GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Name: ***Perry P. Jurancich***
Certification: GIAC Security Essentials (GSEC)
Assignment: Version 1.4

Setting up a Secure Home Office Network

Introduction

The federal government's draft of the National Strategy to Secure Cyberspace[1] released in September, 2002 states "while large companies employ experts and spend millions to protect data, less-sophisticated home users with broadband connections may be unwittingly providing hackers easy access to public and private networks." Even the home user and small business can be damaged severely and, in some cases, be used to damage others." Most corporate employees fit into the "home user" category and do not have the expertise to adequately secure their computers and the data they contain. Corporations are now waking up to the fact that a comprehensive approach to securing those "home" resources is required.

With the proliferation of multiple computer households, the impact of a home office network on the corporate networking environment is significant. The question is how do corporations deal with and manage this new resource as extensions of the corporate network? Adapting the corporate computer security and usage policy to a home office environment is the most effective means to mitigating the vulnerabilities. I will address the makeup of a common home office network. With the policy in mind, the following topics will be covered:

- Why home networks must be considered extensions of the corporate environment.
- Melding home networks into the corporate computer networking and security policy.
- Providing fundamental concepts of home network vulnerabilities and security, including wireless local area networks (WLAN).
- Mitigating vulnerabilities using host and network based firewalls, virus scanners, host based intrusion detection (IDS), as well as a sound patching policy.
- Securing the communication to the corporate network using IPSec VPN connections, including a "compare and contrast" of IP IPSec solution versus PPTP/L2TP.

At the conclusion of this document, it will become evident that aligning the structure of a home office network to corporate policy is a smart business decision. This paper will act as a framework to attain a secure home office network that will ultimately be a resource to a corporation and not a liability.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Home Office Environment

A home network is essentially the same as a business network except for the size and scope of the resources. For the purpose of this article, we will consider a home network to have three computers, one connection to the Internet and a single printer/scanner to share.

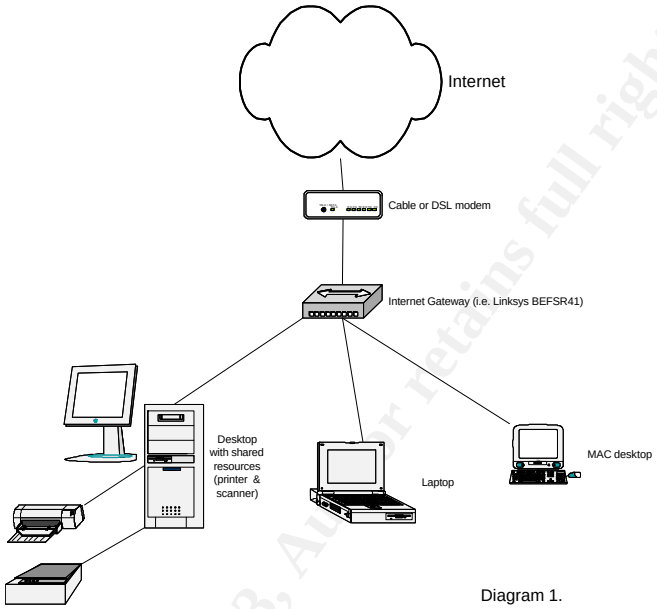


Diagram 1.

In this setup, a cable modem is connected to an Internet-connection sharing device. The industry uses several different terms for this device's functionality. Some examples are Internet routers, SOHO firewalls, home gateway switches, cable/DSL routers (Linksys), broadband routers (D-Link), or a combination of several of these descriptions – cable/DSL broadband router (D-Link), and many more. Each has the same basic functionality; acting as a Network Address Translation (NAT) device with the ability to hand out private IP addresses to the network client machines. Additional information on NAT will be addressed later in this document. For the purpose of this article, the term "router" will be used for the device between the cable or DSL modem and the computers on the home network.

© SANS Institute 2003, Author retains full rights.

Home Networks as Corporate "Resources"

Market research shows that current PC owners are buying most of the new computers. According to International Data Corp. (http://www.idcresearch.com) by the end of 2000, about half of all U.S. households had a computer, and more than 20 million of those had more than one computer. The International Engineering Consortium (http://www.iec.org/) defines a home network[2] as: "The collection of elements that process, manage, transport, and store information, enabling the connection and integration of multiple computing, control, monitoring, and communication devices in the home." In non-technical terms, a home network is two or more computers in a residence that share resources between each other as well as an Internet connection.

The result is a growing population of corporate employees working from a home office, at least part time. Since work is being done outside of a corporate office, where work is done becomes a concern for the corporation and by default, becomes a corporate resource. Therefore home office therefore needs to be treated as a "resource" due to the fact business is being conducted there.

Prior to the advent of high-speed (AKA-broadband) Internet connections, the risk to the corporate network was significantly lower with dial up solutions. Corporations typically had their own modem banks that connected directly to the company network, not going across the Internet, and were controlled by the IT department. With the proliferation of high-speed always-on connections to the Internet, it is typical for a home office to be connected to the Internet via a router and a cable or DSL modem. The comment in the opening paragraph "home users with broadband connections may be unwittingly providing hackers easy access to public and private networks" succinctly defines what corporations are up against. The "private networks" being referred to here are the corporate networks that hackers want to access.

Corporations are forced into dealing with remote office networks, but how to do so can be very complex, time consuming, and ultimately expensive. However, the effort and cost of supporting home networks pales by comparison against an intrusion with a potential loss of untold tens of thousands, and quite possibly millions of dollars in intellectual property and man hours. As a result, more Corporations have realized they need to extend protection to their home office users in the same way they protect regular corporate networking environments. Next, let's take a look at how a policy can support us in that effort.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Corporate Home Office Computer Security and Usage Policy

Computer and Security Usage Policies are created to establish ground rules and identify resources, which are permitted and disallowed. They cover a wide range of topics ranging from how someone is identified (their user ID) to how they will log onto a computer and into a domain (their authentication), to email use and misuse. A good rule of thumb is if someone has to ask "can I do this on my computer?" then there should be a statement in the policy addressing the issue. Also, the policy is a "living" document and reviewed often. The computing environment changes so rapidly, 6 months without an update can make the best policy severely outdated.

The following is an example of a subsection of a general computer security and usage policy for the ABC Company relating to Home Office Computers[3]:

> **4.20.2 Home Office Computers:** All policies applying to ABC-owned equipment apply to home office computers used to access ABC networks (and ABC confidential, proprietary, or sensitive information). Since many home office computers also contain programs and personal data not related to business, additional protection practices might be necessary. Routinely, connections to ABC networks should only be enabled during the period of work, and should definitely be disconnected when non-ABC employees are using the home computer. Home wireless networks (WLAN) shall be disconnected from any computer when that computer is used to connect to ABC networks. Connections to ABC networks shall not be used as a general use Internet service provider (ISP) for non-business functions. The same protection against viruses, executable e-mail attachments, and appropriate access to the Internet, among other practices, are necessary for home systems on which the ABC network is accessed or business is conducted. The use of any programs that would be prohibited on the office network is also prohibited from being present on a computer that is used to connect to the ABC corporate network.

While this section of the policy does not address issues some people might ask about, other areas of the policy would cover them. Keep in mind that any reference made to the ABC systems, the restriction also applies to personally owned equipment when it is used to connect to the ABC network. In example:

> **4.10.2 Freeware Software Usage**
> Free programs that appear to enhance your system or add features such as graphics should not be downloaded or installed on ABC desktops or laptops. These programs may have hidden "features" that may cause serious damage to the system, or worse, to the entire ABC infrastructure. ABC computers should be loaded only with business-related software approved by the Company and/or local system administrator.
>
> **4.10.3 Virus Protection and Disruptive Software**
>
> ABC policy prohibits introducing into a computer system any software or hardware intended to disrupt normal operations. This includes programs known to carry a destructive or nondestructive "virus," "worm," "logic bomb," or "Trojan Horse." In addition to violating ABC ethical standards, such actions may be illegal.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Numerous freeware peer-to-peer file sharing software programs such as Gnutella, Morpheus, Bearshare, or KaZaA have been developed to facilitate file sharing over the Internet. The use of these types of programs is not acceptable for use on ABC computers or computers used to connect to the ABC network. Only Collaboration software approved by the Director of IT Security may be used at ABC. Downloading software from the Internet can introduce security risks such as viruses, Trojan Horses, or "backdoors." In addition, these programs cause extra unneeded network traffic and may contain "adaware" or "spyware" that can violate confidentiality or track the habits of the user. Using such peer-to-peer programs to share programs, music, movies, etc., may result in a violation of software licensing or copyright infringement, which could expose ABC to litigation.

Home Network Security and Vulnerability Concepts

The possibility of valuable information being compromised or lost is an increasing threat to corporations. This threat can be from within a company or from outside, and may be intentional or inadvertent. To prevent these losses, every member of a company who is involved in using computers, or handling computer-generated information shares responsibility for protecting that information. A company depends on its employees to act responsibly and ethically. Ultimately, practicing good security is the duty of every employee.

The philosophy when approaching how to deal with home networks needs to be one of adapting the home network to comply with the corporate policy and not one where the policy conforms to the user. In a home office environment, at least one computer needs to be isolated for work related activities and one or more for family use. Typical family uses are file sharing programs and playing games. Since these activities are considered a high threat to virus transmission and present opportunities for hackers to gain access to systems, NEVER play games or share files with the computer used for work.

General Security Concepts

When considering home office networks and their potential impact to the corporate network, the concept has to be one where we apply the corporate policies to “less-sophisticated home users.” While some processes may be routine and fully understood by many in the IT world, most home users will have no idea what it means to “secure their home network.” The concept must also consider how to present the policy in such a way as anyone can understand it without any ambiguity. Just as a chain is only as good as its weakest link, a policy is only as good as its implementation. A strong security policy for home networks is mandatory.

There are some basic security concepts to consider regarding home network vulnerabilities and how to combat them. The primary concept to keep in mind is Defense-in-Depth. Defense-in-Depth is the layering of defensive measures to provide the maximum amount of protection to a given situation. Applying Defense-in-Depth to a home network would mean the following:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Using a router to provide firewall type protection from the Internet
- Configuring the router to turn off all unnecessary services
- Configuring the PC using the SANS/SARA FBI top 20 vulnerabilities as a guide
- Use host based firewall and IDS on any system connecting to the corporate network
- Use a standardized anti-virus product on any system connecting to the corporate network
- Establish a standardized patching policy

Providing a thorough customer education program also has to be considered an integral part of a security program. The weak link of uneducated users could compromise all of the security efforts a corporation has in place.

Vulnerability Concepts

Volumes of information extolling the hazards of the Internet have been compiled over the past few years regarding vulnerabilities of computer systems. A list of common vulnerabilities that can directly impact a corporate network from a remote access user with a home office network is long and involved. Numerous resources exist for system administrators to use to keep current on information regarding vulnerabilities. Several of the common resources are:

- Computer Emergency Response Team (CERT) at www.cert.org[4]
- The National Institute of Standards and Technology's Computer Security Division, http://icat.nist.gov/icat.cfm
- Bugtraq, http://www.securityfocus.com/
- Symantec Security Response Team, http://securityresponse.symantec.com/

These sites cover virtually all operating systems and are constantly updated and routinely send out notices when new exploits are found. This list is merely a small sampling of available resources to keep current on vulnerabilities, exploits, and security tools.

Wireless Networking Concept

The concept of a wireless local area network (WLAN) network is very attractive and rapidly gaining acceptance in the home office environment. Many corporations are also embracing the idea of WLANs. Among a myriad of reasons are WLANSs ease of setup and the fact they are getting cheaper every day. Instead of stringing cables around the office or taking the time and money to have them installed into the walls and the extra equipment that is necessary, a WLAN can be set up in minutes for a fraction of the cost. Additionally, WLAN capabilities are being built into hardware devices, such as Palm PCs and laptop computers making it even easier to deploy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A wireless LAN operates via radio waves using the 802.11b or 802.11a IEEE standard. The "a" and "b" designation refers to the speed of the connection; 11b operates up to 11 mbps and 11a operates up to 55 mbps. An access point (AP) acts as a receiver for radio waves coming from a wireless NIC. The primary issue to understand is when a WLAN is used corporate data is going across the airwaves, thus making it vulnerable to snooping and potentially being captured. When a WLAN is first set up, the AP typically has no security features enabled, which is commonly referred to as "wide open." This is obviously a gaping hole in any network security plan and voids the best policies. "Wide open" refers to the fact that anyone with a wireless network card in his or her computer has wide-open access to connect to the AP. This includes uninvited users who happen by to find the AP. Once connected to the AP your uninvited user can watch everything happening on that segment.

WEP, or wired equivalent privacy, is the industry's effort to protect wireless communications from eavesdropping. WEP encrypts the data between the AP and a users PC using one of several levels of encryption schemes. The minimum is 40 bit encryption while some offer 128 bit encryption, and up to 168 bit encryption. Each level of encryption refers to the number of bits used in the "secret key" and a 24 bit "Initialization Vector" (IV) to encrypt the traffic.

Unfortunately, WEP is not a very secure means of protecting the data as it travels across the wireless link. Using off-the-shelf products can capture data and crack a 40-bit encryption key in just a few seconds. Brad Knowles notes in a May 2001 article[5] "In 1998, the EFF reported the results of their "Deep Crack" machine that was built out of standard off-the-shelf gate array technology to crack the DES 56-bit key, and did so in just 56 hours -- since each additional bit doubles the length of cracking time, this means similar hardware could crack a 40-bit key in about three seconds (56 hours * 60 minutes/hour * 60 seconds/minute = 201600 seconds, and 2^16 = 65536, so 201600/65536 = ~ 3.076 seconds)."

What this demonstrates is WEP does not secure WLANs very well. For this reason many corporations have taken a hard line and are not permitting WLANs to be connected in any way to the corporate network. This prohibition extends to the home networks as well. The short answer is, don't use wireless networks until the security improves.

Mitigating Vulnerabilities

Mitigating vulnerabilities refers to specific steps a user takes to remove or reduce the opportunity for someone to take advantage of security vulnerability present on a computer. Mitigation covers the range of security steps from completely removing a computer from a network to protecting it down to each file being

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

used. A logical process must be used to determine what vulnerabilities exist and how to mitigate as many as possible. The model to be used during that process should follow the computer industry's computer security best practice.

Using the Defense-in-Depth model, the process to mitigating risks starts at the edge of the network, so protecting the network's Internet connection is mandatory. To mitigate the risks of having a home network connected to the Internet, using an Internet router is essential for the first line of defense. The router will protect against hostile intruders wishing to surreptitiously access computer systems.

Using an Internet router prevents a great deal of the vulnerabilities normally associated with being connected to the Internet. The typical Internet router uses network address translation (NAT) to effectively "hide" the computers on the private side of the network. The router obtains a "routable" IP address from the ISP for its external interface. Internally they provide IP addresses to client machines from the private IP address ranges, most typically in the 192.168.0.0 network. The "private IP address" ranges 10.0.0.0/8, 172.16.0.0/11, and 192.168.0.0/16 are reserved for private use only and cannot interact directly with the Internet. NAT translates (the "T" in NAT) your computer's private IP address to a routable IP address permitting it to communicate effectively with the Internet.

Concealing your computer from the Internet mitigates a significant portion of security vulnerabilities since an intruder can no longer scan the computer directly and determine what vulnerabilities your computer may exhibit. There are users (read: hackers) who set up computers to scan the Internet in an effort to find a computer they can break into. That particular hacker will not find your computer even to examine.

Having said that, routers also have vulnerabilities, but those usually have more to do with configuration mistakes rather than software vulnerabilities. When setting up an Internet router, insure any service not required is disabled, change default user names and passwords, and disable remote administration. If a user ever needs remote assistance with the configuration, they can enable it for the time they are getting the assistance and then disable it when finished. Many routers have the ability to block all WAN requests. When enabled the router is, in effect, invisible on the Internet.

Since the process of securing a computer system is a Defense-In-Depth approach, additional security steps must be taken to make sure we protect the corporate data. Host based protection is the next step in the process.

Some important steps to consider when working toward the goal of securing corporate computing resources based on the computer security best practice for securing a host include:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Hardening the operating system
  As was done with the router, disable unnecessary services. Most successful attacks stem from exploiting just a few software vulnerabilities on numerous machines running unknown or unneeded services. The SANS/FBI Top 20 List identifies the twenty most critical Internet security vulnerabilities which, if closed off, will go a long way to having a system hardened from attack. Listed below are the SAN/FBI Top 20 vulnerabilities for both UNIX and Windows operating systems:

  Top Vulnerabilities to Windows Systems
  - W1 Internet Information Services (IIS)
  - W2 Microsoft Data Access Components (MDAC) -- Remote Data Services
  - W3 Microsoft SQL Server
  - W4 NETBIOS -- Unprotected Windows Networking Shares
  - W5 Anonymous Logon -- Null Sessions
  - W6 LAN Manager Authentication -- Weak LM Hashing
  - W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords
  - W8 Internet Explorer
  - W9 Remote Registry Access
  - W10 Windows Scripting Host

  Top Vulnerabilities to Unix Systems
  - U1 Remote Procedure Calls (RPC)
  - U2 Apache Web Server
  - U3 Secure Shell (SSH)
  - U4 Simple Network Management Protocol (SNMP)
  - U5 File Transfer Protocol (FTP)
  - U6 R-Services -- Trust Relationships
  - U7 Line Printer Daemon (LPD)
  - U8 Sendmail
  - U9 BIND/DNS
  - U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

- Host Based Firewall Software (also referred to as personal firewalls)
  Host based firewalls inspect all inbound and outbound traffic on a computer at the networking layer. It permits only the traffic specifically allowed to pass into and out of the computer. Many have the ability to alert users to suspicious behavior and upload their event logs to a centralized server. Also, policies can be created either on the fly or manually and distributed to a large customer base. The policies, although they vary widely, can be configured to look at the traffic by source or destination IP addresse; by the service in relation to the source or destination IP address or, in some cases, by the ports. The policy should start off with “deny all except what I specifically allow.” Windows XP has a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

built-in firewall, however, it lacks many of the basic features required by a corporate environment for control, manageability, and alerting.

- Host Based Intrusion Detection Systems (IDS)
  Host Based IDS detects suspicious events regarding files contained on the computer as well as in communications between computers. It looks for suspicious events based on criteria of evaluating essential system resources. When a suspicious event is detected, it notifies the user or centralized server. IDS has a variety of levels of detection and can alert on such things as changes to the central system and/or log files and unauthorized communications between a user's computer and an unknown or unauthorized system.

- Program Access Protection
  Currently there are several products are on the market that provide this feature as part of a suite of host based protection systems. Program access protection involves a process of insuring a computer is free of viruses and Trojans, then base lining the system by validating the existing programs on a computer. Once baselines of each program's files (there are many files for any one program) are completed and validated, the program access protection software will alert the user of any potential change to the program files. This is necessary since several viruses and Trojan horses have used existing programs to cause damage or propagate itself to other systems. For examplt mail programs were used behind the scenes to send themselves to other users without users ever being aware of it hapening. The program access protection process validates that a program was intentionally used to perform a function. If an alert comes up for a program or a process that the user did not start or request, it would indicate a possible intrusion of the computer.

Since the corporate firewall cannot protect remote users on their home networks, tools such as these are essential in extending protection to the home office resources. When extending a service like the host based firewall, consistency and flexibility are mandatory. To achieve consistency centralized management and reporting are required. Several products are available that contain all three attributes (host based firewall, IDS, and program access) as well as centralized management, reporting and alerting. The best way to describe products such as these is Host Based Protection Software (HBPS).

The ISS Real Secure Desktop Protector (RSDP) combines all three protection products into one centrally managed software suite. Zone Alarm, a very popular consumer PC protection software, and Sygate both have their own versions of this product and can also report to a centralized console and alerting station. For more information on these products, go to:

RSDP: (http://www.iss.net/products_services/enterprise_protection/rsdesktop/protector_desktop.php)
Zone Alarm: http://www.zonelabs.com/store/content/home.jsp

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sygate: http://soho.sygate.com/products/pspf_ov.htm

Regardless of the product that is used for the protection of the home office resources, it must be able to be standardized and centrally managed. A corporation must take into consideration the impact to support staffs versus the level of protection it offers, when a product such as this is deployed. The products mentioned above are just a few examples. There are many more vendors offering similar products. These products are mentioned because they contain the centralized management, reporting, and alerting functions necessary for deployment to corporate home office users.

- Virus Protection
  Anti-virus software examines files based known definitions and characteristics of computer viruses and takes some kind of action. Typically, it will at least quarantine the suspected file and render it useless. Corporate versions of the software have the ability to not only quarantine a file, but also clean it of the virus and alert the user to its presence. Since viruses often arrive in an email, all email traffic should be checked at the server and at the PC level. Even so, some viruses make it through all of the checks intact. The anti-virus software should be able to detect and defend against a virus that is accidentally invoked as well. No computer user, corporate employee or an individual computer user, should ever operate a PC without some kind of anti-virus software running at all times. The corporate policy should state the user is responsible for insuring the anti-virus definitions are updated regularly and system scans are completed weekly.
- Patching Policy
  Forcing and validating home office users actually keep their systems patched is a very difficult challenge at best and impossible at worst. IT administrators will have to educate users to routinely update their systems. There are some software products available that can do patch checks, however, they do not operate well when the systems are remote.

The choice of host based protection software is dependent on several factors. A significant factor to weigh with regards to protecting a corporate resource is to balance the level of data protection with the ability to carry on work as well. If the HBPS becomes too intrusive to live with while doing work, many users will just disable it. This renders the HBPS not only useless, but also it wastes financial resources and does nothing to mitigate the risk of compromise of the corporate data. The HBPS is the perfect choice to mitigate situations where services like file sharing (which uses NetBIOS) have to be used. Typically on corporate and home networks, sharing files are a big part of doing business so NetBIOS has to be permitted. A method of mitigating the risk of file sharing is to close all open shares (via the OS) and “deny all except what is expressly permitted” in the HBPS. In other words, use the HBPS to block everyone from accessing a machine, except those intentionally permitted. This does add a step to the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

process of sharing files, but it is worth the effort considering the vulnerability it closes. HBPS is also a good step to take if a split-tunneled VPN is used for communication to the corporate network. There is more information later in this document on this topic.

In review, we have looked at the home network in layers: connecting to the Internet, protecting the computers using that connection (the use of a router), and protecting computers in areas that the router does not apply by using HBPS, A/V, and system configuration.

Securing the Communication to the Corporate Network

The final step in the protection of the corporate assets on a home network is the remote access to the corporate network, typically through the use of Virtual Private Networks (VPN). When a user creates a VPN session from their PC to another location (may be to another PC or to a VPN concentrator), it is referred to as "creating a tunnel." The effect is that all data going through the "tunnel" is only viewable by users on each end, not anyone in between. A VPN is like a long extension cord that goes from a user's home computer to the corporate network. VPN's come in many forms and vary in capability and cost. As with most technologies, the cost associated with implementing a VPN strategy goes up with an increase in capabilities. Since most home networks are a mix of both computers to conduct corporate business and computers to play games, do personal emails, etc., VPN sessions are typically run from one computer at a time connecting to the corporate network. While tunnels can be created to connect an entire remote network to the corporate network, this is not the preferred method for a home office user.

Windows systems have a built in VPN that comes in several flavors; Point to Point Tunneling protocol (PPTP), Layer 2 Tunneling protocol (L2TP), L2TP with IP Security (IPSec), The Point-to-Point Tunneling Protocol (PPTP) was the initial VPN developed by Microsoft and is used to secure PPP connections over TCP/IP links. In a joint effort between Microsoft and Cisco, using Cisco's L2F (Layer Two Forwarding) protocol, L2TP was developed in an effort to short up PPTP's shortcomings and encrypt the data. PPTP and L2TP are based on the PPP used for dialup networking sessions. PPTP/L2TP is built into every current Windows platform so it is financially feasible (read: free) to employ. Additionally, since it is built into each platform, there is little chance of any conflicts with other Microsoft products.

IPSec is actually a suite of extensions to the IP protocol. It provides two basic functions: authentication/verification, and confidentiality. Authentication makes sure the data came from whom it says it came from and verification insures it has

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

not been altered. Confidentiality means the data could not be read in transit between the sender and receiver.

When comparing PPTP/L2TP and an IP IPSec solution, several things become apparent. L2TP with IPSec is still PPTP at its core. There are improvements for L2TP, but the same basic vulnerabilities that existed in PPTP also exist in L2TP. Bruce Schneier of Counterpane Systems and Mudge of L0pht Heavy Industries accomplished a complete technical analysis of PPTP[6]. In the analysis, they stated, "Because both the Lan Manager and Windows NT hashes are transmitted even in a Windows NT-only environment, it is possible to attack the weaker Lan Manager hash in every case." Even using IPSec to encrypt the data, the core underpinnings of the PPTP/L2TP are still weak and vulnerable.

Recently it was brought out that L2TP is also vulnerable to a replay attack as well. On Oct 7, 2002, SANS reported in their Critical Vulnerability Analysis (CVA): (http://www.sans.org/newsletters/cva/cva1_11.php) describing the vulnerability.

According to a posted advisory, Win 2000/XP servers running a PPTP server or client are vulnerable to a buffer overflow. A remote non-authenticated attacker can send a maliciously crafted PPTP packet to port 1723/tcp on the victim (both PPTP servers and clients listen on this port) and cause the system to hang. Further, it is believed that the vulnerability allows remote execution of arbitrary code with system privileges.

IPSec on the other hand does not have PPTP at its core. It is a suite of options applied to IP. When IPSec is used to secure IP traffic over the Internet, all of its components act together. Considering the weaknesses of PPTP/L2TP, going with a straight IP IPSec solution is a more secure way to go. There are numerous vendors who do various types of VPN's, but the mainstay in the security world for a client machine VPN connection is IPSec. It offers options for authentication and confidentiality. Many of the VPN systems (also referred to as appliances) are easily managed through web interfaces. While PPTP/L2TP may be a little cheaper to initially set up, the cost is easily off set for a large corporation to have the flexibility and security an IPSec VPN appliance offers.

A typical VPN can be setup in two modes; split tunneled and non-split tunneled. A split tunnel connection permits a user while on their home network to connect to their corporate network through a VPN and maintain the ability to go directly to the Internet and the local machines. The best analogy would be a garden hose as a VPN. You can stretch the garden hose across the street to another house (your connection back to the corporate network) and put water on (send data to) your neighbor's yard. All of the water is going to your neighbor's yard and nothing is going into your yard. That would be a "non-split" tunnel. To have the ability to water your yard and your neighbor's at the same time, you could put a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

splitter at the spicket. If you connected a hose in your yard and one to go across the street, you have a split-hose setup to water both yards at the same time. Your data is the same as the water, when a VPN is run in split-tunnel mode you can send data locally (your hose) or send it to the corporate network (the hose to your neighbor's yard). Here is a diagram to illustrate the differences.

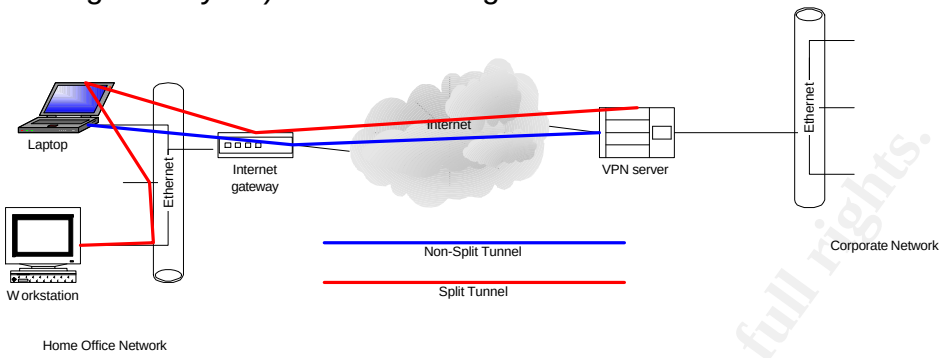


Diagram 2

A significant security concern with regards to tunneling is the choice of split-tunneling versus non-split-tunneling. A split-tunnel is not the most secure way of setting up VPN tunnel. Actually, it violates a general security principle of bridging different networks in some people's minds. Having a split tunnel VPN exposes users to the potential of having a PC remotely controlled by a hacker on the Internet who can then use the VPN connected machine to get to the corporate network. This is what happened to Microsoft during 2000. This type of activity is so difficult to detect and track; the hacker who exploited the split-tunnel connection into Microsoft is estimated to have run around the internal network for a matter of weeks before being detected. To see more about the intrusion, please go to http://zdnet.com.com/2100-11-525083.html?legacy=zdnn. To combat this vulnerability, a HBPS can be used to reduce the possibility of a hacker being able to remote control a session as happened in the Microsoft case.

Summary

Since conducting business at a home office has become routine, corporations have no choice in regarding them as a network resource. Proactively taking steps to insure corporate home office network resources are protected will be money well spent if it prevents even one intrusion. Adapting the corporate computer security and usage policy to home office resources have to be protected, wherever they may be located. Conceptually understanding home office network vulnerabilities and security practices is essential to process of securing all resources. Security for WLANs has not yet matured enough to properly secure them and as a result, they should not be used. However, what should be used is an HBPS along with an A/V product with a strict updating routine. Insuring system patches are updated is another area to help mitigate vulnerabilities that are commonly exploited. Typically, PPTP or L2TP are not the corporate VPN of choice. Third party solutions are more secure and offer more flexibility and choice options. Taking the information in this paper into

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

consideration and applying it to the home office environment will significantly reduce the increasing threat to a corporate network. The smart business decision in securing the home office resource is one of being proactive and not reactive.

References:

1. Microsoft Unveils Tools for Secure Home Networking, Sept 19, 2002
Paul McDougall
http://www.informationweek.com/story/IWK20020919S0004

2. Home Networking: Definition and Overview
No author identified:
http://www.iec.org/online/tutorials/home_net/

3.The Corporate Home Office Computer Security and Usage Policy, Jan 2003
Actual Text
Michael Scott, ABC Company (real company name was changed

4. Common Vulnerabilities
Computer Emergency Response Team (CERT)
General Information pages
Oct 2002
www.cert.org

5. Is Your Wireless Connection Secure?
May 21, 2001
by Brad Knowles
Columnist

http://www.powerbookcentral.com/columns/knowles/052101.shtml

6. Cryptanalysis of Microsoft's Point-to-Point
Tunneling Protocol (PPTP)
Authors
Bruce Schneier
schneier@counterpane.com
Counterpane Systems
101 East Minnehaha Parkway,
and
Mudge
mudge@l0pht.com
L0pht Heavy Industries
P.O. Box 990857
Minneapolis, MN 55419 Boston, MA 02199

http://www.counterpane.com/pptp.pdf

© SANS Institute 2003, Author retains full rights.

Miscellaneous Resources

Security of the WEP algorithm

Jointly by Nikita Borisov, Ian Goldberg, and David Wagner
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
Jan 2001

Institute of Standards and Technology's Computer Security Division,

ICAT web page
Oct 2002
http://icat.nist.gov/icat.cfm

A firewall in an IT system

Date:	**Aug 30, 2002**
Section:	**Articles :: Firewalls & VPNs**
Author:	**Krzysztof Zagrodzki**
Company:	**Krzysztof Zagrodzki**
	Printable Version

The term "firewall" evokes the image of a solid wall in a building, which prevents a fire spreading from one part of the building to another. Sometimes it is understood as a "wall of fire" blocking the entrance.

Making the Connection: IDC's 2002 Annual Consumer Survey on PCs and Home Networks
Dec 2002
Schelley Olhava and Danielle Levitas
Dec 2002 Doc #28622 Study
Price $4,500

Operating Environment Minimisation for Security
Jeffrey Bailey
March 25, 2002
http://www.sans.org/rr/sun/op_environment.php

IEEE

Institute of Electrical and Electronics Engineers
http://www.ieee.org/portal/index.jsp

Building an In-Depth Defense

July 9, 2001
Brooke Paul
http://www.networkcomputing.com/1214/1214ws1.html

RealSecure Desktop Protection

Jan 2003
http://www.iss.net/products_services/enterprise_protection/rsdesktop/protector_desktop.php

Norton Anti-Virus

Jan 2003
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=64&EID=0

© SANS Institute 2003, Author retains full rights.