Global Information Assurance Certification Paper

Matthew Thiel
December 22, 2003
GSEC Practical Assignment
Version 1.4b

Vulnerabilities of running P2P software

Abstract
Ever since Napster was released in mid-1999, the use of file-sharing programs has exploded. Ordinary people now had the ability to download music, movies, and software straight to their home computers. However, there are inherent risks associated with using file-sharing (also known as peer-to-peer or P2P) software that individuals may not be aware of:

- Viruses can be distributed through P2P systems
- Adware can track a user's Internet usage
- Buffer overflows can cause a hacker to control a user's computer
- A person's IP address is made available when P2P software is used
- Lawsuits by the music industries occur when copyright songs are shared

These are potential problems that a person must accept when installing and running file-sharing software. Corporations are also vulnerable to risks if P2P software is installed, even if they have network security practices and only one computer contains the file-sharing software. Fortunately, there are methods individuals or companies can implement to lower the risks involved with using file-sharing software. This paper will explore the risks involved with using P2P software, along with means to alleviate these risks.

An Introduction to the Risks

In late 2002, the Aspen, Colorado, municipal computer network was hacked by a Canadian man.[1] (http://www.sans.org/newsletters/newsbites/vol4_37.php) This individual was able to bypass the system firewall and even gain access to the network administrator's entire hard drive. This man was not a malicious hacker, nor was he intending to gain access to the network. In reality, the network administrator had simply installed a piece of software the previous day which inadvertently allowed access to his hard drive. It was a piece of software that millions of people have downloaded and installed on their home computers. The network was hacked because of file-sharing software that was running on the network. The network administrator had placed the KaZaa file-sharing software on his computer the day before the intrusion.

The Aspen case illustrates a serious problem: what information is readily available to other people on the Internet when file-sharing software is used?

A computer is vulnerable of being hacked anytime it is connected to the Internet, and an even greater risk exists when file-sharing software is running. Companies can share sensitive or private information with the outside world and not even realize it. Corporations also can accidentally get infected with viruses when downloading files from complete strangers.
Of course, businesses are not the only entities at risk. Individual people are more likely to download and use file-sharing software to download movies, music, and software.

Before P2P
Although trading copyrighted material was made popular due to the advent of the Napster music-swapping network in 1999, for years people used FTP, the primary source of transferring files from one computer to another across the Internet. FTP, short for File Transfer Protocol, was created long before the World Wide Web was even conceived.
In order for people to trade music files via FTP, people must know a specific IP or domain address, along with a port number, to connect to an FTP server (usually servers with MP3 files loaded on personal computers). This information, along with a username and password, is often posted by the server owner in chat rooms or message boards. The user uses an FTP program to connect to the server (assuming all the user slots are not full; otherwise, the user cannot connect), where he or she can download music files or receive additional instructions on how to download the files. Frequently this means uploading music data before being able to download, or registering for free accounts on other web sites; both methods end up being beneficial to the FTP owner (either by new music files or money from the web site).
Of course, FTP sites go down all the time, and when a person finally gains access to an FTP site, he or she may discover that the server contains none of the music he or she is looking for. These reasons, along with the above tedious process of gaining access to an FTP site, enabled Napster to become such a success when it was first introduced. A non-technical person is not going to spend several minutes going through multiple steps to gain access to one person's music collection, when one simply can open up a single program and search hundreds of thousands of users' music collections.
After Napster took cyberspace by storm, many other file-sharing programs burst upon the scene (such as KaZaa, Gnutella, eDonkey, and Xolox). Most of these allowed people to search and download any type of file, not just music files. Software, movies, television episodes, or text files could be downloaded by anyone with an Internet connection. The ordinary person now had the power to get nearly anything he or she wanted on these networks.

What is P2P?
A P2P network is defined as "a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives" [2] (http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html).

Special software must be installed and run in order to connect to the networks. File-sharing software can be downloaded free from the programs' official Web sites; these programs are reviewed on Zero Paid [3] (http://zeropaid.com), which also provides news regarding the file-sharing community. There are several different file-sharing networks in operation today, such as KaZaa, eDonkey and BitTorrent. These networks are not compatible with each other; people who use the KaZaa network cannot connect to people who use eDonkey. Each network requires its own software program to connect to other users and share files, although some networks can be accessed by more than one program (the eDonkey network can be accessed by eMule and mldonkey, as well as the original eDonkey software).

Some file-sharing programs require connection to a server in order to link with other users (Napster, eDonkey); some programs do not (Overnet). Most programs use a computer's local ports to connect to other users; since most ports are automatically blocked by firewalls, these ports must be opened, or forwarded, in the firewall's settings.

A person can search for files to download by using the search function within the program or by using Web sites which list file releases for specific P2P networks (For example, Sharereactor [4] (http://sharereactor.com) lists files shared on the eDonkey network). A person can search for (and share) any type of file, but the types of files most likely to get results are music, movies, and software. The rarer the file, the less likely a person will be able to download it.

When a person chooses to download a file, the P2P software connects to other people who already have the file and requests to download it. Someone with the file will upload the file to the person making the request to download. If the person who has the file is already uploading his or her files to other users on the network, the person who requested the file will be placed in a queue. A person can be in a queue for minutes or hours. If many people (the number could be in the hundreds or thousands) have a file, the chances of a person receiving the file are much greater because traditionally, more sources means shorter queue times.

Most P2P networks share all types of files, but some networks are more suited to certain types. KaZaa is ideal for music files, but not for large files such as software, movies, or TV episodes. While KaZaa provides faster downloads than eMule, the KaZaa network has a reputation for sharing corrupt files (error-filled files; corrupt music files contain audio blips or other noticeable sound flaws) or fakes (files with the same name and size as desired software or movies, but contain no information. Fakes are released by the software and film industry to deter people from using P2P networks).

I like to use the eMule software when downloading because the files are guaranteed not to be corrupted when downloading due to eMule's error-correction feature. Also, I can use Web sites such as Sharereactor to look for releases so I am certain the files will not be fake. I occasionally use KaZaa when looking for small files (MP3 or fonts) that I would like to obtain quickly.

As stated before, computer neophytes helped make Napster a sensation. These people are unlikely to know the dangers of connecting a computer to the outside

world, with the possible exception of viruses, and the risks are increased when file-sharing software is used. These people must be educated on these risks and take steps to protect their computers while using file-sharing software.

Viruses

Viruses are one of the more well-known hazards of computing. Most Internet users are aware of the existence of viruses, and virus detection software is among the best-selling software packages. However, many people still are not fully aware of the risks of viruses and do not know how to defend against them with the purchase (or upgrading) of antivirus software.

Users are more at risk of virus infection if file-sharing software is used to download files. According to William Couch, laymen are less likely to check their downloads for viruses than people who are knowledgeable with computers [5] (http://www.sans.org/rr/papers/index.php?id=510). Novice computer users may inadvertently share files infected with viruses on file-sharing networks; they can download the infected file and either infect their own computer or spread the infected file to others.

While users can also download infected files from web servers or have infected files sent to them through email, they are less likely to be infected this way than through file-sharing networks. Web servers are checked for viruses regularly (because most web servers are owned by companies or experienced computer users), and most virus detection software will check and repair incoming and outgoing email messages, including any attachments.

Some users have created worms that are specifically to be spread on file-sharing networks. For example, the KWBot worm changes its own filename so it has the same name as popular movies or applications that are desirable to sharers, so it will be spread throughout the network [6] (http://zdnet.com.com/2100-1105-942033.html). The worm makes copies of itself and alters the Windows registry so it will run every time Windows boots, and attackers can gain access to the machine via commands through IRC.

Adware

Even though many file-sharing software is created by individuals with no intent on generating income, most file-sharing software is released by commercial, for-profit corporations. Napster was created by Shawn Fanning as an easy way to share MP3 files to and "create a music community" [7] (http://zdnet.com.com/2100-11-502047.html?legacy=zdnn), but in mid-2001 Napster.com was receiving advertising revenue from companies such as State Farm and Allstate [8] (http://news.com.com/2100-1023-246339.html?legacy=cnet).

Current P2P companies have survived by selling advertising to companies; however, not all ad revenue comes from banner or pop-up ads on the companies' home pages. Many file-sharing programs contain adware that tracks individual users' Internet-related activities. Adware is third-party software that is loaded onto a computer when another piece of software is downloaded and installed by a user [9] (http://news.com.com/2009-1023-885144.html). Adware runs in the background, even when the file-sharing software is not running.

Since many software packages that are available for download are free, there are companies that place adware within their software in order to generate revenue. This way, "software developers are giving advertisers direct access to people's computers" by tracking a user's Web activity which generates ads appearing in Web pages. [9] http://news.com.com/2009-1023-885144.html)
Given that many programs require a connection to the Internet to function correctly (such as file-sharing software), it is desirable for marketing companies to have their adware accompany Internet-based programs. Also more people are using DSL and cable ISPs; these users are constantly connected to the Internet whenever their computer is on. This is an additional boon to the marketing companies, because not only are people likely to use the Internet more often, the adware can send the tracking information at any time.
In many cases, the adware is installed legally. Many freeware programs' software licenses explicitly state that additional software will be placed on the user's machine. For example, KaZaa's terms of service agreement points out that Cydoor, a maker of adware software, may use the "Internet connection to update its selection of available ads and stores them on [the user's] hard drive" [10] (http://www.kazaa.com/us/help/resource_usage.htm). However, this information may be buried within hundreds or thousands of words, and a large majority of users blindly click the "Agree" button without realizing their computer is being used for marketing purposes.
Recently, software makers have shown more honesty concerning adware. KaZaa.com openly states that its free file-sharing program is "ad-supported" (KaZaa also offers an ad-free version for $29.95) [11] (http://www.kazaa.com/us/products/index.htm). Most likely this is due to the bad publicity which arose when users discovered adware installation is discussed only in the license agreements, which KaZaa knows are unread by a large portion of users [5] (http://www.sans.org/rr/papers/index.php?id=510).
Since adware is a piggy-back program which runs separately from the program it accompanies, it uses additional processing power, hard drive space, and bandwidth. For users with older computers or slow Internet connections, an additional program running in the background may noticeably slow the computer down, as well as consume a large percentage of available throughput. Adware may conflict with other programs and may cause a running program, or the operating system itself, to lock up.
If a user is running a software firewall program and adware is attempting to send data to the company server, the firewall will display a message requesting an outgoing message for the adware program. Denying incoming or outgoing connections of an adware program is one way to prevent companies from gathering information about a user (even though the program is still installed and running). This is one reason why installing a firewall on any computer connected to the Internet is a beneficial idea, even though a firewall is not a "magic bullet" solution to Internet security (this will be discussed later).
However, users may blindly choose for the firewall to allow all connections for any software attempting to connect to the Internet. Since there are many programs (which include applications integrated within the operating system) that

access the Internet, most computer users may believe that all of the programs that ask for permission to use the Internet are legitimate, even if they do not recognize the program's name. More knowledgeable users may recognize the names of famous adware (Gator, BonziBuddy, etc.) or do research on programs they do not recognize to see if they are adware. Users must be extremely careful when allowing programs to access the Internet.

Free, downloadable programs that will scan and delete these unwanted programs from a person's computer are available. Spybot Search and Destroy [12] (http://www.safer-networking.org) and Ad-Aware [13] (http://www.lavasoftusa.com) are two such programs that will seek out and delete adware files on a user's computer. Both are available free to download.

Similar to anti-virus software, people can use these programs to scan for and delete known adware programs, including advertising cookies which track people's Web surfing activities. Spybot contains an additional option to scan and delete "Usage Tracks", which contain information on any documents, web pages, or applications the user recently opened or visited (for example, the "My Recent Documents" folder in Windows XP's Start menu is emptied when this track is cleared). While this extra level of security can prevent companies from learning personal information about a user, this reduces the convenience factor.

Anti-adware programs are ineffective unless they are updated frequently with the most recent definitions. New adware programs are discovered often, and existing adware software is updated by the marketing companies on a regular basis. Commercial sites also place advertisement cookies on people's hard drives to generate revenue.

I currently have both Spybot Search and Destroy and Ad-Aware loaded on my personal computer, and I use them frequently to remove these unwanted files, including listings of previously used documents and programs. I have noticed that Spybot detects a larger number of files than Ad-Aware, but I have noticed that Ad-Aware identifies material undetected by Spybot.

The first time I scanned for adware (after nearly two years of Internet use on my machine), I discovered I had over 100 such files and programs on my computer! This fact alone illustrates the importance of scanning for adware. However, after the initial deletion of the adware files, one of my programs I purposely placed on my computer was unable to run. KaZaa kept giving me an error message stating that a file was missing, and it could not run without this file.

After some investigating online, I discovered not only is adware placed on a person's computer when KaZaa is installed, but removing those files renders KaZaa useless. Unfortunately, KaZaa is not alone in discouraging users from removing adware from their machines; many programs that originally came with adware cannot function without these marketing tools, including KaZooM MP3 KaZaa Accelerator.

The inclusion of adware with KaZaa (as with any software) is reviled by many Internet users; this is why a group of programmers were inspired to create an alternate version of KaZaa, called KaZaa Lite [14] (http://zeropaid.com/kazaalite). KaZaa Lite does not include any form of adware. It even contains a few features not included in the original program, and it is absolutely free to download.

As of December 3, 2003, the KaZaa Lite project has been shut down by Sharman Networks, KaZaa's parent company [15] (http://www.zeropaid.com/news/articles/auto/12052003h.php), Kazza Lite is no longer available on the official KaZaa Lite Web site, and no future versions of the software will be produced, but the most recent version is still available to download throughout the Internet.

Buffer Overflows

A buffer overflow is a software glitch that has been the cause of many problems for users and software developers. Software buffers are necessary for software programs to work. When a program or process attempts to store more data than the buffer can hold, the extra information is spilled into adjacent buffers, which can overwrite or even corrupt the valid data in these buffers [16] (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html). Buffer overflows exist because the C program language is used to create the software containing the vulnerabilities. Programs written in C language do not automatically check if a buffer has enough room to contain the information, allowing the extra data to cause harm to the computer. Programmers do have the power to help alleviate this problem, however. If more developers would include subroutines that checks if a buffer has enough room to contain information, a large portion of the problem could be solved. Nonetheless, this is not a perfect solution; attaching characters in a loop could cause a buffer overflow error [17] (http://www.networkmagazine.com/article/NMG20000511S0015).

Buffer overflows can be a major security issue if a malicious user wishes to take advantage of this flaw. For example, in 2000 Microsoft's Outlook and Outlook Express email clients were discovered to have buffer overflow vulnerabilities; an email message could be sent with superfluous data within the message header, which would cause the header buffer to overflow and allow the perpetrator to run any code contained within the email document [16] (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html). The user does not need to actually open the email document; the buffer overflow occurs when the message is downloaded by the email client.

Buffer overflow flaws exist in file-sharing software as well. In May 2003, the KaZaa software (version 2.02) was reported to have a buffer overflow vulnerability. Computers running KaZaa and acting as a supernode (a computer that allows other KaZaa users to upload lists of their shared directories to the supernode-enabled machine; this is meant to help other KaZaa users search for files) are vulnerable to attacks if they receive packets with more than 200 IP addresses of other supernodes [18] (http://www.kazaa.com/us/help/faq/supernodes.htm). "A remote user can send 203 entries to the target supernode to trigger the flaw and cause the supernode to crash" or execute code on the victim's computer. [19] (http://www.securitytracker.com/alerts/2003/May/1006846.html)

Users cannot protect themselves from buffer overflow attacks if their software contains this defect, but they can perform updates if they are available.

Whenever a buffer overflow flaw (or any bug) is discovered in software, developers will either offer a patch or update their software online. The user that owns the software can freely download the updated software or patch to correct the security hole. However, this requires the user to take the time to update the software, and when a developer announces that their software contains a security hole, malicious users may take advantage of this error and attempt to wreak havoc on unprotected systems.
Personally, I have not experienced buffer overflow attacks. I check for updates often for all of my software programs, including operating system fixes. When they are available, I download and install them on my machine. I believe that my example validates the need for updated software.

IP Disclosure
In January 2000, when Napster was still the king of P2P software, an Internet security consultant discovered a major security problem: in addition to allowing other Napster users to view the contents of their shared music directories, the software broadcasts the IP address of the machine to the outside world. [20] (http://news.com.com/2100-1023_3-236132.html)
This can be devastating to users with static (fixed) IP addresses. It is much easier for a hacker or an organization to find a particular user if his or her IP address never changes. Even if the user has a dynamic IP which changes each time the computer connects to the Internet, the IP can identify which Internet Provider is being used and possibly narrow the geographic location to a specific area if the ISP is small enough.
Most other file-sharing problems contain this same drawback. Fortunately, newer file-sharing programs such as Filetopia use encryption algorithms to "hide" the IP address and provide additional protection for the user. [5] (http://www.sans.org/rr/papers/index.php?id=510)

Legal Risks
For years the recording RIAA (the Recording Industry Association of America) has been in uproar over people downloading pirated material. If people can download near-perfect copies of music for free, why should people spend money to purchase CDs?
Conversely, the public has complained about the RIAA's business practices. People have stated they are tired of paying for a CD that costs the same as a DVD and only has one or two desirable songs. They are also complaining that the artists only get a small portion of each CD sale and that distributing songs on the Internet actually gives more exposure to small groups. Music-sharers also argue that people who download music are more likely to purchase the CD legally if they like the songs, thereby supporting the artist.
In 2000, Metallica, a band opposed to music-sharing, identified more than 335,000 users who were sharing the heavy metal band's songs on the Napster network in a lawsuit against the music-swapping service [21] (http://news.com.com/2100-1023-239956.html?legacy=cnet). That May, Napster had officially banned those users from the network [22] (http://news.com.com/2100-

1023-240331.html?legacy=cnet&dtn.head). These banned users were greeted with a shocking message when they attempted to log on; they were being prohibited from the network and could no longer share any songs.
However, some users complained that they were falsely identified as Metallica pirates, and many of them (about 17,000) filed an official appeal with the band. This helped spur the decision to allow banned Napster users to be reinstated, but only if they submit an electronic counter-notification asserting that they have not traded any copyrighted music [23] (http://news.com.com/2100-1023-240611.html?legacy=cnet). Naturally, these users are at risk of being sued if they were, in fact, distributing illegally obtained songs or begin to pirate music after signing.
Some users have tried to get back on the network without signing the agreement. Re-registering with a different user name could not get around the ban. Removing and reinstalling the Napster software resulted in the same outcome [24] (http://zdnet.com.com/2100-11-520673.html?legacy=zdnn).
How was this ban accomplished? When users who had banned usernames logged on to the network, they received a message that a new version of Napster (Version 2, Beta 6) would be installed on their computer. Since automatic upgrades of software are commonplace, even in early 2000, this did not seem unusual to users. However, what was unusual was after this particular upgrade many Napster users were unable to use the network. The new version of Napster had inserted registry keys that identified the computer itself as a "banned" computer [24] (http://zdnet.com.com/2100-11-520673.html?legacy=zdnn).
Some users discovered ways to get back onto Napster without signing the agreement and posted these techniques on the Internet [24] (http://zdnet.com.com/2100-11-520673.html?legacy=zdnn). One posted method was to reinstall the Beta 5 version and register under a different name, and another was to remove the registry entries identifying banned user as "banned", either by removing them manually or running a batch program.
The RIAA has used its corporate muscle to close down the free Napster service in 2001 (Napster re-opened as a legitimate pay-for-music service on October 29, 2003), as well as the popular AudioGalaxy music-sharing service [25] (http://www.epidemic.ws/song-swapping/EN/A%20song-swapping%20timeline.html). This has not stopped music downloaders from sharing; however, in June 2003 the RIAA made an announcement that sent a shockwave throughout cyberspace: the organization would crack down on individual people who share illegal MP3 files [26] (http://www.techtv.com/news/culture/story/0,24195,3480861,00.html).
Since the ultimatum, the RIAA has sued hundreds of file-sharers for $150,000 per song shared, but they have settled out of court with many clients for a relatively small amount, usually a few thousand dollars per client [27] (http://news.com.com/2100-1023-5072564.html?tag=nl).

Preventive Maintenance

There are ways a person can use file-sharing software and eliminate (or reduce) the possibility of being sued. Removing any commercially available file from the

shared directory once the file is downloaded is considered the best option [28] (http://www.eff.org/IP/P2P/howto-notgetsued.php). Another option is to disable the uploading of files in the shared directory. Both options will hurt the network, but the music industry is far more likely to sue people if they upload pirated material to others. The feature to disable uploading is available to KaZaa, Morpheus, and Gnutella users, but eDonkey and eMule users must upload to download material.

Disabling other network users from viewing a person's shared directory (including unfinished files) is another way a person can protect himself or herself [28] (http://www.eff.org/IP/P2P/howto-notgetsued.php). However, that person is unlikely to be contacted by other network users with the same tastes in media. Also, people may configure their clients not to upload to people who have disabled the uploading feature, so this may limit the availability of downloadable sources.

Not every file available from file-sharing networks is illegal. Many small bands freely post MP3 files of their music online. Individuals have created audio, video, and software meant to be downloaded by others freely. Many television shows and some movies are not commercially available (and have not been aired on television for years), but some people have taken old recordings and put them online.

The Digital Archive Project [29] (http://dapcentral.org) specializes in the release of television shows that are currently not available commercially on video, despite loyal audiences, such as "SCTV" and "The Tick". If a show (or specific episodes) is announced to have a future home video release, then the group removes the episode(s) from distribution.

Protection Through Firewalls

An individual can use a firewall to protect his or her computer when connected to the Internet. There are numerous free firewalls to download from several companies, including ZoneAlarm [30] (http://ZoneAlarm.com) and Sygate [31] (http://Sygate.com). These companies also sell firewalls with more features than the free versions.

As stated before, installing a firewall will not completely protect users from network security risks. Computers are still vulnerable to viruses and hackers even with a firewall. Incorrectly set up firewalls can, in reality, prevent Internet applications from working correctly. For example, I had problems sending email through Outlook. At first I thought the problem was with my ISP, but in fact my firewall was preventing me from sending messages. Re-configuring my firewall by allowing Outlook to accept all incoming and outgoing connections cleared the error.

Nevertheless, firewalls are essential to network security. Firewalls automatically block a computer's ports, which can protect users from different types of attacks and block worms (such as the recent Blaster Worm) from infecting a person's computer. They can automatically alert a user if an attack is being attempted, and automatically block the attacker for a period of time. Even if a hacker

bypasses the firewall and attacks a computer, a user can check the security logs to identify the IP address of the attacker.

People can check their firewalls' effectiveness by using free scanning tools by Gibson Research Corporation [32] (http://grc.com) and Sygate [33] (http://scan.sygate.com). These scanners attempt to gain information about a person's computer, including open ports and Web browser information. If the scan was successful and private information is being sent across the Internet, the sites give advice on how to fill these security holes. People are encouraged to test the computer twice: once with the firewall(s) activated and once with no firewall protection to ensure that the installed security system is protecting the computer.

Firewalls can be configured to block specific IP addresses from being able to access a user's computer. There are Web Sites [34] (http://www.bluetack.co.uk) that list IP addresses submitted by users belonging to companies known to search people's computers for copyrighted material. A downloader can take IP addresses run by the various entertainment institutions and paste them into the block list of the firewall on the computer running the P2P software. There are two major problems with this method: many IP addresses are discovered after an individual has been scanned, and legitimate Internet sites, including Web sites and personal servers, may be within the listed IP ranges and may be blocked by the firewall.

I have personal experience blocking Web sites and friends' servers when using blocklists. When I engage in file-sharing, I use the blocklists, because I think the extra protection is worth not being able to access certain sites. When I do not run any P2P software, I de-select the blocklist from my firewall so I may continue my normal internet use.

Hardware firewalls are also available to individuals. Routers, which are used to connect multiple PCs to a single high speed Internet connection (Cable or DSL), often contain built-in firewalls. Netgear and Linksys are two such manufacturers of firewall-protected home routers, which block suspicious packets from ever reaching the PCs.

In the past, I have used both the hardware and software firewalls for extra security. I incorporated Linksys's firewall, as well as the fee-based Sygate Personal Firewall Pro firewall on my DSL-connected PC. I prefer the advanced version of Sygate's firewall because I like the extra features that come with the more advanced versions, such as the Intrusion Detection and Stealth Browsing features to block known Internet attacks and prevent Web servers from discovering my operating system and Web browser.

I have had some difficulty using P2P networks when I use both the hardware and software firewalls. I turned off my hardware firewall to find out if my connection to the file-sharing networks would be improved. After doing so, I was able to log onto the networks much quicker, and I received noticeably faster download rates. I discovered the hardware firewall was blocking the P2P software on my computer from fully connecting to the networks, despite opening the correct ports on the firewall. Currently, when I use file-sharing networks, I only use the

software firewall. When I do everything else online, I use both the hardware and software firewalls.

Corporate Use

While people are at risk for lawsuits if they share copyrighted material in their own homes, people who place P2P software on their workstations at their place of employment are at an even greater risk of trouble. Corporate productivity and bandwidth can be severely compromised if employees download music, movies, or software using P2P software.

According to a 2003 survey by AssetMetrix, file-sharing software is widespread in the corporate world. P2P software was identified on at least one computer in 77% businesses around the world [35] (http://news.com.com/2100-1027_3-1026184.html). Every company surveyed with a minimum of 500 employees had file-sharing software installed on at least one machine. Overall, one out of every ten corporate computers contains P2P software [36] (http://www.assetmetrix.com/pdf/p2prisk.pdf).

AssetMetrix has concluded that there are three major risks associated with file-sharing programs, some of which were mentioned earlier in this paper. Adware programs are being loaded onto the corporate computers along with the file-sharing programs. Virus, worms, and other dangers can be spread very easily using file-sharing software. However, potentially the most damaging risk of P2P is the availability of private information to anyone with an Internet connection [36] (http://www.assetmetrix.com/pdf/p2prisk.pdf).

A hacker can "break into" a user's computer and gain access to files if it is connected to the Internet. This is a risk that exists when using the Internet; however, this danger can be lessened if the user installs a firewall (Sygate's Personal Firewall protects local network traffic by blocking external NetBIOS packets). On the other hand, placing files in "shared" folders greatly increases the possibility that someone will access those files, and no hacking may be necessary to gain entry.

In Windows, a user has the option of "sharing" one or more folders to make them available to other computers on a local area network. One must be aware of the possible dangers of readily available files. If private information is available for anyone, even trusted employees, to view, change, or even delete, the effects can be devastating. Even if the folders are shared as "read only" (network users can only view the files), or if the folders contain sensitive data such as employee social security numbers or bank account information, a network user can cause significant damage to the owner of those numbers.

Sharing a folder in a file-sharing network can be even more dangerous. If a person on a LAN steals and uses private information maliciously, the network administrator may be able to find the perpetrator through detective work (checking the access logs), unless the perpetrator has covered his or her tracks. If a person hundreds or thousands of miles away steals and uses confidential information through P2P software, it may be very difficult to catch the criminal. With file-sharing software, many people around the world can connect to the

computer, and the firewall logs may list hundreds of IP addresses (only one of them representing the culprit) connecting through the file-sharing software. Additionally, the company itself can be held liable for damages and can be sued if copyrighted software is downloaded and shared on the Internet. For example, Integrated Information Systems (IIS) is one company that got in trouble with the RIAA with illegal MP3 files [37] (http://www.bizjournals.com/phoenix/stories/2003/08/25/story7.html). The company did not get into trouble due to an employee taking advantage of the corporate-offered bandwidth and disk space offered to download MP3s. In fact, the company was offering the music files freely to its employees [38] (http://techrepublic.com.com/5102-6264-1048032.html). The company settled for one million dollars, and now IIS is working along with Patchlink, a network security company, to remove illegal digital music files from other company's networks.

Most experts believe that the risk is too high for a company to use P2P software, even if corporate policy permits only public-domain material to be downloaded. Many experts express the need of companies creating corporate policies to prevent such programs from being installed. Security expert John McCormick suggests "setting up a company policy that prohibits users from installing peer-to-peer software on company systems due to the security risks, legal issues, bandwidth problems, and lost productivity that accompany rampant use of these programs" [38] (http://techrepublic.com.com/5102-6264-1048032.html). Some companies are using third-party companies, such as Integrated Information Systems and Patchlink, to search for and stamp out corporate P2P use.

A September 2003 TechRepublic article [39] (http://techrepublic.com.com/5100-6264-5065981.html) describes four steps that companies can take in order to stamp out corporate P2P use. I have already mentioned setting up a corporate policy banning file-sharing; however, no policy is effective unless each employee is fully aware of the consequences if any violation takes place, and that any subsequent punishments should be imposed harshly.

Other methods include having employees be made aware of lost productivity and any risk incurred by the company when using file-sharing software, and installation of software on corporate machines should only be limited to certain administrative personnel. This can be accomplished through group permissions on the network; if this is not possible, audit-performing software can check if file-sharing programs have been installed on the network or if there is illegal material on any of the computers, and who has installed these files.

Finally, TechRepublic suggests that the P2P packets should be prevented from ever entering the company at all, even if the other recommended measures are in place. Steps can be taken on the network level to program the corporate firewall to drop any incoming unauthorized packet; the corporate firewall can be configured to block any ports used by popular P2P programs. If any packets do get through, third party solutions, such as PacketShaper by Packeteer, Inc. [40] (http://www.packeteer.com/prod-sol/products/packetshaper.cfm), can control and monitor the application level of the network so these packets never reach the clients, and it can even block certain URLs from being accessed by employees.

Conclusion

The old saying, “If it sounds too good to be true, it probably is,” applies to using file-sharing software for the downloading of movies, music, and software from the Internet. Many people are so enthralled with the idea of downloading anything they want for free, they may not be aware of the dangers that exist when using these programs. A person who is unaware of the security threats when simply connecting a computer to the Internet is taking a great risk when file-sharing software is installed.

While most people have heard of viruses, too many non-savvy users do not protect their computers with updated anti-virus software. Even if they do, they may not check their computers for viruses on a regular basis and unintentionally distribute viruses across the Internet.

Adware is a relatively new threat to security. While most adware is installed legally on a person’s computer, many people may not realize their actions are being tracked, or their bandwidth and stability are being compromised while these programs are installed. There are free software solutions to dispose of adware although people must be aware these scanners must be updated and run regularly, and some software programs require adware to function.

Buffer overflows can give hackers free reign to a person’s computer. While there is not much a person can do to overcome these software errors, they must be conscious to the fact that this security hole exists. They must be aware that when a developer releases a new software version or a patch they must download and update their software.

People must be aware that they are not completely anonymous when using file-sharing software. Their IP addresses are being broadcast whenever the P2P software is used, and a hacker can use that information to damage a user’s computer.

Individuals can lessen the risks associated with using file-sharing software such as removing copyrighted material from shared folders or eliminating uploading of material altogether. However, they must be aware this may prevent them from getting files that they desire.

People can install a firewall to protect their computer from P2P risks, but they must recognize this is not a final solution to security. They can block certain IP addresses from accessing their computers, but they can inadvertently block sites they want.

People who have shared copyrighted songs have been sued by the RIAA, and Napster has banned people who have shared Metallica songs on the network. Many of the sued individuals have settled out of court, and many banned Napster users have been reinstated by signing affidavits declaring they have never shared Metallica songs.

Corporations are encouraged not to allow file-sharing in any way, due to the dangers of lawsuit and lost productivity. There are a lot of companies with file-sharing software installed, but there are companies that offer methods to erase and block the P2P software from the corporate networks, including educating employees on the risks.

Nonetheless, people must be somewhat familiar about computer security, or at least cognizant of the dangers, in order to fully appreciate the risks in using file-sharing software. These are the people who are the most likely to take the above precautions in order to protect themselves. In the case of corporations, the risk may be too great to run file-sharing software at all.

References

1. “City Employee Opens Hard Drive to KaZaa Network.” SANS Institute. September 11, 2002. URL: http://www.sans.org/newsletters/newsbites/vol4_37.php (December 22, 2003).

2. “Peer-to-Peer – a searchNetworking definition.” searchNetworking. September 24, 2003. URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html (December 22, 2003).

3. “Zeropaid.com – The File Sharing Portal.” Zeropaid, Inc. URL: http://zeropaid.com (December 22, 2003).

4. “NEWS – Sharereactor.com.” Sharereactor.com. URL: http://sharereactor.com (December 22, 2003).

5. Couch, William. “Peer-to-Peer File Sharing: Security Risks.” SANS Institute. URL: http://www.sans.org/rr/papers/index.php?id=510 (December 22, 2003).

6. Loney, Matt. “New Worm Eats into KaZaa.” ZDNET (UK). July 8, 2002. http://zdnet.com.com/2100-1105-942033.html (December 22, 2003).

7. Varanini, Giancarlo. “Q&A: Napster creator Shawn Fanning.” ZDNet Music. March 2, 2000. URL: http://zdnet.com.com/2100-11-502047.html?legacy=zdnn (December 22, 2003).

8. Jacobus, Patricia. “Napster spurs advertisers to pour money into MP3 sites.” CNET. September 28, 2000. URL: http://news.com.com/2100-1023-246339.html?legacy=cnet (December 22, 2003).

9. Borland, John and Konrad, Rachel. “PC Invaders camp out in hard drives.” CNET News.com. April 18, 2002. URL: http://news.com.com/2009-1023-885144.html (December 22, 2003).

10. “Resource Usage.” Sharman Networks. URL: http://www.kazaa.com/us/help/resource_usage.htm (December 22, 2003).

11. “KaZaa – Products”. Sharman Networks .URL: http://www.kazaa.com/us/products/index.htm (December 22, 2003).

12. “Home - The Home of Spybot-S&D!” URL: http://www.safer-networking.org (December 22, 2003).

13. “Lavasoft.” Lavasoft URL: http://www.lavasoftusa.com (December 22, 2003).

14. “Zeropaid.com – KaZaa Lite.” Zeropaid, Inc. URL: http://zeropaid.com/kazaalite (December 22, 2003).

15. “KaZaa Lite Shut Down.” Zeropaid, Inc. December 05, 2003. URL: http://www.zeropaid.com/news/articles/auto/12052003h.php (December 22, 2003).

16. “Buffer Overflow – A searchSecurity definition”. searchSecurity. September 17, 2003. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html (December 22, 2003).

17. Farrow, Rick. “Blocking Buffer Overflow Attacks.” Techweb. November 1, 1999. URL: http://www.networkmagazine.com/article/NMG20000511S0015 (December 22, 2003).

18. “Supernodes.” KaZaa.com. URL: http://www.kazaa.com/us/help/faq/supernodes.htm (December 22, 2003).

19. “FastTrack P2P (KaZaA) Buffer Overflow May Let Remote Users Execute Arbitrary Code on a Supernode.” SecurityTracker.com. May 26, 2003. http://www.securitytracker.com/alerts/2003/May/1006846.html (December 22, 2003).

20. Festa, Paul. “Security problem discovered in Napster music software.” CNET News.com. January 26, 2000. URL: http://news.com.com/2100-1023_3-236132.html (December 22, 2003).

21. Borland, John. “Metallica fingers 335,435 Napster users.” CNET News.com. May 1, 2000. URL: http://news.com.com/2100-1023-239956.html?legacy=cnet (December 22, 2003).

22. Borland, John. “Napster boots 317,377 members from service” CNET News.com. May 9, 2000. URL: http://news.com.com/2100-1023-240331.html?legacy=cnet&dtn.head (December 22, 2003).

23. Borland, John. “Napster says 30,000 Metallica fans appeal ban.” CNET News.com. May 16, 2000. URL: http://news.com.com/2100-1023-240611.html?legacy=cnet (December 22, 2003).

24. Wheeler, Marylynn. “Banned Napster users strike back.” ZDNet News. May 10, 2000. URL: http://zdnet.com.com/2100-11-520673.html?legacy=zdnn (December 22, 2003).

25. Lampo, Luna and Serina, Merina. "A song-swapping timeline." Version 1.1. URL: http://www.epidemic.ws/song-swapping/EN/A%20song-swapping%20timeline.html (December 22, 2003).

26. Martell, Lindsay and Stevenson, David "RIAA Readies Lawsuits." TechTV. July 21, 2003. URL: http://www.techtv.com/news/culture/story/0,24195,3480861,00.html (December 22, 2003).

27. Borland, John. "RIAA Sues 261 File Swappers." CNET News.com. September 8, 2003. http://news.com.com/2100-1023-5072564.html?tag=nl (December 22, 2003).

28. "How Not To Get Sued By The RIAA For File-Sharing." Electronic Frontier Foundation. URL: http://www.eff.org/IP/P2P/howto-notgetsued.php (December 22, 2003).

29. "Digital Archive Project." Digital Archive Project. URL: http://dapcentral.org (December 22, 2003).

30. "Zone Labs: Zone Labs, Internet security products, online safety, software, protection." Zone Labs, Inc. URL: http://ZoneAlarm.com (December 22, 2003)..

31. "Sygate - Enterprise Security Solutions, Personal Firewall Solutions, Professional Services." Sygate, Inc. URL: http://Sygate.com (December 22, 2003).

32. "Home of Gibson Research Corporation." Gibson Research Corporation . URL: http://grc.com (December 22, 2003).

33. Security Scan – Sygate Online Services (sos)." Sygate, Inc. URL: http://scan.sygate.com (December 22, 2003).

34. "bluetack.co.uk – home." URL: http://www.bluetack.co.uk (December 22, 2003).

35. Borland, John. "Corporate P2P use is common, study says." CNET News.com. July 26, 2003. URL: http://news.com.com/2100-1027_3-1026184.html (December 22, 2003).

36. "Corporate P2P (Peer-To-Peer Usage and Risk Analysis." AssetMetrix, Inc. July 2003. http://www.assetmetrix.com/pdf/p2prisk.pdf (December 22, 2003).

37. Kress, Adam. "IIS aims to help others avoid pitfalls of illegal MP3s" American City Business Journals, August 25, 2003, URL:

http://www.bizjournals.com/phoenix/stories/2003/08/25/story7.html (December 22, 2003).

38. McCormick, John. “Take precautions against peer-to-peer threats.” TechRepublic. April 22, 2002. URL: http://techrepublic.com.com/5102-6264-1048032.html (December 22, 2003).

39. Mullins, Michael. “Kick file-sharing apps off your network in four steps.” Techrepublic. September 3, 2003. URL: http://techrepublic.com.com/5100-6264-5065981.html (December 22, 2003).

40. “Packeteer > Products and Solutions > Products > PacketShaper.” Packeteer, Inc. http://www.packeteer.com/prod-sol/products/packetshaper.cfm (December 22, 2003).

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS