Global Information Assurance Certification Paper

Applying Defense in Depth Concepts to Small Office, Home Office (SOHO) Networks

by

Michael A. Zeigler

A practical submitted in partial fulfillment of the requirements for SANS GSEC certification (Option 1)

6/7/2004

TABLE OF CONTENTS

Executive Summary

This paper will explore the explosive growth in home PC networking, including a discussion of the various broadband connectivity alternatives, firewalls, and risk mitigation strategies. It will provide comprehensive and actionable guidance in planning, implementing, configuring and monitoring a home network, to assure the owner a most pleasurable and secure networking experience.

Being an IT professional, I have been involved with Networking and to some extent Security for several years. This included building large scale private, Frame Relay, and more recently Internet VPN networks in the private sector. In addition, I will cover "practical aspects" of home office networks by sharing my experiences in planning and deploying my own home network.

In the recent past, I have personally set up and configured home based networks using both cable modem and DSL from several different providers. I also recently upgraded my home network to wireless, to enjoy the convenience of being able to move about with my laptop without the annoyance of long patch cables or the effort and expense of installing Category 5 cabling.

By spending the time to consider and deploy a few basic security measures at differing points in the network, the home user can gain a significant amount of security, monitoring and control over the typical "out-of-the box" installation. I hope that others may gain some insight and will be able to avoid some of the pitfalls into which I have fallen. Experience is often the best teacher.

Growth of PC and Broadband

Home PCs Sales Increasing

All it takes is a glance at a computer store flyer, or a visit to a PC vendor or VAR website to see that PC prices are dropping like a rock. The main players in the market now seem to be HP and Dell. HP sales recently climbed by about 20%, attributed mostly to a rise in sales of notebook PCs. HP said that notebook sales grew by 60 % year-over-year, twice the market rate. [1]

It is not surprising that many of these consumer PCs are purchased for Small Office / Home Office (SOHO) networks connected to the Internet. In fact, "…56% of Americans now use the Internet." [2] In terms of rate of growth, the number of broadband subscribers increased by almost 50%, while the number dial-up users dropped by 12% (May 2003), according to Internet measurement firm Nielsen/NetRatings. Students, accounting for about 7.8 million users, are seen as the largest collective users of broadband. [3]

Also consider the following US Government statistics: [4]

- Between August 2000 and September 2001, residential use of high-speed, broadband service doubled—from about 5 to 11 percent of all individuals…
- Forty-five percent of the population now uses e-mail, up from 35 percent in 2000. Approximately one-third of Americans use the Internet to search for product and service information…
- Among Internet users, 39 percent of individuals are making online purchases and 35 percent of individuals are searching for health information...
- With more than half of all Americans using computers and the Internet, we are truly a nation online. At work, schools, and libraries, as well as at home, the Internet is being used by a greater number of Americans.

AOL Users moving to Broadband
Casual users are moving away from AOL in large numbers, many of them going to broadband services provided by their cable TV or home telephone company.

"The company's (AOL) dial-up subscriber base has declined by nearly 2 million subscribers over the past four financial quarters because of subscriber defection to broadband…In the quarter ended Sept. 30 (2003), AOL reported a 688,000-member decline and a 33 percent drop in advertising revenue from the previous year." [5]

Many of these users are not Internet savvy, and are not fully aware of the dangers of an unprotected broadband network. This brings about increased risk.

Why protect?

While you may not have classified or proprietary data on your hard drive, stop to think about the personal information it might contain about you. Have you used your PC to…

Check your bank balances or run financial software like Quicken?
Do your taxes?
Make purchases on the Internet?
Download and store data files?
Open and send e-mail?
Use a word processing package to create and save personal documents?
Keep a home budget in Excel?

It is unlikely that you would be willing share or post personal data of this nature on the Internet. Also, data integrity is important since you would not want this data to be changed without your knowledge. So it is a vital asset – it has value and is worth protecting.

Risk of loss is also an important consideration. How much wasted time and effort would go into rebuilding the PC from scratch? Not to mention the aggravation, monetary costs, and loss of productivity during the downtime.

Identity theft is a major concern when doing business on the Internet. The loss of secure information such as credit card numbers would be a major issue for any consumer.

One other thing to consider, how would you feel getting a call from your ISP telling you they are detecting Denial of Service (DoS) traffic from your IP address and to cease and desist immediately? You have no idea what's going on, but have a sinking feeling you've been had…

A much more comprehensive reference entitled "Home Network Security" from the CERT Reference Center can be found at:
http://www.cert.org/tech_tips/home_networks.html

Additionally, a good interactive resource (including a newsletter) from Microsoft is found at: http://www.microsoft.com/security/protect/default.asp

Broadband Alternatives and Cost comparison

In most areas, the primary choices for broadband Internet access will be Cable Modem or Digital Subscriber Line (DSL). Comcast offers broadband cable modem access via its expansive Cable television presence.

DSL services are normally provided by the telephone carrier. Here, Verizon arrived on the scene a little later, but come to the market from a strong position as an RBOC. Their recent marketing blitz touts broadband DSL for a mere $ 29.95 per month and new subscribers get the first month free. After three months, the price goes up (unless you sign up for additional Verizon local service bundles).

For a very comprehensive listing and review of Broadband carriers, see the Broadband Reports website at www.broadbandreports.com.

Security aspects

The Security methods presented in this paper provide countermeasures to protect the home network PC user regardless of the choice of ISPs or network access methods. I would like to briefly address some of the inherent differences and similarities in broadband access methods, particularly cable modem and DSL. In the end I would suggest that as long as you stay with one of the larger, more established providers, the deciding factor may be a matter of price or performance.

Broadband signals for cable modem leverage the existing cable network, which is a shared media, tree like architecture. The cable signal is distributed over coax cable which is divided and subdivided many times before eventually reaching your home. Due to this shared infrastructure, it is possible that someone having access to a network Sniffer (e.g., Snort) could intercept your data. Also, as the infrastructure is becoming more saturated, cable companies are starting to limit end user bandwidth. Comcast, critics say, is imposing limits without telling consumers that service is limited. [6]

DSL is deployed in a star topology using a dedicated local loop, the DSL signal being carried over "dedicated" copper cable. This is part of the existing telephone company infrastructure, so there is less chance of snooping. However, bandwidth limitations may be an issue depending on the DSL technology in use and your home's distance from the telephone company central office (CO).

I had subscribed to DSL prior to the availability of cable modem. When cable modem was available, I signed up with Comcast and was generally happy with the service. I recently changed back to DSL by taking advantage of a Verizon DSL promotion, due primarily to cost considerations. With the new Comcast offers, I am probably going to jump back to cable modem.

Wireless Internet Access

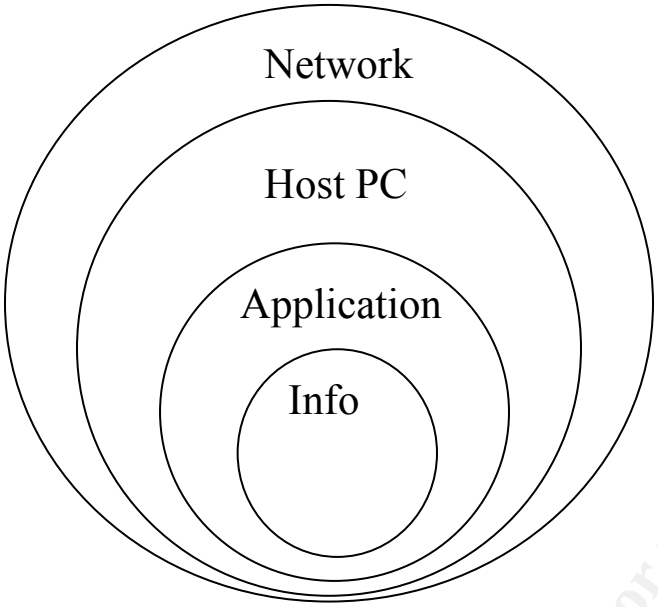
If you reside in a rural area, there may be limited broadband options. DSL has the noted distance limitations and cable TV has not extended too far out of suburbia. Your only alternate to dial-up might be ISDN. Since ISDN is normally usage priced, it can get very expensive.

Another alternative may be wireless. In the Northeast, Beacon Wireless provides ISP access to rural areas, see www.beacon-wireless.net.

Also check out the listings on Broadband Reports to research the alternatives in your area. Regardless of the ISP or access method, the security principals discussed here should be of great value.

Applying Defense in Depth Principals

The following drawing is a good way to visualize the concept of Defense in Depth [7]



As the figure illustrates, at the core is the information you are trying to protect. Around the core are successive layers of security controls applied at various layers, or places in the SOHO network. For example, virus scanning is a control that exists in the application space.

A firewall is another countermeasure that exists in the Network layer. The safety and security of the core data is well protected in that an intruder must compromise multiple differing defenses at various points to get at the protected information resources.

"Each of these technologies complements the others and helps to create a more effective security program…By layering technologies, we are in effect closing the windows after locking the doors." [8]

This paper will discuss and examine at a high level many different security controls for the SOHO, giving specific guidance and recommendations for effective protection.

Network Design

It can be said that a good Project Manager will "begin with the end in mind…" This is also good advice in the networking world. If you are thinking about a home network, here are some things to think about before you dig in. The better you plan up-front, the easier it will be to "build-in" security and the fewer problems you'll have in the long run:

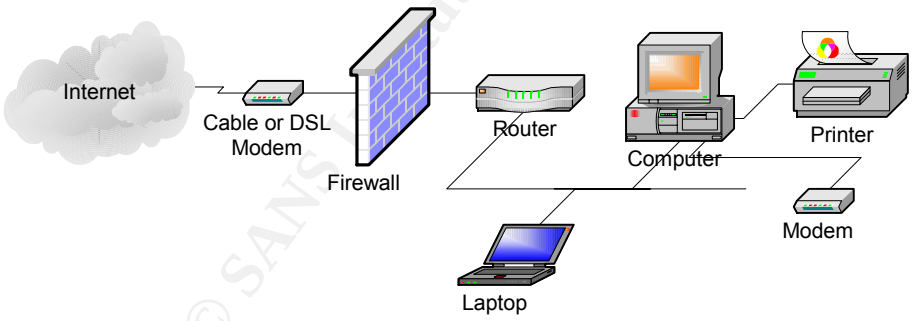
- What devices and how many do I need to connect?
- Where am I going to locate the equipment? Do I have enough power outlets?
- Do I need Wireless?
- Do I need Network Printing or Printer Sharing?
- Do I need a VPN? Will I need to handle any incoming connections?
- Where will I place my Firewall (stand alone, in router, in PC)?
- What is my budget?

In terms of Security, we sometimes think of it as a binary thing – either something is or is not secure. It is often helpful rather to think of Security as a continuum - as more and more Security is applied (generally at increasing cost), the level of risk is decreased. The challenge often is to find the balance point between the cost of safeguards, and the value of the data itself.

It is outside the scope of this document to cover details of asset valuation, but the point here is to consider cost and what you are protecting. A good rule of thumb in a SOHO is to keep things simple. If you can implement a security measure for little or no expense, then it is probably a good idea for most users to implement it.

Your plan should result in a procurement list and a simple network diagram, such as the one that follows. This will form the basis for building and configuring a secure SOHO network.

Home Network Basics and Security Components



Typical SOHO Network

The figure above represents a good model for a typical SOHO. The WAN router will most likely also perform the functions of a network firewall (software), however it is not uncommon to find other stand-alone systems (e.g., Cisco PIX, Nokia, etc.).

SOHO Router configuration basics

Note: The information in this section was compiled primarily from experience with the Linksys and D-Link routers however the principals should apply universally.

The first visible step (after planning) to establishing a SOHO is to purchase the equipment and to make the necessary physical connections, according to the plan. Good organization is key from the start. Use quality patch cables of varying lengths, cable labels and cable tie raps and take the time to create a clean physical network. The time you put in upfront will most certainly pay off later when you have to troubleshoot a problem.

Most home routers come with integrated hub or switch ports. When plugging in the cables be sure to identify the WAN or uplink port (where the cable from the cable or DSL modem goes). Also, there may be a special port designated as the DMZ port (more about that later).

Another good practice is to pull out a hard copy of the network drawing and document the configuration and settings (IP addresses, etc.) while you work. Jot down your changes to "default" settings. Some ISPs require special values like hostnames or domain names to be included in the configurations, so make sure they are also included.

RTFM, especially for security issues

OK, I admit it, sometimes I let my enthusiasm get the best of me and I dig in before reading the manual. Try your best to avoid doing this. Reading the manual is probably the best way to assure a secure and trouble free installation. Take some time to look it over carefully.

Configure the router for maximum security

Most routers can be configured using a web browser. Simply enter the router default LAN IP address, and then provide the user name and password (typically admin).

Before going any further, CHANGE THIS!!!!! The user name and password of "Admin" is the most insecure password (it's not much better than no password) and this presents a great risk. Everybody knows this as a default password.

Enter a unique password that complies with strong password rules (see below). Do NOT use readily guessable things like the word "password", the name of your spouse, children, favorite team, or other words found in the dictionary. These are all really bad passwords. I would also change the username, if possible from "Admin" to something unique, such as "Operator".

The rules for strong passwords are:

- A mix of upper and lower case letters
- At least one number (not in the first or last position)
- At least one special character (like "!")

Be sure the password is 8-12 characters long. This protects from "brute force" attacks and a long password improves disk encryption. Writing it down is not a good idea, but if you must, make sure it is kept in a secure place. This might be accomplished by placing the written password in a sealed envelope and placing it in a secure location.

Another common scheme to help remember strong passwords is to create a password based on a popular phrase, book title, movie or the like. For example, "usethe4sLuke!"

Code updates – firmware and software code

The next thing is make note of the router OS and firmware versions and visit the vendor web site to assure you have the latest. It is a good idea to run the latest major release, and avoiding minor releases or patches unless you have a particular need. Print out and read the release notes carefully. There may be known issues for your environment.

A more conservative approach, referred to as "N minus one" would be to avoid the latest major release and go to the previous major release. Although this approach may be more risk aversive, in a SOHO environment you should be OK with the latest.

The following excerpt from PC World magazine is a great example what can happen if you fail to check for upgraded software. "Linksys BEFSR41 EtherFast Cable/DSL Router is a low-cost router… A security hole in some versions of the software--called "firmware"--used by the router could allow a remote user to cause the device to crash…The damage might be slight… But they recommend that users upgrade the router firmware to version 1.42.7 or later to guard against such an attack." 9

Setting up the IP addressing (DHCP)

Using DHCP for the local LAN is simple and efficient. Computers on the LAN can obtain IP addresses from a DHCP server built into the router. This is an example of the principal of using centralized control and will simplify network configuration and change management.

For security purposes you may want to limit the pool of addresses or use static DHCP. My D-Link router came with a default pool of 100 addresses (way too many for me)! I have a maximum of three PCs so I changed it to three. I recommend that you take a similar approach, especially in a Wi-Fi network.

Another option is to link the DHCP supplied IP address to the specific PC MAC address (Network Interface Card). This is done by entering the PCs unique physical or MAC address (e.g., 00 B0 D0 57 C5 C5). If you do this for all PCs on the LAN, "rouge" devices will not be able to get an IP address or join your network. This option is also useful if using filtering or firewall rules based on specific PCs.

A useful GUI Windows utility that is easier than entering DOS commands for checking and troubleshooting DHCP issues is WNTIPCFG and can be found here –

http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/wntipcfg-o.asp

Network Address Translation (NAT)

Most all SOHO routers rely on Network Address Translation (NAT) as the main feature to secure your LAN from the Internet. NAT prevents outsiders on the Internet from identifying the actual IP address of a PC inside the firewall or router. This is the simplest and safest configuration if you do not require communications originating outside of your LAN.

On a LAN each computer is assigned its own logical IP address. When the router gets data to be sent out to the Internet, it replaces the "inside" source IP address with a different routable IP address, called a "translated" or "hide" address. The data transmitted out to the Internet therefore does not contain the actual IP address of the source computer. In this way the inside PCs are hidden, safe from potential attack.

Perimeter Security using a Firewall

The term firewall is generally used in Security to describe a device or measure that protects a network. Much like a physical firewall prevents the spread of fire from one physical location to another, a data firewall controls or limits the flow of data between network segments. These segments are commonly referred to as the trusted network (the LAN), and the untrusted network (the Internet).

Firewalls are commonly implemented either as stand-alone devices or as a distinct part of the router. In a home network, the WAN router is typically the gateway to the Internet, so purchasing a router with a built-in firewall is a good idea. It will protect the entire local network, while providing traffic management and basic logging functions to alert you in the event of a potential threat. More extensive capabilities are provided in a stand-alone firewall such as a Cisco PIX or Nokia firewall appliance.

There are two basic firewall types in use today, Stateful Packet Inspection (SPI) and Proxy firewalls. SPI firewalls inspect data packets to make sure they are permitted or that they correspond to an established request. Unsolicited or possibly harmful packets are dropped in the "bit bucket".

SPI firewalls inspect the IP address header of the data, so you configure them to make forwarding decisions relative to an established rule set. Rules can permit or deny traffic in a variety of ways including by protocol, host address, subnet, and destination. Rules are directional, so they can (must) be applied to outgoing traffic, incoming traffic, or both. SPI firewalls also become aware of where connections originate from, thus understanding their state. They uses this information in the decision process. For example, connections are allowed in from the Internet only if in response to a request originating inside the firewall.

Proxy firewalls work like a "middle man" to the Internet, and handle communications by masquerading as an end system, while establishing their own background connections to the Internet host. The source PC thinks it's talking to the Internet, and the Internet host thinks it's talking to the source PC. Proxy firewall proponents claim that these firewalls provide more protection than SPI firewalls. "When communication is attempted, the message is moved up the stack to the application level - such as FTP, HTTP or Telnet. At the application level, more data can be analyzed than just the address header…." [10]

CERT also advocates the use of firewalls, citing another advantage, "Firewalls are also important since they can provide a single "choke point" where security and audit can be imposed….the firewall can act as an effective "phone tap" and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc." [11]

Set up logging – Linksys utility or other

Maintaining and reviewing the router/firewall logs on a regular basis is a key defense in depth approach to Security. It is important to identify scans and trends to identify and prevent potential intrusions. Logs will most likely be cleared if a device is rebooted, so some routers allow sending the log information to an external source.

Log distribution might be accomplished either by e-mail or SMTP, requiring you to invoke the transmission manually or done automatically via a remote syslog function using a syslog server. I find the syslog server a real advantage, since this allows much greater capabilities to parser to analyze the log information. Linksys provides a free log viewer on their website.

IP Filters

IP Filters can be used to block specific internal LAN users from accessing the Internet. You can set up a filter on an IP address, protocol, or network Port number. This can be useful for example to implement a form of parental control. IP and/or MAC Filters could be set up to allow web browsing (HTTP) but deny file transfer (FTP).

IP filters are normally applied to the outbound traffic and will block traffic to web sites (URLs) pre-established site URLs, sites containing a specific key word match (e.g., "porn"), or even entire Internet domains (e.g., nasty.com).

Another feature of IP filters is a scheduling capability to filters only during certain time periods. This could be used to control Internet access during periods which the network is not under your physical control (e.g., “latch key” children at home). You could set-up a filter to be active only during business hours, say 8 AM until 6 PM.

Use of IP filters can also improve overall SOHO security. Underground web sites are notorious for using unscrupulous cookies, ActiveX controls, adware and other malware. They frequently use social engineering techniques, trying to fool the unsuspecting user into taking an action to permit unwanted program installation (in response to a prompt appearing to be beneficial). The changes may not manifest themselves until later, such as seeing a different IE home page or toolbar, or much worse discovering a rouge application has been installed.

Blocking WAN requests

To block external parties from getting a response to an ICMP (ping), you will want to enable the "Block WAN Request" feature. Selecting to block WAN requests will drop any TCP requests and ICMP (ping) packets, rather than returning anything that could be used by an intruder.

By blocking WAN Requests, your network IP address is totally stealth to ping. It also adds another layer of security to your network by hiding network ports. Not blocking WAN Requests returns an unreachable message which may allow an outsider a clue that there is something there to work their way into.

Dynamic Routing

Dynamic Routing enables use of a routing protocol such as Routing Information Protocol (RIP). RIP broadcasts routing information to other routers on the network. Unless you have a very complex home network I would not recommend running a routing protocol or enabling dynamic routing.

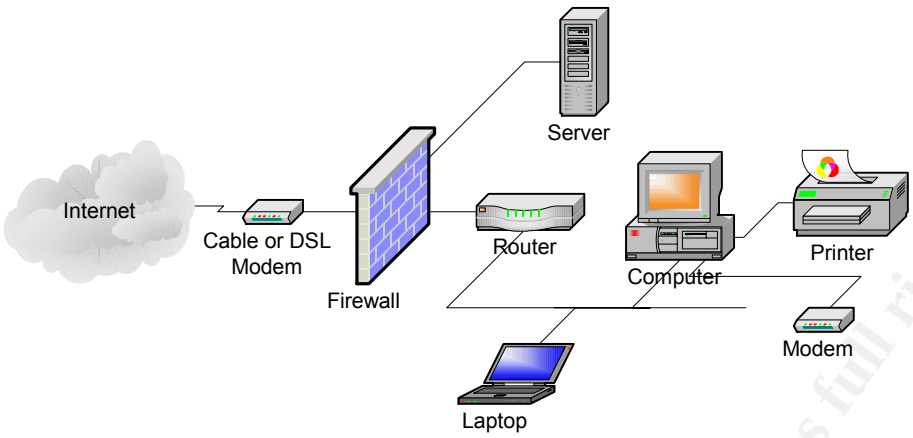
Static Routing

Generally disable. If there are multiple routers on your home network, it may be necessary to configure static routing. Consult you router documentation if you need assistance.

DMZ Host

A DMZ Host would be used to allow a specific local LAN PC or server machine to be exposed to the Internet. This would be for a special-purpose service such as a web site, or FTP server. Exposing a single computer by the computer’s IP address is preferred over otherwise exposing the entire LAN.

The following drawing illustrates the most common SOHO architecture including the addition of a DMZ and host server.



Typical SOHO Network
with Server

There are significant risks in exposing a PC even if it is on a DMZ. Unlike in NAT, this machine's IP address will be routed on the Internet. This means that it will be vulnerable to attacks like SYN flood and DoS. It could also be used as a "hopping off point" if compromised. Although it is beyond the scope of this paper to discuss all potential attacks, further information from Microsoft on hardening the TCP/IP stack and effective countermeasures can be found at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTHardTCP.asp

Virtual Private Networks (VPNs) and IPSec

VPNs enable secured Internet communications with other remote computer systems, typically a corporate network. This is done by using a secure, encrypted connection or "tunnel". The most common VPNs use IPSec tunneling to provide an easy way for the remote user to access secure resources. For example, a telecommuter may have a VPN connection from the SOHO to access secure resources behind the corporate firewall. More recently, SSL VPNs are becoming popular because they typically do not require special VPN software on the client PC.

If you require secure connections via VPNs, most routers have the ability to use IPSec tunneling. Consult the specific router documentation.

Blocking NetBIOS
A common exploit on Windows based computers is file and printer sharing. If you do not need file and printer sharing delete it (use IP printing). Be sure to block NetBIOS traffic from getting out to the Internet. This is accomplished by blocking TCP ports 135, and 137 thru 139. That will filter out well known ports for protocols related to file and print.

Remote Management and Upgrade
Remote Management allows the router to be configured via the WAN interface, presumably across the Internet. It is useful only in the case where you want someone outside the firewall (e.g., vendor technical support) to be able to login to the router for problem resolution purposes. It is best to keep this disabled at all times and turn it on / off for the very rare case described.

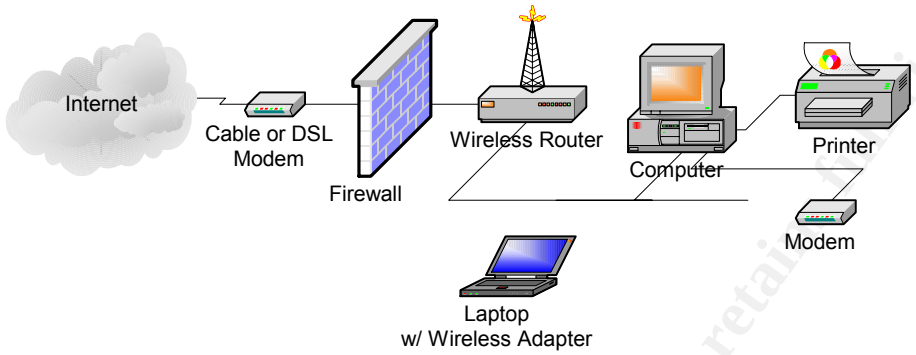
SNMP and Community strings
Recently publicized threats to the Simple Network Management Protocol (SNMP) have resurfaced on the Internet. Some SOHO equipment may include support for SNMP. Although SNMP is useful if you want to see network management statistics (e.g., bandwidth utilization) from your network devices, you should disable it if not needed. If you do want it, care must be taken to assure devices running SNMP are secure.

Here are some guidelines:

- Allow SNMP only on a trusted interface (e.g., the LAN side).
- Change the default community strings to something unique (never use “public” and “private”).
- Disable SNMP write access and only enable read.
- Set-up an SNMP access list and include only the IP address of your system.

Wireless security

The following drawing illustrates the most common SOHO architecture including the addition of a Wi-Fi router and wireless LAN.



Typical Wi-Fi SOHO Network

Wi-Fi routers, access points and network card prices are coming down fast. The introduction of newer 802.11G or 54 Mbps wireless gear has resulted in bargain basement pricing on older 802.11B, or 11Mbps gear. Both standards use 2.4 GHz technology which provides adequate coverage for about 200-300 feet. Walls and ceilings will reduce coverage significantly, so placement of the router or AP should be central to the desired coverage area. Also, other devices that generate RF signals such as cordless phones and microwave ovens may affect signal quality. I recently purchased a bundled B router and PCMCIA card for about $50 (after rebate). In fact, I'm typing this section right now from the comfort of my Living Room couch.

If you're going to create a WI-FI home network, here are some additional security concerns to think about. These risk factors will vary depending upon where your network is located. If you live in a city and are close to roadways and other buildings, the ability for someone to discover and use your wireless network for free bandwidth to the Internet might be a concern. If you are in a rural area, the risk of stealing service or snooping data while being undetected could be minimal.

LAN (wireless) side - SSID

The Service Set Identifier (SSID) will normally be set to "default", so it should be changed to a unique value for your network (e.g., AP001!). This is similar to an SNMP community string – if you don't have the correct value, the devices will not communicate. In order for a wireless client to connect, they will need to configure their PC card to match the SSID on the access point or router.

It is a good idea that you make all configuration changes to the AP or router from a LAN (wired) PC, not from the wireless client. Some changes, such as the SSID will cause a disruption of the Wi-Fi communications, and could create significant re-work.

WEP Encryption
WEP stands for Wired Equivalent Privacy. It is normally DISABLED by default. If encryption of the wireless traffic is desired, typically either a 64-bit or 128-bit can be selected either using a HEX or ASCII key. Encryption will certainly affect wireless performance, so depending on your situation you can deicide whether or not to use it. This encrypts the wireless traffic to the AP or router and thus prevents someone with an RF sniffer from intercepting and reading it (clear text).

Authentication
Usually if Encryption is enabled, you can also select to have the wireless clients authenticate themselves to the AP or router. This would be a good idea if using encryption.

Transmit Power
Again, depending on your particular situation, this may or may not be a risk factor; however there usually will be some control over the output power (watts) of the Wi-Fi transmission. The idea here is that you can crank down the power to avoid "leakage" of the RF signal outside of your desired geographic coverage area. This would be useful in a small apartment or office.

It may take some time to get all of the WI-FI settings configured the way you want them. If all else fails, do like I did and reset the router to factory settings and start over!

PC Security (WinTel)

Now that we've covered some of the security aspects of the SOHO network, let's start from the inside out, reviewing some of the controls that can be applied to PC end systems, working our way out toward the network perimeter.

Hardened OS
The first step to securing a home PC is to install and configure the OS in such a way as to provide only the applications and services that are necessary for the end user. Since most PCs these days run a Microsoft Windows OS, and that is what I am most familiar with, I will focus primarily on the Windows based OS.

Services – delete or shut down
Non-essential services such as the following vulnerable ones should be disabled or removed:

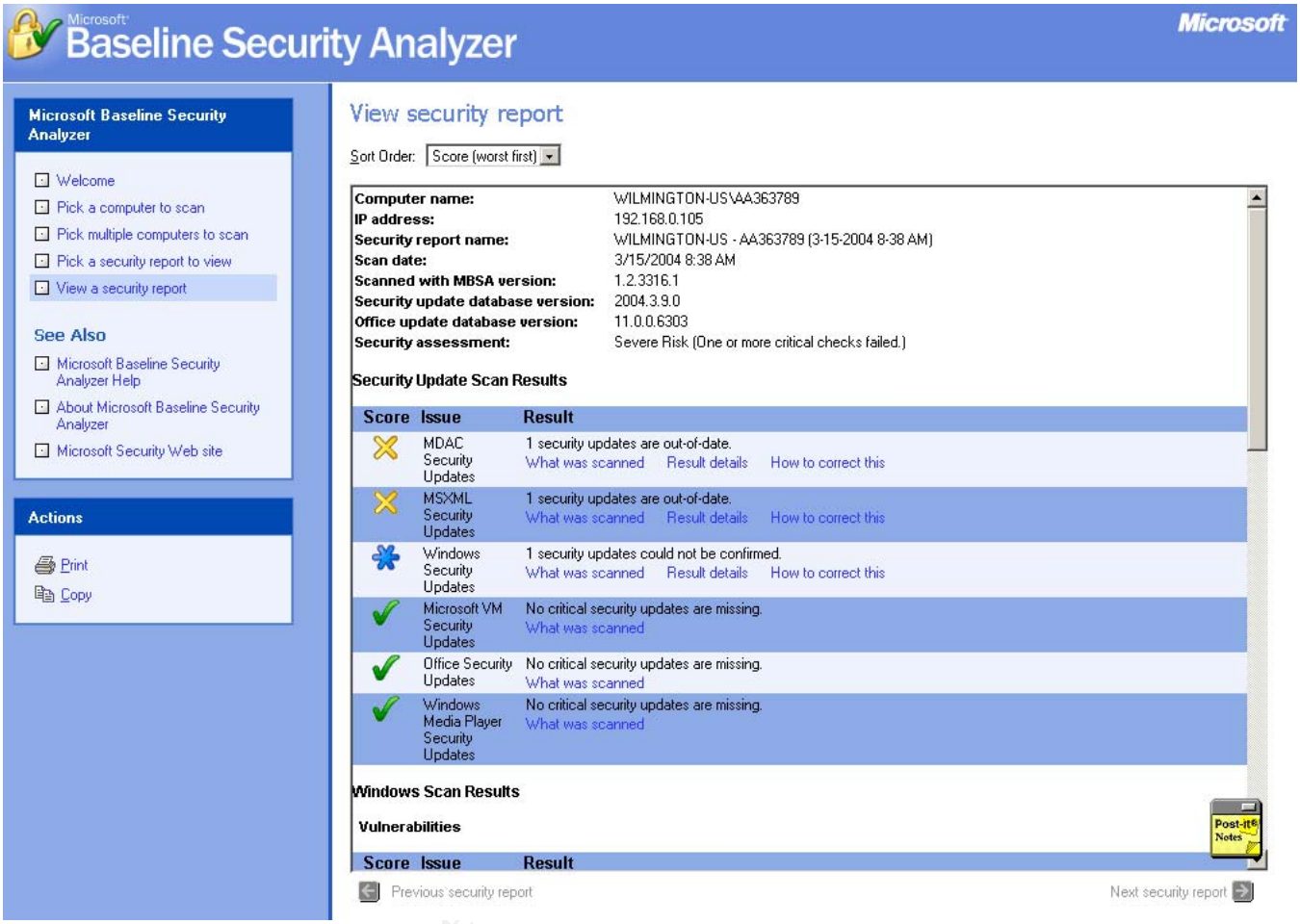
- FTP
- Telnet
- Web (IIS)
- SMTP
- File and Print
- Remote Management

A more detailed reference (Windows 2000) can be found at:
http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp

Microsoft Baseline Security Analyzer (MBSA)
Mighty Microsoft seems to be doing a lot these days related to PC and Software security. They recently released a significant update (1.2) to their Microsoft Baseline Security Analyzer (MBSA). The update includes scanning for updates to more applications (e.g., Office) and provides more features, such as ICF configuration checker.

I recently downloaded, installed and ran the MBSA (see below). The initial report flagged my system as a "Severe Risk". There were two Windows Security Updates and one Office Security Updates missing. The report interface is quite nice, having links to explain the issues as well as "fix it for me".

Here is a sample MBSA report:



The program did not run without flaws, however. One of the critical updates flagged was MS03-030, and issue with DirectX. When I followed the link to the source page, the patch applicability specifically stated it was only for Windows XP. My system is Win 2000. Other than that, I was quickly and easily able to install all of the updates I needed. In addition, there was also several less sever issues MBSA identified including vulnerabilities with non-expiring user passwords, open shares, and potentially unnecessary services (e.g., telnet).

I suggest that everyone running a Windows OS view the Microsoft Security page and download the MBSA at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp

Patch management - Shavlik tools

The developers of MBSA, Shavlik technologies, have a very useful patch management tool called HFNetChkPro. It goes beyond the MBSA and incorporates scanning, reporting, and patch deployment. It can be found at: http://www.shavlik.com/

Microsoft Windows Update

Anyone who runs a Microsoft OS or applications should be up close and personal with the following URL http://v4.windowsupdate.microsoft.com/en/default.asp

With this resource, you can keep your Microsoft products up to date with minimal effort.

Other Vendor sites

One of the best ways to stay in touch with updates to your hardware and software is via e-mail. Most PC vendors' web sites include an area for registering you equipment and creating a profile. The advantage to setting up a profile is that e-mail notifications are targeted to the specific model, operating system, or environment of your choosing. In this way you are not overwhelmed with e-mails that you don't care about.

Dell File Watch

I really like this service from Dell, and I wish other vendors would take their lead. You can sign up for File Watch on the Dell support site. It's a breeze; you simply enter your e-mail address and service tag of your system. File Watch links with the records of the system and knows details like model, version, OS, BIOS, drives, etc. The service then looks for new files that specifically match your system. When a relevant file becomes available, it sends you an e-mail.

For example, an e-mail like this just arrived for one of my Dell laptops:

> Greetings from Dell's File Watch service! File Watch has located a new file that matches your current profile. Service Tag: 2SM5QXX System model: Latitude C510 Criticality: Optional. Dell recommends the customer review specifics about the update to determine if it applies to your system. File Date: 2003-12-01. File Category: Network Drivers, Supported Devices: Dell TrueMobile 1150 Series PC Card Release Type: Driver Dell Version: A20 Vendor Version: 7.44 Supported Systems: Latitude C500, Latitude C510, Latitude C540…Supported Operating Systems: Microsoft Windows 2000
>
> File Description: Device driver version 7.44 (A20) for the True Mobile 1150 Wireless PC card. Windows 2000. Fixes and Enhancements: New feature enhancements.
>
> You can view the details of this file at the following location...
>
> [http://support.dell.com/FileLib/Format.aspx?ReleaseID=R70175&sws=fw]

Without effort on my part I have been made aware of a potential vulnerability. The notification was automatic and totally non-obtrusive. I own several Dell laptops so the fact that the message included specific tag number was a bonus. If I want to install the file, I click the imbedded link and it takes me straight to the download page. Par excellence!

There are some negative issues with "push" systems like this. Some use a service that runs in memory or in the task bar. I do not like this since I already have too much there already and am concerned about performance. Also, I like to control when my PC contacts the "mother ship" and when updates are installed. The thought of this entire process going on behind the scenes without my knowledge kind of scares me a little. Downloading updates and installing manually may result in less risk than total auto-pilot.

cNet Download.com newsletter
At one time, cNet had a nice update site called catchUP. It would scan your PC for software patches and updates (similar to Microsoft Windows Update). The nice thing was that it worked with many non-Microsoft products. I guess it took a lot of time and effort to maintain so they discontinued the service. I wish they hadn't.

Alternatively, cNet has a new site download.com (http://www.download.com/). There is a "What's New" section showing upgrades and new versions of popular PC software. Visiting this page on a regular basis can be useful to keep updated on new releases. If you prefer the push (as I do) sign up for the e-mail newsletter.

User Management and Passwords

I suggest that you require unique user IDs and passwords. This requires all home users be accountable and allows for traceability. Assure that users are using strong passwords. See above for rules for strong passwords. Another good practice is to change the Administrator account name to something unique (e.g., Operator). Review all accounts on a regular basis and look for things like unrecognized user names, passwords that never expire, or other things that appear unusual. If you are really innovative, you can use policy services to force a local password policy.

Physical Security

SANS defines physical security as "The practice of providing protection to IT people, processes, and tools through the implementation of tangible controls". [12] In the SOHO context it includes the following considerations:

- Component placement and connection
- Power considerations
- HVAC and environmental
- Peripherals
- Safety

Generally, an office or other secure area inside the home will provide adequate physical controls. Assure that the area has appropriate cooling and ventilation, AC power, and structural integrity.

Power and Back-UPS
An important element of physical security is protection from AC power problems. Electrical protection is often forgotten about until something happens, like a spike during a thunderstorm and it's too late.

A simple and effective power strip that includes surge protection can go a long way. Be sure that the PC and network equipment are plugged into this strip and are protected. An option would be to invest in a UPS system with battery back-up. This would be important especially if you have servers that need time to shutdown.

I use and recommend APC products. They are inexpensive and reliable. Here is a link to a cool interactive product selector:

http://www.apcc.com/template/size/apc/index.cfm?action=single_workstation&temp_country=US&device_type=workstation

Back doors, PC Anywhere etc…

Many PC users transitioning from dial to broadband seem to forget about the old trusty modem. They do a relatively good job of "locking up the front door" with firewalls, but they sometimes let the "backdoor" wide open. Don't fall into the trap of not securing the dial-up connection….

PC Anywhere
The use of Symantec's PC Anywhere or other similar RAS solutions allows placing the PC modem in an auto-answer state. This is useful for example in a situation where a home user dials into an office PC to access their files and the corporate network.

This is neither good for the Corporate LAN or the SOHO. Even if it is not activated, or is password protected, it represents great risk. There may be a hidden script, left by the owner or by an attacker that inadvertently puts the modem into answer mode. I recommend that you uninstall any RAS packages and disconnect the telephone line until you really need it. Air is the best firewall!

Scurrying RATs (Remote Access Trojans)
I recently read about RATs, or malicious programs that run invisibly on host PCs and permit an intruder remote access and control. Evidence of a RAT might be strange symptoms including slow performance, events like a CD-ROM tray opening seemingly at random, odd error messages, etc. Types include Cult of the Dead Cow's Back Orifice and The Thing.

Some RATs mimic the functionality of legitimate RAS programs such as pcAnywhere, but work with stealth installation and operation. Hackers can hide RATs in a game or other program that unsuspecting users download and execute. Alternatively, they could be delivered via a malicious e-mail attachment.

"RATs can gathered confidential information from the hard drive and can be more dangerous than all other types of malicious code." [13]

Configuration Management - WinPatrol

A good way to assure that a PC has not been tampered with is to implement some form of configuration management. This also provides for quicker problem resolution and lower times to restore service if a problem does occur.

WinPatrol is a nice utility that does this and a lot more for you. See http://www.winpatrol.com/

Scotty the watchdog quietly sits in the taskbar and will pop-up and bark if he sees anything unusual. PCWorld magazine writes "Don't you hate it when you press Ctrl-Alt-Delete and find there are a dozen mystery programs running that you didn't even know about? WinPatrol gives you greater control over just what and what does not get permission to run on your machine… You'll also be alerted when new cookies are added to your system, and see what information is being stored there …" [14]

Windows Messenger Service

By default, Windows operating systems come with the Windows Messenger Service (WMS) enabled. This service allows someone on the Internet to pop up Windows on your PC. They do not need to know anything about your computer and it is typically not stopped by firewalls or other security devices. It's actually a feature of Windows.

WMS is commonly misused by advertisers to deliver pop-up "spam" that promotes their product or service. The messages have "Messenger Service" in the Window title. Mostly, they are just irritating; however, more dangerous is a message that uses social engineering techniques to get an unsuspecting user to install rouge software on their PC.

For example, a recent pop-up exclaims, "Spyware detected on your computer – Click here to clean." If you click, it actually **installs** the SpyWare rather than removing it!!!!! Even the savviest user could fall prey to this scheme.

WMS experienced more bad press in the fall of 2003, when it was disclosed that it contained a flaw which allowed a hacker to take control of a vulnerable Windows system. Microsoft has since issued a patch fix however this is another black mark against a relatively useless service.

Late in 2003, some large services such as AOL took unprecedented action to kill off the Windows Messenger service for subscribers. Microsoft also began disabling WMS and activating Internet Connection Firewall (ICF) by default on XP (SP2), in a move to better shield Windows PCs against hostile attacks.

The thing to take home here is - Disable it!!! A quick and easy way to disable the WMS service is called “Shoot the Messenger”. It can be found at:

http://www.pcworld.com/downloads/file_description/0,fid,23016,00.asp

Peer-to-Peer Network Dangers

Roughly 35 million American adults download music, according to Pew Internet & American Life Project surveys, and about 21% of all current American Internet users, say they allow others to download files, like audio or video files from their computers.

Using popular Peer-to-Peer (P2P) network clients like Kazza, Grokster and Limewire that can be obtained free on popular Internet Web sites, users can share and download MP3 files of most popular music and share them with other Internet users. This practice has become quite popular with teens looking for free tunes.

The Recording Industry Association of America (RIAA) recently delivered copyright infringement lawsuits to individuals who download and share copyrighted music. Under the Digital Millennium Copyright Act (DCMA), Internet Service Providers (ISPs) were subpoenaed and had to provide information about users whose accounts were found to download copyrighted music.

Using these P2P networks to share copyrighted material is illegal and could compromise the security of your computer and privacy. There is also the risk of loss, integrity, or disclosure of personal information by allowing others to access to your hard drive. And if that’s not enough risk, read on…

Trojans and Sleepers

Another Internet danger is the stealth installation of malware that goes unnoticed and silently sleeps on a user PC, only to be awakened at some future time, possibly in an organized effort such as a distributed denial of service attack. The client PC becomes a zombie or reflector against a target of the hacker’s choosing.

In April, 2003, Kazaa confirmed that they had been bundling with their software code from a company called Brilliant Digital Entertainment. The intent of this software is still debated, but the fact that it was installed unknowingly on literally millions of PCs illustrates the real and present danger, and potential for misuse in this type of attack vector.

Sharman Networks, who owns Kazaa published a statement saying that “Nothing has been downloaded which breaches Sharman's or industry standards of users' privacy protection,” and that they had acted “much the same way that major software publishers such as AOL, Microsoft, and Real Networks (do to) deploy components for future functions. “ [15]

SpyWare and AdWare

Definitions of spyware and adware vary, but it's generally thought of as software installed on a PC (usually without notice or permission) that monitors the user's browser or collects useful personal information. This data is transmitted and used by the marketer to learn more about the user in order to perhaps target them using a technique called “one-to-one marketing”.

There are many ways spyware or Adware can be introduced on to a computer. Sometimes freeware or shareware programs commonly available on the Internet contain hidden installation steps to silently install bundled Spyware during in the program install. This is common with P2P file-sharing and MP3 programs such as Kazaa, and LimeWire.

Spyware can also be introduced by parasites that exploit Internet Explorer's ActiveX controls. This allows the unscrupulous website operator to automatically install Spyware on your machine without your knowledge just by visiting that website. Additionally, there are bugs Internet Explorer and Windows if left un-patched could allow Spyware parasites to get on your machine without your knowledge.

What can be done about Spyware
I have installed one of the popular programs called Spybot – Search and Destroy. It can be found at:

http://www.safer-networking.org/index.php?page=home

America Online plans to introduce anti-spyware software using Spybot for subscribers as part of an optional service upgrade.

> "It's going to help members identify, remove and protect their PCs from surveillance and advertising spyware," said Bentley, who declined to comment further on how the software will work.
>
> “AOL's addition of anti-spyware software is significant, because it signals a mainstream awareness of the mounting threat spyware poses to Web surfers and corporations. In the last three years, the number of spyware programs circulating on the Net has shot up 13-fold, according to security software company PestPatrol. More dangerous is "remote surveillance" software, which disguises itself on a computer and reports back to whoever installed it every keystroke made on that PC.

Most spyware protection software, such as Spybot Search & Destroy, is designed to help Web surfers detect and uninstall all variations of the software from their PCs. According to AOL's Bentley, AOL's spyware protection will likely do the same. More importantly, it will give AOL's roughly 25 million Internet subscribers a free service to root out such programs at the ISP level." [16]

Virus Scanning

Another critical component to assure the security and operability of any SOHO connected PC is to install a good virus scanning and prevention package and regularly update for computer viruses.

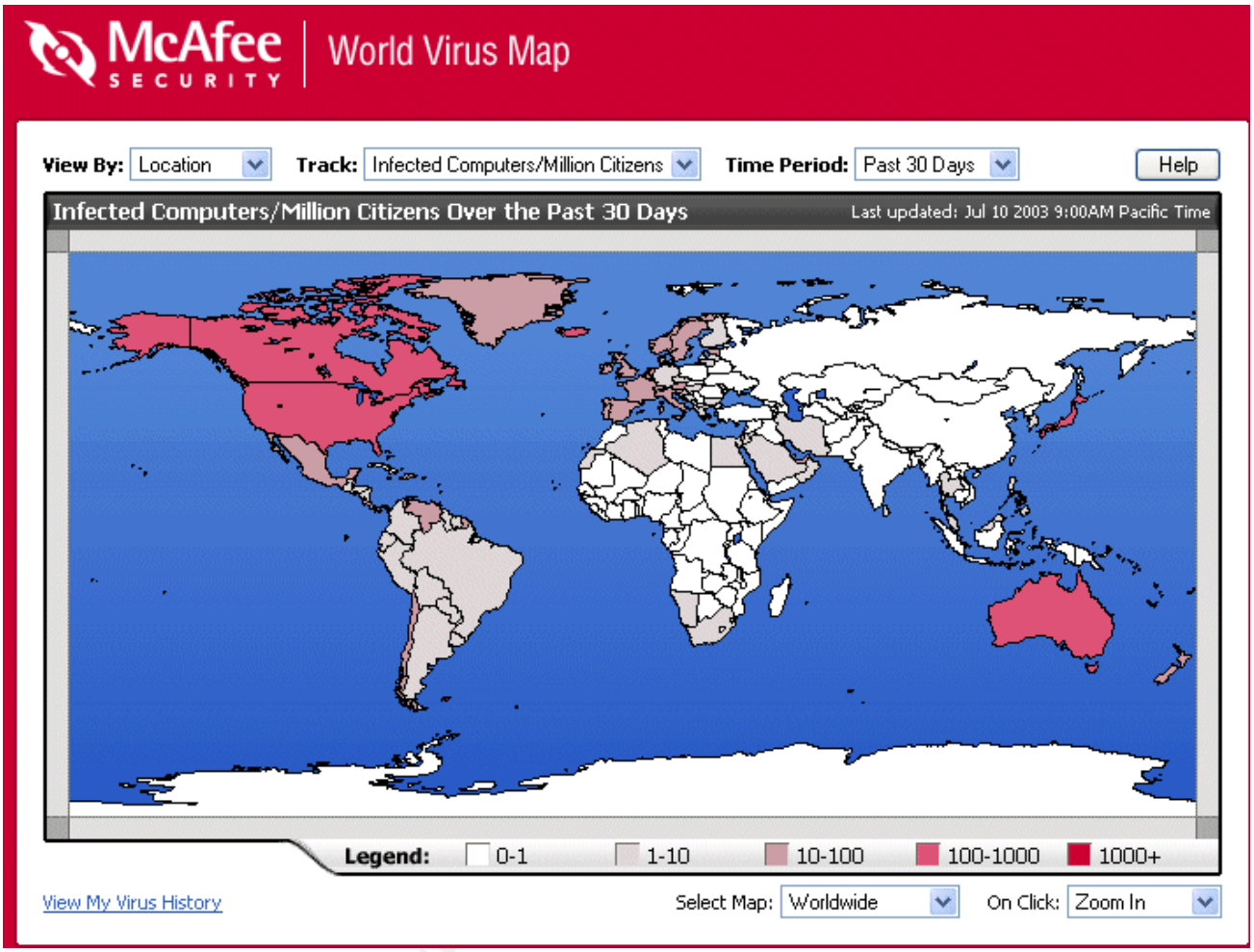
My experience is primarily with McAfee, since that is what I use on my own SOHO network. Right around the holidays I upgraded to the latest version, McAfee VirusScan 2004 (version 8.0). On top of the typical scanning and virus identification, it offers the following advanced features:

- **Email and Instant Message Attachments Scanning**
- **Script and Worm Stopper**
- **ActiveShield (real time protection)**
- **Spyware and Adware Detection**
- **Windows Explorer and MS Outlook Integration**
- **Silent Updating**
- **Ability to Submit Files to AVERT**

There are two particularly notable new features:

- **Virus Map & Information Library -** Users can see how the latest threats are infecting computers worldwide, and then research them via direct links to the McAfee Virus Information Library (see below)..
- **Visual Trace -** According to Sam Curry, McAfee.com security architect, "Visual Trace is a traceroute application that allows users to discover information about Web sites, networks, and the routes their computers take to connect to other computers on the Internet. By integrating it with the…Personal Firewall a user will be able to run traces when the firewall sends an alert that attempts are being made to connect to their computer" "Running such a trace will enable users to receive information about who is trying to connect and their network connection and then report that data to law enforcement or to McAfee.com's shared database" [17]

Here is the McAfee Virus Map:



Regardless of the vendor chosen, the most important thing in my mind is to STAY UP TO DATE! Make sure you regularly install new virus definition files, especially when threats of new viruses are in the news.

Personal Firewalls

The addition of a PC based firewall is an excellent and inexpensive measure for adding an additional layer of security to a networked home PC. In contrast to traditional hardware firewalls, or firewall functionality built into network routers discussed previously, the PC firewall does not stop intrusion into the network, rather constructs an additional barrier on each PC. You can think of it loosely as protecting the PC at the network interface level.

Several PC based firewalls are available as freeware and as commercial products. If you have upgraded to Windows XP, you have a PC based firewall included, but you may not have enabled it.

Microsoft Windows XP now comes with a built-in firewall: the Internet Connection Firewall (ICF). Although it is relative light-weight and lacks some of the features of other products (e.g., it does not handle outbound connections), it is useful for hiding the PC from the Internet – and it's FREE. You will likely want to invest in a good third-party personal firewall anyway. [18]

If you have a company laptop, check with your company administrator, Intranet or Help Desk. Chances are there will be a corporate license and standards for use a PC firewall. It may even be a required item. The corporate firewall policy might also apply to employee owned home PC systems that are used to connect to a corporate network. An unprotected PC system using dial-up or VPN tunneling into a corporate LAN could become vulnerability if hijacked or used as a jumping off point for intruders. For this reason, companies are now establishing requirements that extend to these devices.

The company I work for provides several alternative PC firewalls, including ISS Black Ice, and ZoneAlarm PRO. I also use the McAfee firewall at home. It was purchased as a bundle with VirusScan. It was a good deal at Costco ☺.

PC Internet Security Suites – Not so sweet?
For my money, having one integrated anti-virus, firewall, and anti-SPAM package is easier to operate and maintain and is a good value. Others may not agree…

I recently read a review on ZDNet that compared the two leading suites, McAfee and Norton, and the author "could not endorse either without some serious qualifications." The main downside cited with McAfee was poor SPAM filtering, and with Norton it was the performance "drag" and deficient privacy controls. Both products were said to "fail when it comes to technical support policies" in that it was free support was not offered without paying a fee ($30 -$40). [19]

Browser security

This section discusses the security features provided by the major web browsers, IE and Netscape. Some suggestions are provided that offer a higher level of protection and security…

Digital certificates and 128 bit SSL encryption
128-bit encryption is the most secure of protection generally available for Internet communications. Most banks and online finance sites require the use of 128-bit encryption (rather than the older 40-bit), including credit cards and financial transactions. If you are not using Internet Explorer 5.5 or above you should upgrade to gain the high encryption support.

The main difference in the encryption schemes is in the key length and thus the ability to crack the encryption. 128-bit encryption provides a significantly greater amount of cryptographic protection than 40-bit encryption. The longer the key the more difficult to break the encryption.

> According the Netscape, "Digital certificates encrypt data using Secure Sockets Layer (SSL) technology, the industry-standard method for protecting web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on their SSL capabilities. Their latest browsers, including Netscape Communicator 4.0 and up include the ability to encrypt transactions in 128-bit sessions. Netscape licensed the RSA public key cryptography from RSA Data Security Inc. for use in its products, specifically for authentication." [20]

"Public key encryption (PKI) is a technique that uses a pair of asymmetric keys for encryption and decryption. Each pair of keys consists of a public key and a private key. The public key is made public by distributing it widely. The private key is never distributed; it is always kept secret." [21]

"Data that is encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. This asymmetry is the property that makes public key cryptography so useful." [22]

Encrypting File Systems

In order to hide sensitive data from others and protect your computer and increase Internet privacy, you may want to deploy an Encrypted File System. This is an example of implementing a data defense. EFS is supported in Windows 2000 and newer (but unfortunately Windows XP Home edition does not include it). You must be running the latest Windows file system NTFS. If your hard disks are still FAT, you can convert them without reformatting using the Microsoft Convert utility.

With EFS, data is encrypted and stored directly on the disk at the file system level using a PKI based integrated service. In order to access the data, a user with the private key for the file will be able to conveniently access, read and write to the file as a normal document. A user without the proper credentials will be denied access.

There are several ways to encrypt NTFS file systems, supporting encryption of individual files, but the most convenient implementation is by directory.

EFS uses symmetric (one key is used to encrypt the files) and asymmetric (two keys are used to protect the encryption key) cryptography. File encryption uses the symmetric key, which is then encrypted with the public key of a public key encryption pair. The key pair is bound to a user identity and made available to the user who has the appropriate user ID and password. The default North American encryption methodology is DESX, which provides a 128-bit key. [23]

Fully removing files - CyberScrub

As we all know, when a file is deleted the actual data is not removed from the media. Rather the file name and location is removed from the disk index so that it can no longer be located. It is quite easy to recover the data using commonly available un-delete utilities such as Norton, OnTrack and others. .

If you work with sensitive data and need to fully erase files and folders, I recommend you look into using a complete file deletion utility. This is also a smart thing to do if you dispose of, sell or donate a PC. On such method for fully "wiping" data is called CyberScrub. CyberScrub is a security application designed to completely eliminate sensitive data from the drive and protect your privacy. It can be found at:

https://buy.cyberscrub.com/pitch.php?ReferrerId=278

Common Windows tweaks

Several articles can be found on the Internet on how to tweak various Windows TCP/IP defaults, particularly in the Registry (e.g., MTU, TCP window, etc.). If you are not comfortable mucking with the Registry, there are also some automated ways to do this. Dr. TCP, available at Broadband Reports is a good tweak utility. It can be found at:

http://www.dslreports.com/drtcp

Speedguide.net also has a great utility called TCP Optimizer to automate learning and setting these parameters based upon your connection.

http://www.speedguide.net/downloads.php

TCP Maximum Transmission Unit (MTU):
MTU is the largest amount of data that can be transferred in one IP frame on a network. If a packet is sent that has a smaller MTU than the packet's frame length, fragmentation may occur. MTU can range from 68 to 1500 bytes, and larger MTUs generally provide lower overhead (fewer headers). The idea is that generally, larger packets have less overhead and thus will increase performance. But be careful with this, especially if you are using VPNs.

TCP Receive Window Size (RWIN):
RWIN is the TCP Receive Window. TCP/IP transfers packets in "streams" rather than one at a time. RWIN is a setting that adjusts the buffer for storing incoming packets. TCP transfers include acknowledgement packets (acks) that notify the sender that the data was received by the far end. By increasing RWIN you are increasing the allowable "window" between acks. If the data transfer is running relative error free, larger RWIN sizes will be more efficient and provide better throughput.

The TCP Receive Window default value is about 8K bytes (Windows 95/98/NT), or about 16K bytes (Windows Me/2000/XP). Increasing the TCP Receive Window to between 32 and 64K may improve throughput on high-speed broadband connections with greater latency (e.g., the Internet). "A well tuned RWIN can…greatly improve transfer speeds by increasing data transfer efficiency." [24]

Download Accelerator Plus (DAP)

DAP is a download acceleration package I use for downloading daily syslog data from an FTP server. DAP is fully integrated into the windows browser. It is purported to "speed up your downloads by up to 300% (according to users and websites reviews)".

DAP's main advantages are in the ability to accelerate file transfers using FTP and HTTP, the capability to pause and resume downloads (recovery for dropped connections), and the ability to simplify the process of repetitive downloads. It does acceleration by implementing "multi-connection downloading". According to DAP "…the file is downloaded in several segments through multiple connections and reassembled at the user's PC. This results in better utilization of the user's available bandwidth." DAP can be used with dial-up, cable, DSL, etc. Another nice feature of DAP is that it executes a proximity check to see if there are possible mirror sites available that are more responsive relative to your location. DAP is available at:

http://www.speedbit.com/DAP7/FAQ.asp?V=5.3.9.7

Testing Broadband Performance and Security

When considering and testing various ISPs and Internet access options such as cable modem, DSL, and ISDN, it is desirable to have a way to objectively verify and compare network bandwidth and response times. This also helps to assure that you're getting what you're paying for in. Additionally, if you are installing or upgrading equipment or are making changes or tweaks it is nice to have a better idea of how they actually affect performance. These tests also demonstrate that your security countermeasures are properly established and are effective.

The most comprehensive site I've found is Broadbandreports.com, at http://www.dslreports.com/stest

This site contains lots of information and forums about selecting and using Broadband, including a great security link (on the left side of the page) and a security forum discussing security elements.

Simple Speed Testing
A quick and dirty "speedometer" test provided by McAfee is located at:
http://us.mcafee.com/root/speedometer.asp

This link can come in handy for a quick check of Internet performance. Suggest you click on the "bookmark" link.

Vulnerability testing
I came across ShieldsUP on the Internet.
http://grc.com/x/ne.dll?rh1dkyd2

This is a VERY good site not only from the standpoint of providing comprehensive FREE vulnerability testing from the Internet, but it also provides a detailed explanation of each test and result, including the risk factors and remediation.

Here is a sample report:

This textual summary may be printed, or marked and copied for subsequent pasting into any other application:

```
-------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2004-03-15 at 17:16:50

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                            119, 135, 139, 143, 389, 443, 445,
                            1002, 1024-1030, 1720, 5000

    0 Ports Open
    0 Ports Closed
   26 Ports Stealth
--------------------
   26 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED - ALL tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - NO Ping reply (ICMP Echo) was received.
```

Firewall Leak tester

There is also a link at GRC to another utility called LeakTest:
http://grc.com/lt/leaktest.htm

This one attempts to get out thru your firewall to assure you have configured it properly. It also demonstrates and tests for simple application "masquerading" vulnerability.

eMail security

Lotus Notes

In Notes “the need for a good security subsystem was evident from the start.” [25] Notes was one of the early adopters of RSA Public Key Encryption technology. “They banged on Lotus’s door and asked if there was anything we were doing that might be able to use their encryption technology. The result is that many users today may not even realize they are using certificates. They are given an ID file that has certificates in it when they start using the product… The user never even notices that they are using a complex public key technology…” [26]

Microsoft Outlook

If you use Outlook 2002 or above you are already protected from many kinds of viruses. These enhancements have come from experience with recent virus outbreaks. The latest version of Outlook:

- Blocks e-mail attachments associated with unsafe files.
- Prevents programs from accessing the address book or sending mail, thus prevent the spread of the viruses to others.
- Gives administrators an option to customize e-mail settings to meet specific security needs.
- Sets the default Internet security zone to Restricted to help protect HTML messages from viruses spread by scripting.

Outlook 2000 or Outlook 98 Users should download the Outlook Security Update to assure the latest security capabilities. [27]

Digital certificates

A digital certificate is "Attachment for a file, macro project, or e-mail message that vouches for authenticity, provides secure encryption, or supplies a verifiable signature…This signature confirms that the macro or document originated from the signer, and the signature confirms that it has not been altered." [28]

Using cryptography for more secure communications

"Cryptography is a set of standards and protocols for encoding data and messages, so that they can be stored and transmitted more securely." [29] Cryptography helps to have more secure communications, even when the transmission medium (i.e., the Internet) is untrustworthy. You can also use it to encrypt your sensitive files, so that an intruder is less likely to understand them. Cryptography can be used to help ensure data integrity as well as to maintain secrecy. Cryptography helps to verify the origin of data and messages, by using digital signatures and certificates.

Outlook 2003 uses certificates in cryptographic e-mail messaging to help provide more secure communications. To use cryptography when you send and receive e-mail messages, you first obtain a Digital ID (Contains a private key that stays on the sender's computer and a certificate (with a public key). The certificate is sent with digitally signed messages. Recipients save the certificate and use the public key to encrypt messages to the sender from a certificate authority

A Digital ID contains a private key that is stored on the sender's computer and a certificate (with a public key). Your certificate is sent when you digitally sign messages to help authenticate you to the recipient. You also use a certificate in Outlook when you encrypt messages." [30]

Summary and Conclusions

This paper covered a wide array of security methodologies to construct and improve a SOHO Network. We have discussed Defense in Depth principals and countermeasures that can be applied at differing points in the network, ranging from the edge, core, and end PC systems. Within PC systems we have covered security applications, controls and best practices. In the network space we have discussed perimeter defenses, network assessment and intrusion detection in wired and Wi-Fi networks.

Inadequate security in a SOHO could result in the loss of confidential or private information, pose data integrity issues, create network downtime or lead to malicious destruction of equipment or data due to a security breach.

The SOHO owner must be well prepared and stand ready to prevent and combat the growing potential attacks coming from the Internet. It takes good planning and effective use of security controls through the application of Defense in Depth principals to remain safe. In addition, one must remain vigilant at all times to keep informed and up-to-date on newly identified vulnerabilities and countermeasures. I hope that by reviewing this paper and taking advantage of all of the resources and tools I have covered, you are now better prepared to deal with these issues.

Good luck in your efforts to build and maintain a secure and functional SOHO network!

Footnotes and References

[1] Source : http://www.washingtonpost.com/wp-dyn/articles/A63248-2003Nov19.html Note: Taken from the Washington Post Online 3/1/04. Page no longer available at this time.

[2] Blankenhorn, Dana, "A-Clue.com", Volume V, No. VIII, http://www.a-clue.com/archive/01/cl010226.htm

[3] Blankenhorn, Dana, "A-Clue.com", Volume V, No. VIII, http://www.a-clue.com/archive/01/cl010226.htm

[4] Portions taken from US Department of Commerce, Economics and Statistics Administration, http://www.esa.doc.gov/reports.cfm

[5] Olsen, Stefanie, "AOL fights spyware in coming software upgrade", Dec. 2, 2003, http://news.com.com/2100-1038-5112843.html

[6] Fordahl, Matthew, "Comcast Limits Broadband Usage", Jan. 30, 2004 http://cbsnews.cbs.com/stories/2004/01/30/tech/main597032.shtml

[7] Adapted from Cole, Fossen, Northcutt, Pomeranz, SANS Security Essentials, ver 2.1, Vol 1, page 36

[8] McCullough, Jack, "A multilayered strategy helps neutralize internal security threats", July 1, 2002 http://techrepublic.com.com/5100-6313-1051506.html

[9] Roberts, Paul, "Source Linksys Router Flaw Reported", November 04, 2002, http://www.pcworld.com/news/article/0,aid,106632,00.asp

[10] Ploskina, Brian, "Two Companies Release NT-Based Firewalls" Dec. 9, 1998, http://www.findarticles.com/cf_dls/m0FOX/1998_Dec_9/53361418/p1/article.jhtml

[11] Curtin, Matt and Ranum, Marcus J., CERT "Internet Firewalls: Frequently Asked Questions", 12/01/2000, http://www.faqs.org/faqs/firewalls-faq/

[12] Cole, Fossen, Northcutt, Pomeranz, "SANS Security Essentials", Version 2.1, Vol 1, page 255

[13] Grimes, Roger A., "Danger: Remote Access Trojans", Sept. 2002, http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/26103/26103.html

[14] http://www.pcworld.com/downloads/file_description/0,fid,22728,00.asp

[15] Borland, John, "Kazaa exec defends sleeper software", April 3, 2002, http://news.com.com/2100-1023-875016.html

[16] Olsen, Stefanie, "AOL Fights Spyware in Coming Software Upgrade" December 2, 2003, http://news.com.com/2100-1038-5112843.html

[17] Portions from Costello, Sam, "McAfee.com Merges Visual Trace, Firewall", February 13, 2002, http://www.pcworld.com/news/article/0,aid,83863,00.asp,

[18] Microsoft, "Install a Firewall to help protect your computer", updated Nov. 24, 2003, http://www.microsoft.com/security/articles/firewall.asp

[19] Vamosi, Robert, "Why Internet security suites aren't so sweet", Dec. 1, 2003, http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5109501.html?tag=adss

[20] Netscape Network, "Secure Sockets Layer", http://wp.netscape.com/security/techbriefs/ssl.html

[21] Netscape Network, "Secure Sockets Layer", http://wp.netscape.com/security/techbriefs/ssl.html

[22] Netscape Network, "Secure Sockets Layer", http://wp.netscape.com/security/techbriefs/ssl.html

[23] Microsoft, "Encrypting File Systems for Windows 2000", posted July 1, 1999, http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp

[24] Mad_Mortis, "DSL FAQ>>2. DSL 201", http://www.dslreports.com/faq/7799

[25] Rutherford, Laura, "Notes and Domino security: Past, present, and future", http://www-10.lotus.com/ldd/today.nsf/8a6d147cf55a7fd385256658007aacf1/fe0953d746cc6b8c85256abc000c85f5?OpenDocument

[26] Rutherford, Laura, "Notes and Domino security: Past, present, and future", http://www-10.lotus.com/ldd/today.nsf/8a6d147cf55a7fd385256658007aacf1/fe0953d746cc6b8c85256abc000c85f5?OpenDocument

[27] Microsoft Office Online, “Security Features for Outlook 2002…” posted April 26, 2002, http://www.microsoft.com/office/previous/outlook/2002security.asp

[28] Microsoft Office Online, “About Digital Signatures”, http://office.microsoft.com/assistance/preview.aspx?AssetID=HP052495551033&CTT=98

[29] Microsoft Office Online, “About Digital Signatures”, http://office.microsoft.com/assistance/preview.aspx?AssetID=HP052495551033&CTT=98

[30] Microsoft, **“**About certificates and cryptographic e-mail messaging in Outlook”, http://office.microsoft.com/assistance/preview.aspx?AssetID=HP010461711033&CTT=98

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event