Peer-to-Peer File-Sharing Networks: Security Risks

William Couch

William Couch
GSEC Practical Assignment
Version 1.4.b

Peer-to-Peer File-Sharing Networks: Security Risks

Abstract

The popular peer-to-peer (P2P) file-sharing networks, which have appeared in the past few years, are introduced. The rise and evolution of these networks is discussed, along with some of the reasons for their popularity. Then the security implications, to users' computers, networks, and information, are examined. The status of P2P networks in business is discussed. A summary of the current state of the security risks of this technology is presented.

Peer-to-Peer (P2P) file-sharing networks have become wildly popular. The first major file-sharing network was Napster, which was designed to allow music fans to share MP3 music files.

Napster was mired in well-publicized legal proceedings concerning their responsibility to help combat the unauthorized distribution of copyrighted music. Suits filed by record companies and others resulted in injunctions forcing Napster to cease operations. Eventually, Napster signed an agreement with entertainment giant Bertelsmann AG of Germany, perhaps signaling a realization on the part of the music industry that Internet-based music and video sharing is inevitable, and that the wise course of action is to try to steer it in more copyright-friendly directions, rather than trying to eliminate it.

It is not within the scope of this paper to discuss the legal ramifications of P2P file-sharing. Driven by consumer demand, after Napster burst onto the scene, it was followed by a host of other similar services, which have extended the file-sharing past MP3 music files, to include all types of electronically transferable information, including videos, software, and virtually every other form of digital information. These services include KaZaA, Morpheus, Limeware, Grokster, Bearshare, and many others, as well as the GnutellaNet, "a loose federation of users and organizations that make a wide variety of information available to the world at large."[1] (http://content.techweb.com/encyclopedia/defineterm?term=gnutella) The numbers of users and files shared are staggering, even by Internet standards. KaZaA, as of August 30, 2002, claims "111,119,811 KaZaA Media Desktops downloaded so far... 2,497,794 downloaded last week!"[2] (http://www.kazaa.com/en/index.php) KaZaA also claims that its users share 85 million files per day.[3] (Pruitt)

Why is P2P software so popular? From the point of view of the individual, there are several reasons. There's a world of free stuff out there, just waiting to be

downloaded. It's very easy to do. The software is simple to install and configure, and searching for music, movies, or whatever is as easy as typing in a keyword and clicking "OK".

Despite its ease-of-use, P2P software is becoming increasingly sophisticated. It may search the entire network of users for the requested content, download from multiple sources simultaneously, and recover from broken connections. The user may be able to preview videos while they download. Some packages create queues for popular peer download sites and “hold” users’ places in line. Chat facilities allow P2P users to interact in real-time. Bandwidth management features allow users to limit the amount of bandwidth other users consume while uploading files. Large libraries of downloaded files can be easily managed. Many of the P2P software packages include tools for playing downloaded files and burning them onto CDs.

There are more and more ways to use the downloaded content, too. Most PCs sold today come with a CD burner standard. Compressed music formats like MP3 allow twenty hours of music to be put on a single MP3 CD. Sophisticated software allows users to build extensive multimedia libraries and create custom collections on CDs, minidisks, etc. And the types of sharable information are constantly increasing - for instance, DVD videos, originally intended to be "copy-proof", can now be turned into digital files and shared with ease.

It appears, then, that P2P file-sharing is here to stay, regardless of the evolution of copyright law and the efforts of content owners to control it.

However, there is a potentially dark side to these services, and not just due to any moral or legal concerns about sharing files. There is a very real security risk to every user who chooses to use P2P file-sharing software. This paper is an attempt to assess the current state of this security risk.

The nature of P2P file-sharing networks is, as the name implies, peer-to-peer and decentralized. There is no central server that uploads, stores and downloads content - each user (potentially) acts as a server for each other user. One effect of this is that there is no way for the software provider to control what content is made available for sharing, or to check it for viruses, trojans, or other malware. This is made clear by the software providers themselves:

"All files that are accessible using KaZaA Media Desktop (KMD) originate from other users of KaZaA. This means that there will always be the risk of irresponsible users introducing viruses...."[4]
(http://www.kazaa.com/en/help/virus.htm)

Of course, "irresponsible" in this context might mean careless or malicious. There is no way to guarantee that the file a user downloads is what the filename implies, or even the same type of file. This makes P2P networks a ridiculously

easy way for authors of viruses, worms, Trojan horses, etc. to distribute their handiwork. Simply naming or describing a file as a popular movie, song, or program practically guarantees that it will be willingly uploaded.

Further, many P2P users do not check their downloaded files before making them available for upload by others. They use the program defaults and make their download folder sharable, thus potentially propagating harmful content unknowingly. KaZaA encourages this, suggesting that users "go with the default settings...to allow everyone safe file sharing." Users' downloaded files will then automatically go into the shared folder and be available for search and download by other users.[5] (http://www.kazaa.com/en/help/big3.htm)

Another way individuals could distribute malicious content would be to "impersonate" a P2P software download site. With the tremendous volume of software downloads occurring, advertising one's site as a download mirror site might fool some users into downloading a malicious program, thinking they were getting P2P software.

Still another vector for malicious software through P2P networks is the P2P software itself. The download of the P2P software can introduce malware (not to mention spyware - this is also outside the scope of this paper). A page on Grokster's website explains how a "Trojan horse" was accidentally introduced into their released code, and then downloaded onto users' computers.

Grokster, like many P2P software vendors, bundles advertiser applications with their software to generate revenue. Grokster accepts whatever "adware" their client gives them, taking them at their word as far as what it does. In this case, an advertiser, ClickTilUWin, gave Grokster an application and told them it placed a link to a free online casino on the user's desktop. What Grokster didn't know (and the website doesn't make clear whether ClickTilUWin did) was that it installed a Trojan called W32.DlDer.Trojan. Grokster's anti-virus software didn't pick it up, and the infected software was downloaded by Grokster users for three weeks.[6] (http://www.grokster.com/dlderinformation.html)

From these examples, we can see that the stated policy of the P2P software vendors is that protection from viruses, Trojans, and malware is solely up to the user. Are viruses a real threat to P2P users? A look at some newsgroups indicates that users are regularly encountering viruses in files they've downloaded. Besides such anecdotal evidence, there is hard data from the P2P vendors and security companies, as well. For instance, the following notice appeared on Bullguard's website (which was linked from KaZaA's website):

"Users of the popular file-sharing service KaZaA are now targeted by the Benjamin worm. The worm is considered relatively harmless, although it takes up hard drive and processor power, rendering the infected computer slow. But it does attract special attention because it's the first of its kind to target the popular

p2p network. Looking like popular music, movie and software files, the W32.Benjamin.Worm spreads in the KaZaA network by tricking the KaZaA users into downloading a phony media-file to their computer and opening it. The size of the worm can vary since the worm pads itself with garbage bytes."[7] (http://www.bullguard.com/news20020520.aspx)

KaZaA itself had this to say about the Benjamin worm:

"Worried About Benjamin?
Recently a new virus was introduced to the Internet that specifically targets users of KaZaA Media Desktop and other p2p applications called Win32.Worm.Benjamin. So far the risk is low and the virus is not widely spread. We recommend you use the new 'Bullguard Benjamin Tool' to quickly and easily check your system."[4] (http://www.kazaa.com/en/help/virus.htm)

There is another risk to users of P2P software, one that results from the software's use of IP addresses to create P2P connections. Letting another Internet user know one's "real" IP address is a security risk in itself. In addition, someone sniffing on the network could hijack a session, spoof one or both users' addresses, or otherwise cause harm. One company that claims to address this vulnerability is Filetopia. Their software "uses a choice of strong ciphers and public key techniques for all communications"[8] (http://www.filetopia.org/home.htm) and other techniques to protect users' IP addresses. It supports, by default, the AES (Advanced Encryption Standard) encryption algorithm, as well as Blowfish, Idea, and seven other symmetric ciphers. For its Public Key (PK) functionality, Filetopia uses an asymmetric cipher based on elliptic curve algorithms.[9] (http://www.filetopia.org/encryption.htm#Rijndael (AES))

As mentioned above, the issue of "spyware" within P2P software is beyond the scope of this paper. However, common sense dictates that when you run a program on your computer which does more than you intend (e.g., capturing personal and/or demographic information and sending it to a third party, besides enabling you to share files), you are increasing your risk of system compromise. A look at the P2P software packages available indicates the prevalence of embedded advertising (which is how many P2P software vendors generate income). Some vendors are up-front about what third-party code is in their product and what it does. But not always. Recently, IDG News Service reported on the following attempt to use KaZaA users' computers without their knowledge:

"Software that will set up a network built from users' hard drives and bandwidth has been quietly bundled into the KaZaA file-sharing program owned by Australian holding company Sharman Networks and may also be distributed with other file-sharing programs.

"Los Angeles advertising software and design company Brilliant Digital Entertainment plans to use the Altnet network software that is bundled with KaZaA to build a distributed supercomputer for tasks such as weather-mapping and genome-cracking. It also plans to use the network as an alternative file-serving system for Internet ads or other content.

"The Altnet software has been downloaded along with KaZaA's file-sharing software about 20 million times, according to Brilliant. Most people don't realize Altnet is present if they installed the programs together."[10] (Chidi)

Since the news of Altnet's presence in KaZaA's software become public, KaZaA has offered an explanation of what they're doing. Initially, Altnet will provide KaZaA users with the choice to download files directly from entertainment companies (read copyright holders), in addition to all the peer users' files already available. KaZaA stresses that these files will be guaranteed high quality, virus-free, and accurately labeled. They may or may not carry a price tag – the distributors of this content "may be presenting demo versions, promoting a new idea or offering you pay per use content."[11] (http://www.kazaa.com/en/aboutaltnet.htm) The choice of whether to download, or keep, the file is up to the user.

KaZaA goes on to describe the Altnet resource-sharing application discussed above ("Does Altnet Have Anything Else To Offer Me? Yes, it's in the works.)"[11] (http://www.kazaa.com/en/aboutaltnet.htm) and stresses that it's entirely voluntary for KaZaA users. If a user decides to opt into the program, he will earn reward points redeemable for "goods and services made available by Altnet and its business partners."[11] (http://www.kazaa.com/en/aboutaltnet.htm) In addition, the user will be able to control how much of his computer's resources are made available.

It's possible that, if it hadn't been "caught", KaZaA would have introduced the resource-sharing aspect of Altnet without notifying its users or giving them a choice in the matter. As long as P2P networks rely on third parties for a revenue stream, this kind of deception will always be a threat, and a potential security risk.

Another real danger of P2P networks is that, although theoretically the user controls what subdirectories he/she makes available to peer users, sometimes more subdirectories are shared than is known or intended. For instance, the worm "Win32.Worm.Duload.A/B", discovered on August 22, 2002, can cause this. From The Bullguard website (accessed by a link from KaZaA's [http://www.kazaa.com/en/help/virus.htm]:

"The worm activates the KaZaA sharing and adds the above directory Media to the list of folders shared by KaZaA, so these files will be found by other KaZaA users."[12] (http://www.bullguard.com/virus/96.aspx)

Even without worms modifying P2P software's behavior, the risk is great that unintended files will be shared. As reported in AOL Computer Center, KaZaA's users may often be sharing private data without being aware of it.

The authors blame the “confusing and somewhat misleading nature” of KaZaA’s user interface for their finding that more than 60 percent of KaZaA downloads might be files not intended to be shared.

The article says that KaZaA creates a default directory of files to be shared, called the “download folder”. What many users may not realize is that when they add files to the download folder, all the files in the directory, as well as the directories below it, can be recursively shared.

The authors devised a test to determine how often unintended files were being shared by KaZaA users. Over a 12-hour period, they performed regular searches on KaZaA for Microsoft Outlook Express e-mail files, assuming that users would not intend to share private e-mails. Of 443 searches, 61 percent returned one or more hits for the e-mail files. In addition, other tests showed up word processing documents, Web browser caches and cookies, and financial software files.

“Dismayed with the results, the researchers wrote that 'while KaZaA is not a security application ... it nonetheless shares similar responsibilities to its users.'”[3] (Pruitt)

Nor is KaZaA alone. In April 2002, Europemedia.net reported that Morpheus users risked having their hard drives accessed, after security experts discovered a security hole in the program. This hole allowed the experts to catalog the contents of users’ hard drives and copy files from them.[13] (http://www.europemedia.net/shownews.asp?ArticleID=8205)

As if inadvertently sharing personal files with other P2P users weren't scary enough, there are others on the Internet who would like to see whatever is being shared, with or without the owner's permission. A product called ShareSniffer searches the Internet by IP address, looking for open Windows shares. It then builds a central database on an Internet newsgroup, listing all the open shares discovered by all its users. The rationale behind this? "ShareSniffer, Inc....asserts that if a computer is accessible on a network, its hard drive is therefore available for public consumption. Hence the motto: 'Because it's there.' ...ShareSniffer executives maintain that their program is a new permutation of peer-to-peer (P2P) software, and contend that anyone who leaves their computer IP address open to others is deliberately making his or her computer available for file-sharing. 'I want to emphasize that this is public and voluntary,' said Kerry Rogers, developer of the program. 'Microsoft Windows, by default, will not expose files to the Internet. It has to be consciously configured to expose files to the Internet.'...Rogers fails to note, however, that unlike other P2P systems like

Napster and Gnutella, one does not need to have ShareSniffer installed before one's computer can be tapped. Instead, ShareSniffer users can access any Windows computer that has file-sharing or print-sharing enabled and does not use firewalls or passwords, and can download or upload files to or from the computer's hard drive. In addition, ShareSniffer enables its users to modify or delete files on other computers."[14] (Weisman)

Many P2P users probably would not agree that they are implicitly inviting the world to browse, and potentially change, the contents of their hard disks. However, the laws concerning this topic are still evolving, and P2P users should be aware of this risk.

There is another behavior of some P2P software which can cause confusion and poses a potential security risk. When (supposedly) shut down, some programs, such as LimeWire, stay open and continue sharing files as long as there are active up/downloads in progress. This behavior can give the user a false sense of security if he thinks he's quit the program and stopped transferring data, but he hasn't. This behavior is documented in a FAQ on LimeWire's website.

"Q: When I go to quit LimeWire, it sometimes disconnects from the network but stays open. What's going on?
A: On Windows, Linux, all Unixes, and Mac OSX, LimeWire's default closing behavior is to remain open until all current uploads and downloads are completed. This means that LimeWire will not allow any new uploads or downloads, but it will automatically stay open for current transfers to complete before shutting down. You can change this behavior in the Tools>>Options window under 'Shutdown.'"[15] (http://www.limewire.com/index.jsp/faqs#gen4)

In addition to the significant risks of system compromise, P2P software also potentially poses huge risks to the networks to which its users are connected. It is obviously in the interests of the P2P software vendors to maximize hits on their download sites and use of their software. Some of them are financed by advertising revenue, and therefore they want their users to use their software (and therefore see their clients' ads) as much as possible. So it must be assumed that security is of secondary importance to them, despite their assurances that using their software is - or can be made - safe from a security point of view. For example, here is an excerpt from Bearshare's website, under the section titled "Gnutella Good Citizen Tips":

"PROPER SETUP OF FIREWALLS: Firewalls are important, especially when using a peer-to-peer program like BearShare, and although being behind a firewall doesn't prevent you from sharing to everyone (you can still upload files to some people), firewalls can still be a hindrance for you and other users.

It is almost impossible to establish a direct connection with another firewalled computer. Consequently, firewalled users will be unable to download files from

you, and you'll be unable to download files from other firewalled users. You will see their files as 'Unreachable' when you're firewalled, and that is exactly how other firewalled users see your files. *Therefore, if at all possible, it is important to get rid of your firewalled status for sharing purposes* (italics mine).

You don't need to get rid of your firewall completely, *you just need to 'drill a hole' in it for BearShare. It won't decrease your security because BearShare doesn't contain any security holes* (italics mine). Please read BearShare Firewall Tutorial for instructions how to configure your firewall."[16]
(http://www.bearshare.com/help/citizen.htm)

Most security administrators would probably take issue with the italicized statements. Encouraging users to "get rid of [their] firewalled status for sharing purposes" would probably violate even the most general security policy. "You just need to 'drill a hole' in it for BearShare" is hardly responsible advice for anyone, whether they're on a corporate network or surfing the Internet from home. "It won't decrease your security because BearShare doesn't contain any security holes" is a claim that hardly seems credible to anyone familiar with the current security landscape.

Another example of a P2P vendor giving advice on how to defeat firewall security can be found on Limewire's website:

"...if you or your systems administrator has configured your firewall for port forwarding (i.e. connections are being forwarded from your firewall to your computer), you can force the local IP to the firewall's address. This is often applicable to home users, and will help avoid the "double firewall" issue, and allow for better network connectivity. For further information, see http://www.gnutellanews.com/information/firewalls.shtml."[17]
(http://www.limewire.com/index.jsp/faqs#fir5)

Network security experts should therefore be extremely cautious about letting users share files using P2P networks. Security policies should be crystal-clear about the use of P2P software, both on office and network-connected home computers. Even home computers not connected to the corporate intranet must be viewed with suspicion, since a virus could still reach the corporate network via an infected file on a floppy. All computers should have robust and up-to-date anti-virus and anti-Trojan software installed, and all files should be checked when being transferred, either electronically of via Sneakernet.

Given the lure of P2P file-sharing, policies must be enforced firmly. Regular audits of phone lines should be performed to discover any modems being used to bypass the corporate firewall. The firewall itself should be configured to block P2P traffic, and to alert the network administrator if it sees attempts to use it.

There is interest in P2P technology for business applications, too. The wide distribution of computing resources and data, along with decentralization of network control, means that more and more information is located on employees' computers. There is naturally interest in the sharing of such information among employees, with the additional requirement that the sharing be as easy and non-technical as accessing the data local to the employee's own computer. This makes the P2P file-sharing model attractive. However, before business would embrace such a solution, the security risks of P2P file-sharing would have to be eliminated, or at least greatly reduced. One company that has attempted to address this need is Endeavors Technology, Inc., a wholly-owned subsidiary of Tadpole Technology. Their product, Magi Enterprise, is described in a press release as "a collaboration platform to build and maintain secure communities of collaborators for the sharing and exchange of information using Web-enabled devices."[18] (http://www.tadpole.com/tec/about/press/2001/110501.htm) They say that "Magi collaborative communities will be like a fortress - no one gets in unless they belong, and no one gets access to more than what they need to do their job."[18] (tadpole) To accomplish this, Magi "has financial-grade security tools, using X.509 Public Key Infrastructure (PKI) over a Secure Sockets Layer (SSL) network backbone."[18] (tadpole)

The Butler Group was quoted in the Tadpole press release, and their comments illustrate the need for security in this model. "The major fear for network administrators is that a P2P network would prove highly vulnerable to unauthorized access and subsequent misuse, as was recently the case with the SETI@Home project. Embedding high levels of security, such as authentication processes and potent encryption, throughout any P2P network is obviously a necessity in order to create corporate level confidence that business-critical data will be safe in transit."[18] (tadpole)

Major IT suppliers are also interested in the commercial potential for P2P. In an article in Computer Weekly[19] (Young), author Ken Young discusses the efforts of Sun, Microsoft, IBM, EMO, and Intel, as well as several startup ventures, to develop solutions that deliver the promised benefits of P2P while solving the security and scalability issues. He points out that little is known so far about the management or cost implications of using P2P computing, whether across internal or public networks, and this is making customers reluctant to commit to the technology. Some of the potential benefits to particular customers are noted, such as information sharing and the ability to use spare or dormant processor capacity, both of which translate into cost savings if realized.

But the issues of trust and control, which are largely ignored in the current P2P landscape, are obstacles to its widespread commercial adoption. Its is pointed out that if a P2P solution is deployed behind a firewall (i.e., within the enterprise), these issues are easier to surmount. But commercial success will depend on extending the capabilities beyond the organization.

The article goes on to describe two schools of thought about P2P: data-centered and compute-centered. The major difference is that the data-centered model (represented by the file-sharing networks already discussed here) offers sharing of data held on other users' systems, while the compute-centered model deals with distributed processing, where the main appeal is in using spare processing capacity on the network.

According to the article, the major difference between the two is that the data-centered model does not have a central directory (which leads to many of the security issues discussed in this paper). In an enterprise P2P application, there would have to be a dynamic index server, which would police a set of rules based on security levels or job functions that govern access to content.

In compute-centered P2P, on the other hand, a central server manages the allocation of distributed processing resources to the task at hand. This type of distributed processing is only appropriate for calculations that can be broken down into smaller tasks. In the past, this has usually meant scientific applications, weather modeling, and the like, but commercial applications could include data mining of credit card or shipping data, or the rendering of individual frames of 3-D movies.

How well, and how quickly, the P2P community deals with security issues remains to be seen. However, given the staggering growth of content available on the Internet, especially with users sharing with other users; the ridiculous ease of sharing; and the "because it's there" mindset of many Internet users, it seems likely that the growth of P2P file-sharing networks will continue unimpeded. Therefore, it is up to users, and security administrators, to be aware of the risks implicit in this wide-open architecture. The safest course of action is to not use, or allow, P2P file-sharing software. If it is used, its dangers should be minimized by the rigorous use of backups, anti-viral/Trojan software, and careful configuration of the P2P software to ensure it is doing exactly what the user wants it to do.

List of References

1. TechWeb-The Business Technology Network. CMP Media LLC. http://content.techweb.com/encyclopedia/defineterm?term=gnutella
2. KaZaA website. Sharman Networks. http://www.kazaa.com/en/index.php
3. Pruitt, Scarlet. "Kazaa Users Unwittingly Share Private Files". AOL Computer Center. http://aolsvc.pcworld.aol.com/computercenter/aol/article/0,aid,101726,00.asp
4. KaZaA website. Sharman Networks. http://www.kazaa.com/en/help/virus.htm
5. KaZaA website. Sharman Networks. http://www.kazaa.com/en/help/big3.htm
6. Grokster website. Grokster, LTD. http://www.grokster.com/dlderinformation.html
7. Bullguard website. Bullguard, Ltd. http://www.bullguard.com/news20020520.aspx
8. Filetopia website. Filetopia Inc. http://www.filetopia.org/home.htm
9. Filetopia website. Filetopia Inc. http://www.filetopia.org/encryption.htm#Rijndael (AES)
10. Chidi, George A.,Jr. "Kazaa Download Offers Unexpected Feature". AOL Computer Center. http://aolsvc.pcworld.aol.com/computercenter/aol/article/0,aid,92823,00.asp
11. KaZaA website. Sharman Networks. http://www.kazaa.com/en/aboutaltnet.htm
12. Bullguard website. Bullguard, Ltd. http://www.bullguard.com/virus/96.aspx
13. "Experts find security hole in Morpheus". May 2, 2002. Europemedia. http://www.europemedia.net/shownews.asp?ArticleID=8205
14. Weisman, Robyn. "New Hackerware Makes Everyone a Hacker". March 6, 2001. E-Commerce Times. http://www.ecommercetimes.com/perl/story/7906.html
15. LimeWare website. © 2002 Lime Wire LLC. http://www.limewire.com/index.jsp/faqs#gen4
16. BearShare website. © 2002 Free Peers, Inc. http://www.bearshare.com/help/citizen.htm
17. LimeWare website. © 2002 Lime Wire LLC. http://www.limewire.com/index.jsp/faqs#fir5
18. Tadpole.com website. Nov. 5, 2001. © Tadpole Technology Plc http://www.tadpole.com/tec/about/press/2001/110501.htm
19. Young, Ken. "Is P2P ready to do business?" Computer Weekly, May 24, 2001: 76.

Last Updated: May 29th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Amsterdam August 2020	**Amsterdam, NL**	**Aug 03, 2020 - Aug 08, 2020**	**Live Event**
SANS FOR508 Canberra August 2020	**Canberra, AU**	**Aug 17, 2020 - Aug 22, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**