaving an opening for attack, on the other hand, if properly configured are prone to offer the highest level of security. For a greater depth of understanding in the use and benefits of firewalls see the SANS InfoSec Reading Room – Firewalls & Perimeter Protection[27].

Telephone Systems

Besides the vulnerabilities in the use of computer equipment, there are several risks in using telephone services. Telephones are used everyday. They communicate information in a variety of ways such as cellular phones, cordless phones, Plain Old Telephone Service (POTS) and voice mail. The ability to understand the risks encountered when utilizing these types of services will facilitate steps to help increase the level of security applied to them.

Voice-mail

Voice-mail and or answering machines are used everyday to leave sensitive information by phone. Criminals and deviants access these systems either to gain this information for future exploits or just to embarrass people by leaving insulting messages for the callers to hear. Some simple steps when setting up a system will enhance its limited security. Never allow the voice-mail or answering machine password to be the phone number in itself. Check the system on a regular basis to be sure that no one has inserted unauthorized voice-mail boxes and or modified your personal greetings.

Passwords should be no less than the maximum available character length allowed. By selecting a unique security code, and changing it regularly, preferably every 90 days will greatly secure its contents. Do not assume that a voice-mail provider is supplying

general security and protecting your voice-mail, so do not leave sensitive information on them.

Cordless Phone

When using a cordless telephone there is one important thing, security. A cordless phone is a radio transmitter, it broadcasts signals over the open airways. Therefore, it is possible for other people to listen to or eavesdrop on your phone conversation by using a radio scanner. Did you know that even a baby monitor could pick up conversations? As you can see in figure 12 below the conversations can be monitored without your knowledge.

Figure 12

Digital phones are superior to analog phones and digital spread spectrum (DSS) offers the best protection against eavesdropping. Low-end 43-50 MHz and 900 MHz analog phones are not secure and most baby monitors or scanners can pick up phone conversations within this frequency range. The 2.4 GHz and 5.8 GHz digital phones offer encrypted channels between the base station and handset that offer some degree of protection because most commercially available radio scanners do not extend into this radio frequency range. If the cordless phone does not have DSS, then the conversation is subject to eavesdropping and care should be given when divulging private information.

Cellular Phone

Cellular communications will soon surpass its wired counterpart the Plain Old Telephone Service. The POTS system is more secure in communication as the chances of someone tapping into the physical wiring (figure 13) to gain access to a conversation is difficult, although possible. Cellular sends information in the open air to communicate (figure 14). As we continually use cellular products, our vulnerability to security risks will continue to grow.

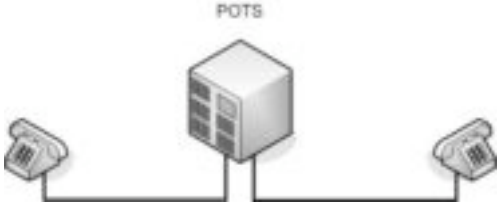

Figure 13

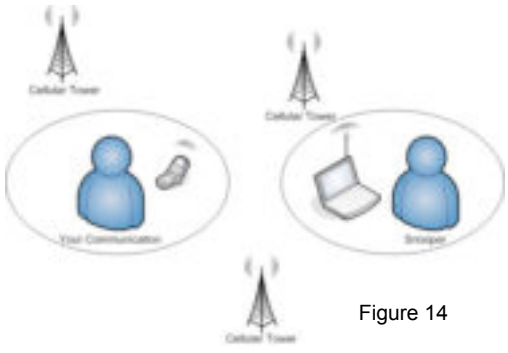

Figure 14

Modern cellular phones now come with a few security features that could be implemented with little effort, though require a slight change in habit. Use features such as Lock Key Pad, Security Code, and Phone Lock each of which provides a different layer of protection and are described below.

- The lock keypad feature temporarily locks down the keypad from functioning and is the least secure of the three.
- The next level of security would be to use the security code feature. This feature locks down the certain features and commands from being modified.
- The phone lock feature, being the most secure, would protect the phone from unauthorized outgoing calls or access to private information stored within such as notes or account information.

All these features may seem cumbersome initially, but when implemented will secure the device from unauthorized use if lost or stolen. Remember when engaged in conversations or data entry on a cellular network be conscious of others nearby, they may be listening or watching. Our personal responses to questions asked by unknown individuals leads me into our next section on other types of vulnerabilities. Social Engineering and Dumpster Diving are methods used in order to gain access to personal, private, and privileged information.

Social Engineering

While technology, configuration, and awareness are critical to ensuring a secure environment, this does not mean that an individual is not vulnerable. Attackers often exploit people as the weakest link in the security chain and use social engineering techniques to gain information needed. One such method is to exploit the accommodating nature of people to gain access to sensitive information for use in fraud, network intrusion, and identify theft.

Although Social Engineering can be difficult to detect some basic precautions should be taken when engaging in conversations with unknown individuals.

- Do not divulge or reset passwords, usernames, and pin numbers to anyone.
- Do not allow the modification to accounts or services unless requested by yourself and you have authenticated the party changing the information.
- Do not write down passwords or sensitive information because they can be copied or removed without your knowledge.
- If you are planning to be on an extended trip or away, do not set up automatic email notifications, voice mails, or answering machines indicating so.

There is a plethora of information available on ways to deal with this topic, but for more detailed information on Social Engineering go to the SANS InfoSec Reading Room - Social Engineering[28] section. Read Radha Gulati's The Threat of Social Engineering and Your Defense Against It[29] were he classifies social engineering into two main types, computer or technology-based deception and human-based deception.

Dumpster Diving

Along with being aware of our social responses to outsiders we also need to be aware or our physical environment. Dumpster diving is one of the most overlooked areas of security. Information is harvested by means of rummaging through garbage in order to procure the valued data. The main threat here is unauthorized access to sensitive information such as medical statements, resumes, utility bills, bank statements, and credit card statements. Stealing trash is very common and recognized as a successful method of reconnaissance for the unprincipled in gaining information.

The best deterrent for this situation is to buy a shredder. Shredding all waste paper is a major step in protecting information. Purchase a shredder with crosscut capability as this is more secure than ones that do not have this function. If you recycle, be sure to destroy any sensitive materials before recycling since you cannot rely on recycling vendors to do this for you. Information is valuable, once taken it can be used to steal your identity. Identity theft is on the rise and securing our environment is important.

Identity Theft

Currently this is the largest and most threatening aspect of individual security. Identity theft occurs when information is stolen via mailboxes, the trash, or hacked by savvy individuals. Once your information is harvested, it will be used. This action is called identity theft and is the intentional use or theft of a person's private information in order to obtain goods or services. Having ones identity stolen and then used to pillage bank accounts and purchase unauthorized merchandise or services is devastating.

If you have determined that you have become a victim of identity theft, there are a few steps to take as outlined by the Federal Trade Commission ID Theft[30];

- Contact credit-reporting bureaus such as Equifax[31], experian[32], and TransUnion[33] to report the theft.
- Close any accounts that have been compromised or opened illegally.
- File a police report.
- Contact the Federal Trade Commission and file a complaint.

Conclusion

Constant vigilance is needed in order to secure information. Conducting regular audits of important systems and changing passwords on a regular basis is a necessity. This includes the default passwords on all equipment and applications. Encrypting information wherever possible on sensitive data can prevent hackers from reading this information. Keeping all firmware, software, and hardware updated will help patch existing security vulnerabilities found by their manufacturer.

Turning off file sharing on a system is an important step to securing it from vulnerabilities outside of the trusted network. Setting up an un-trusted zone enables you to place a wireless network on a separate segment reducing the risk of an uninvited visitor gaining access to the trusted network. Remember that by looking at the way you use personal communication and build a layered defense philosophy around each individual device and situation you will create a more secure environment. Doing so can reduce the likelihood of intrusion. The ability to effectively survey areas and administer tools used in gauging vulnerabilities has a direct impact on securing the information transmitted.

Some of this material may seem a bit overwhelming. If you are unsure of how to accomplish some of these tasks, there are professional services available. Accessing the SANS Reading Room[34] and traversing the internet for more information would also be a prudent step. This paper was written to inform and point out the many areas of vulnerability in our daily communications. Being aware of the risks and taking action to limit the exposures to them will increase your ability in securing personal and home communications.

Reference List

[1] IEEE. “802.3-2002 Standard.” Institute of Electrical and Electronics Engineers Inc. Jan. 2004. URL: http://standards.ieee.org/getieee802/802.3.html (28 Feb. 2004).

[2] SANS. “SANS InfoSec Reading Room – Home & Small Office”. Welcome to SANS' Information Security Reading Room. 2004. URL: http://www.sans.org/rr/catindex.php?cat_id=26 (14 Dec. 2003).

[3] Munson, Shauna. “Defense in Depth and the Home User: Securing the Home PC.” 7 Mar. 2003. URL: http://www.sans.org/rr/papers/index.php?id=894 (5 Jan. 2004).

[4] Harbour, Thomas. “Defence in Depth on the Home Front.” 12 May 2003. URL: http://www.sans.org/rr/papers/index.php?id=1033 (5 Jan. 2004).

[5] SANS. “SANS InfoSec Reading Room – Travel Security.” Welcome to SANS' Information Security Reading Room. 2004. URL: http://www.sans.org/rr/catindex.php?cat_id=62 (22 Dec. 2004).

[6] Palmer, Thomas. “Basic Travel Security Revisited.” 6 Aug. 2001. URL: http://www.sans.org/rr/papers/index.php?id=410 (15 Jan. 2004).

[7] Wireless. “IEEE 802.11 Wireless.” 17 Jan. 2004. URL: http://standards.ieee.org/getieee802/802.11.html (29 Feb. 2004).

[8] Wong, Stanley. “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards.” 11 July 2003. URL: http://www.sans.org/rr/papers/index.php?id=1109 (3 Jan. 2004).

[9] Wardriving. “Wardriving.” WirelessCon and Need Guide. 2004. URL: http://www.wardriving.info/live/ (7 Jan 2004).

[10] SANS. “SANS InfoSec Reading Room – Wireless Access.” Welcome to SANS' Information Security Reading Room. 2004. URL: http://www.sans.org/rr/catindex.php?cat_id=68 (7 Jan. 2004).

[11] Scwartz, Aaron. “Warchalking.” 2004. URL: http://www.warchalking.org/ (7 Jan 2004).

[12] thawte. 2004. URL: http://www.thawte.com/ (15 Jan 2004).

[13] Yahoo. 2004. URL: http://mail.yahoo.com/?.intl=us (2 Feb. 2004).

[14] Ad-aware 6. 2003. URL: http://www.lavasoftusa.com/ (3 Feb. 2004).

[15] Kolla, Patrick M. “Spybot Search & Destroy.” Feb. 2004. URL: http://www.safer-networking.org/index.php?page=home (3 Feb. 2004).

[16] ShieldUp!. "ShieldUp!." Gibson Research Corporations. Feb 2004. URL: http://www.grc.com/default.htm (10 Feb. 2004).

[17] Gibson, Steve. "Hidden Internet Server." Port Authority Edition – Internet Vulnerability Profiling. 2003. URL: http://grc.com/x/ne.dll?rh1dkyd2 (26 Feb 2004)

[18] Zonealarm. 2004. URL: http://download.zonelabs.com/bin/promotions/zap4/11023.html (15 Jan. 2004).

[19] BlackICE. 2004 URL: http://blackice.iss.net/ (15 Jan. 2004).

[20] McAfee Firewall. 2003 URL: http://us.mcafee.com/ (15 Jan. 2004).

[21] Norton Internet Security. "Norton Internet Security." Symantec Corporation. 2004 URL: http://www.symantec.com/sabu/nis/nis_pe/ (16 Jan. 2004).

[22] Siemens. "Siemens." Siemens Subscriber Network. 2004. URL: http://www.efficient.com/subscriber_networks/homenetworking.shtml (2 Feb. 2004).

[23] Linksys. 2003. URL: http://www.linksys.com/ (16 Feb. 2004).

[24] Netgear. 2004 URL: http://www.netgear.com/ (16 Feb. 2004).

[25] BestBuy. 2003. URL: http://www.bestbuy.com/site/index.jsp?KAC-U9844R234552&ref=02&loc=01 (16 Feb. 2004).

[26] CompUSA. 2004. URL: http://www.compusa.com/ (16 Feb. 2004).

[27] SANS. "SANS InfoSec Reading Room – Firewalls & Perimeter Protection." Welcome to SANS' Information Security Reading Room. 2004. URL: http://www.sans.org/rr/catindex.php?cat_id=21 (28 Dec. 2003).

[28] SANS. "SANS InfoSec Reading Room – Social Engineering." Welcome to SANS' Information Security Reading Room. 2004. URL: http://www.sans.org/rr/catindex.php?cat_id=51 (12 Dec. 2003).

[29] Gulati, Radha. "The Threat of Social Engineering and Your Defense Against It." 31 Oct. 2003 URL: http://www.sans.org/rr/papers/index.php?id=1232 (20 Jan. 2004)

[30] ID Theft. "Welcome to the Federal Trade Commission: Your National Resource for Identity Theft." Federal Trade Commission. 2004. URL: http://www.consumer.gov/idtheft/ (07 Feb. 2004).

[31] Equifax. "Equifax Personal Solutions." 2004. URL: https://www.econsumer.equifax.com/ (20 Feb. 2004).

[32] experian. 2004. URL: http://www.experian.com/ (20 Feb. 2004).

[33] TransUnion. 2004. URL: http://www.tuc.com/ (20 Feb. 2004).

[34] SANS Reading Room. "Welcome to SANS' Information Security Reading Room." 2004. URL: http://www.sans.org/rr/ (25 Feb. 2004).