



Security Concerns for Peer-to-Peer Software

Mike Petruzzi <mpetruzzi@ktsi.net>
Rob Sherwood <rsherwood@ktsi.net>
John Dunnivan <jdunnivan@ktsi.net>
Rob Chavez <rchavez@ktsi.net>
Pat Holley <pholley@ktsi.net>

Key Technologies and Security, Inc.
July 18, 2000

Abstract

Peer-to-peer (hereafter referred to as P2P) communication software allows individual computers to share and swap various types of files. Recently, P2P software has been much in the news due to current and potential lawsuits. Napster, the company that makes software for exchanging MP3s (encoded music files), is being sued for copyright infringement; the recently re-released Gnutella has the potential for exchanging all types of files and may therefore be embroiled in litigation even more quickly than Napster was.

More important than any copyright concerns are the potential security concerns for corporations and consumers. For corporations, P2P software threatens:

- bandwidth consumption
- liabilities and acceptable use violations
- undermining of security policies
- Trojan Horse and virus distribution
- disclosure of IP and MAC addresses
- telecommuters

For individual consumers, P2P software represents:

- disclosure of IP and MAC addresses
- disclosure of connection speed
- file sharing
- Trojan horse and virus distribution.

Background

P2P software takes the idea that the Internet is for sharing to new levels. P2P has been described as “an anarchistic threat to the current Internet” (David Streitfeld, *The Washington Post*, July 18, 2000) and Marc Andreessen has called P2P software the most important thing on the Internet in the last six years (when Netscape was first released) and a “benevolent virus.” Ian Clarke, the creator of FreeNet, says, “People should be free to distribute information without restrictions of any form.”

P2P allows users to search for files; some software may allow for this to be done anonymously. All these products, by definition, link computers without the use of a central server using true peer-to-peer networking. Gnutella sends the search request to 10 computers. If those 10 computers do not have the requested file, then the request is sent out to 10 computers from each of the first 10 computers. This number grows exponentially and takes 5 to 10 seconds for each individual search, all at the same time. It is easy to see the attraction to Gnutella. In a matter of minutes, over one million computers could be searched. If the user has enough bandwidth, a download can take mere seconds to minutes. These files can then be downloaded to the user’s computer. Even with a 56k modem, 4 or 5 songs can be downloaded in less than one hour.

Even protected code is not safe. Programs like AOL Instant Messenger, or any other P2P software, can be reverse engineered and released as Open Source software. These programs can then be released for any operating system platform. This also gives malicious hackers the ability to change the software code so that it can be used for other purposes. This requires a great deal of programming knowledge and skill, but can still be done.

The first obvious concern is the liability of copyright infringement. Even though all of the companies that produce and release P2P software issue warnings regarding the illegalities of downloading copyrighted materials, simply releasing the software makes those illegal acts possible. Some P2P software contains security warnings during the installation of the software and enables default settings to protect the naïve consumer and their computer. But armed with some simple knowledge of the Internet and its protocols, even a beginner criminal hacker can cause many security risks to users of this class of software.

Concerns for Corporations

Corporations are at the greatest risk to some of the potential security holes from P2P software. Sophisticated hackers and beginners alike can experiment and gain access to the intellectual property of a company. Worse, Trojan Horse programs and viruses can be released using some of the security holes. However, some simple fixes and common sense on the part of management and network administration are all that it takes to protect a company.

At the present time (July 2000), there are no known weaknesses in the protocol that underlies the P2P software products Napster and Gnutella or the implementation of the protocol. However, if weaknesses exist and are discovered, the weaknesses could allow exploits like buffer-overflow attacks against the client. This would allow any attack up to and including the remote execution of malicious code.

Bandwidth Consumption

For the majority of companies, bandwidth will be a big concern. Internally, every user that is using a P2P program is soaking up network bandwidth. Software like Napster, Gnutella and Scour are generally used to download relatively large files such as MP3s, AVIs, MPGs (AVIs and MPGs are movie file formats) and even some JPGs and GIFs (picture files). If enough users are participating in such downloads, regular business can be brought to a standstill. Universities have begun forbidding the use of Napster on campus for this very reason.

Liabilities and Acceptable Use Violations

Another concern for corporations is that the company can potentially be held responsible and, therefore liable, for the copyright violations that the users of P2P within the company commit. Additionally, most companies have an acceptable-use policy for the Internet. Chances are that huge time wasters like MP3 downloads are violating that policy, not to mention the potential lawsuits for downloading objectionable material. One group known as Zeropaïd tested its theory that the potential for distribution of pornography would increase by making it even more widely available. Using P2P software, they found that files that were given fake names referring to pornography were downloaded at an alarming rate. The especially alarming situation is that the test used phony files with titles that referred to child pornography — and possession of or trafficking in child pornography is a felony in most jurisdictions around the world. The information can be found at www.zeropaïd.com/busted.

Remote users and traveling users are usually under the same guidelines as the users in the corporate office, but these users present a different kind of risk because there is very little that can be done to police them.

Undermining of Security Policies

Security policies are written by companies to protect the company and establish the procedures that the company will follow to create a secure networking environment. Often these policies and procedures define the architecture that protects the network with items like firewalls, routers and proxy servers and the Internet access controls that are enabled on them. Most of the P2P software can be manipulated to allow unhindered travel through the security architecture of the network. This renders the security policy less than effective. AOL Instant Messenger can allow you to “sniff” for open ports to use and Gnutella has instructions on their Web site that will allow a user to bypass the port rules on a firewall. In defense of Gnutella, they do state, “It should be noted that any firewall administrator with half a brain will limit these ports to only go to the systems on which [special] services are running for official business.” They do ruin any credibility for legitimate concern by following up with “Who knows, you may get lucky.”

Trojan Horse and Virus Distribution

As stated earlier, a group published files under fake names that referred to pornography and made them available for download. That the files were downloaded shows that malicious users can freely distribute

Trojan Horse and Virus files. If the user is using a P2P program such as FreeNet, there is little fear of getting caught. FreeNet does not use a central server and IP addresses are not tracked. In fact, the file is copied locally from participating client to participating client until it gets to the requesting client. The possibility of spreading a Trojan Horse or virus then becomes as easy as sending e-mail. The producers of Gnutella address this. They say that the user is exposed to viruses “no more than downloading files from the Internet through any other means such as FTP, the Web, IRC or Usenet. Use common sense and scan executable file[s] using a current virus scanner with a recent list.” But, that only protects the user from existing or known Trojans and viruses. Also, new security holes in operating systems are being exposed daily. Programming languages like Java and ActiveX are being used increasingly to create new types of Trojans and viruses. With new viruses and Trojans being written daily, using P2P software increases the chances of being exposed.

Disclosure of IP and MAC addresses

In order for computers to communicate with each other, each computer needs to know the other’s address. In most cases, this information is stored in a cache that eventually will be overwritten. In any case, even a beginner hacker armed only with the knowledge of basic TCP/IP commands can gain valuable information about where the data are coming from or who is trying to get information from them. Being on the safe side of a DMZ (a “demilitarized zone”, meaning a strong security perimeter) only protects the user; the network is still exposed and a savvy hacker with sophisticated tools may be able to gain access to the network. Even with the exposure of Web pages, the Internet still provides most networks with enough anonymity to feel a certain amount of uneasy safety. The use of P2P software on a network can quickly take away that anonymity. If nothing else, the addresses of routers and gateways are exposed, leaving open the possibility of buffer overflows and denial-of-service attacks. In the rare case that the corporate user is connected directly to the Internet, that IP address is exposed. Gnutella users are even given the IP address from which they are downloading by widening the column immediately to the right of the “Status” column in the downloads window. This can be a simple starting place for a hacker. Take this example; User A is using Napster to download an MP3 from User B, who is located inside a network but who is connected directly to the Internet. User B notices that the download is slowing down his computer and forcibly disconnects User A. User A gets angry and, using simple commands, finds the IP address of User B. Armed with that information, User A then proceeds to gain access to User B’s computer and shut down necessary ports for communication. Now, User B has gone from slowed down to shut down. Imagine if User A were a skilled hacker armed with some sophisticated tools.

Telecommuters

Telecommuters present many new risks. These users have company information on their home computers or company-owned portable computers and in some cases, have high speed Internet access. Even if the coveted “always on” access is not available, telecommuters are still subject to the same risks as corporate computers; the policies and procedures that have been outlined for corporate users must apply to the telecommuter. Unfortunately, in the current state of security, it is unreasonable to expect that all telecommuters will abide by the policies. In an effort to protect these users, the company should provide appropriate security tools for protecting the telecommuter’s systems.

Concerns for Consumers

Consumers are at risk, as well as corporations. In many cases, consumers are subject to the same risks as corporations. There is no acceptable-use policy to give the user guidelines to safe Internet usage. There is no security policy to establish how often anti-virus definition files should be updated or even if an anti-virus program is in place. Bandwidth generally is not a concern for a home user. Most homes are not networked, but home users that connect using cable modems are subject to the same effects as network users since the bandwidth is shared by all cable modem subscribers. While most consumers are not at risk for losing a company’s intellectual property, there are still possibilities for damage. And given that the number of people that are given the opportunity to work from home increases daily, the potential that some of the information that is stored on a home computer is critically important for a business increases, as well. There are other concerns such as the fact that the average home user does not have a Help Desk that they

can call when things go wrong. This is an arena where the rules of common sense do not apply because that common sense would only come from an IT professional or technologically savvy user.

Disclosure of IP and MAC addresses

The rules of Internet protocols are the same for any user on the Internet. But, with the increased desire for high speed Internet access creating an increased availability, more and more home users are connected to the Internet in an “always on” state. These users are given dynamically assigned IP addresses, but unless the user turns the computer on, the lease on that address is theoretically infinite. At the very least, that lease will exist long enough for the potential for damage. Although “personal firewalls” are widely available and increasingly sophisticated, the average home user has nothing between them and the Internet. Now, when an address is exposed, in most cases, it is the direct address to that computer. A simple scan of the computer can tell a hacker what kind of operating system the user has and from there, the hacker can figure out what exploits are available.

Disclosure of Connection Speed

Users of some P2P programs like Napster have access to information concerning connection speed. Because most 56k links and below are dial-up accounts, the hacker may not desire to even waste the effort necessary to gain access. But, connection speeds of 144k and higher can indicate DSL or cable modems, which may be in use by the home users. By executing a simple scan of the computer, a criminal hacker now knows how to begin to gain access to the computer.

File Sharing

Many protected code programs like Napster, Gnutella and Scour have been reverse engineered and released as open-source programs. Although this may be good for users and for the quality of the programs because of faster bug fixes, it also means that the code can be manipulated and used in malicious ways. Napster and Gnutella give all clients direct access to files that are stored on a computer’s hard drive. Such files are stored in folders and directories that are not shared by default, but there is the possibility that other folders can be added and shared. A hacker could figure out what operating system the client computer has and could connect to folders that are hidden shares, thus gaining access to folders and information that were not meant to be accessed. Most home users may find this alarming, but benign. “What do I have on my computer that some hacker would want?” the user may ask. But, information like credit card numbers, checking account numbers and the like could be stored on the computer — for example, using the popular Quicken accounting software. As far back as January 1996, the CHAOS Computer Club demonstrated on German TV that a system running Quicken could be subverted to generate unauthorized bank transfers. The prospect of seeing strangers with access to such data and programs is frightening. s

Trojan Horse and Virus Distribution

Just like the corporate user, the home user is exposed to Trojans and viruses. But, as was stated earlier, most home users do not have access to a Help Desk to help them out of trouble. Most home users do not have access to a network drive to back up their data. Most home users do not have a policy that tells them what anti-virus program to use and how often to update it. Suddenly, the increased potential for virus availability becomes alarming. Trojan Horse programs like Back Orifice can publish the IP address of an infected user making that user subject to attacks from multiple hackers, rather than just the single attack of one hacker that gained the information through IP commands.

Solutions

Solutions for Corporations

Relatively simple fixes and common solutions can be applied and will make the company's network more secure and the employees more productive. The chart below shows best practices and recommendations for dealing with P2P software:

	Best Practice	Recommended
Establish Security Policy	X	
Define Acceptable Use Policy	X	
Perform regular security seminars for users	X	
Block access to known P2P servers		X
Block access to known P2P clients		X
Perform regular audits of security policies and procedures	X	
Install and perform regular updates of Anti-Virus Software	X	

While the above measures may seem too simple for potential P2P problems, they are far more complex when implemented. If none of these measures is already in place, it is highly recommended that a team of security professionals be brought in to assist in finding and implementing the correct solution to the company's security needs. Where no security policy has yet been established, the new measures are often seen as restrictive and counter-productive to employee morale, but they can be easily implemented and accepted if done correctly using sound methodologies of policy development and implementation.

Solutions for Consumers

It is far more difficult to assist a consumer in matters like these. The consumer just isn't aware that a problem may exist. Many times the user stays out of trouble. Sometimes, where media attention is drawn to potential hazards it causes consumers to completely back away from the problem and avoid it altogether. A home user can be protected in many of the same ways that a corporation can be protected. Through simple education, a home user can protect him/herself. There are many products available to protect the home consumer from the dangers that the Internet poses. The chart below describes some best practices for home users:

	Best Practice	Recommended
Install and regularly update an Anti-Virus Program	X	
Install a "personal firewall"	X	
Disable sharing of the hard drive	X	
Use caution when using P2P software		X
Install Internet Access Control Software (especially for children)	X	
Educate all users of the computer	X	

The authors welcome your correspondence. For reprint requests, contact Mike Petruzzi <mpetruzzi@ktsi.com>.

About KTSI - KTSI is an industry thought leader and provider of world-class information assurance products, services, and training

solutions. KTSI's sole focus is on information assurance and electronic business.

KTSI can be found on the Web at www.ktsi.net and its offices are in Manassas, VA.

Key Technologies and Security, Inc.

10688 Crestwood Drive

Manassas, VA 20109

Phone: (703) 330-7117

Fax: (703) 365-0322