Global Information Assurance Certification Paper

The Dangers of Peer to Peer Applications within the Enterprise

By Shawn Wood

GSEC: Version 1.4
July 31, 2002

Abstract

Peer to peer software is a growing concern, especially when considering the threats that are introduced when these applications exist on machines within the enterprise. The threats include susceptibility to viruses, malware and trojans, the sharing of sensitive data, possible corporate espionage, theft of intellectual property, and the availability of resources. These issues will be presented and some solutions will be suggested that may be implemented in an attempt to address them. One particular file-sharing program will not be focused on, so as not to give the false belief that one program is worse than any other - they all present a threat. Within the enterprise the stakes are high and it is this paper's intent to provide the network administrator with an overview of the threats that exist if P2P software is allowed to reside within their network.

How the problem began

It was only a little over a year ago that it was announced that Napster was ordered to shut down its file-sharing network to the dismay of millions of users. In it's early stages in 1999, Napster users barely surpassed a million and was comprised mostly of the young and computer savvy. Over the next two years, with the publicity it received due to the ongoing battle with musicians and the recording industry, this music sharing software sparked the interest of millions of people. In an epidemic like fashion, more and more typical users became enthralled with the ability to freely download music and when the giant finally fell in the spring of 2001, Napster had resided on 60 million computers.[1] Unfortunately the masses had already developed an attraction to the music sharing experience, and in its wake, less popular programs like Kazaa and Gnutella soon gained momentum and now reign over the peer to peer kingdom. The desire to share is as strong as ever and has in fact become a perceived right.

With this in mind, it is not surprising to find that some form of file sharing software has made its way onto desktops within our organizations. The fact of the matter is that peer to peer networking within corporate networks creates a security hole big enough to drive a train through it, and you certainly don't want your network to be railroaded! Now we will take a look at some of the threats.

Bypassing the firewall

The first line of defense between a hacker and the enterprise is the firewall. It sits directly on the perimeter of the network, and if configured correctly and according to your corporate security policy, it helps to protect your internal resources from the outside world. A firewall's job is to act as a filter and basically to either:

- allow packets to pass through, or
- refuse the packets and not allow them to pass (drop the packets).

This decision regarding the passing of packets is made based on the ACL (access control list) that exists in the firewall's configuration. The ACL is a series of entries that are made up of "permit" or "deny" rules that each packet is compared to and is then either allowed to pass or are dropped. There is an ACL that is applied to the inbound interface (internal network) and one that is applied to the outbound interface (external network). When the packet reaches the corresponding interface, the firewall analyses the source, destination, and protocol headers in the packet and begins to traverse the ACL looking for a match. The packet is processed from the top of the ACL to the bottom, and any packets that are "permitted" are allowed to reach their destination, while any that are denied are dropped. If a packet does not match any of the entries in the rules, its fate is decided by the default rule that appears at the end of the ACL – the "deny all that are not explicitly allowed".

For example, an extended access list on a Cisco Pix firewall that allows all traffic to travel out of outbound interface would look like this:

access-list *name* permit ip [source-network] [source-mask] any
access-list *name* deny ip any any [2]

Many firewalls take quite a beating on a daily basis and are very effective in "keeping the bad guys out". Although a firewall may be effective at not allowing undesirable traffic in, many are lax in their ruleset regarding what packets are allowed to travel out (as in the above example). It is for this reason that internal clients are able to connect to peer to peer networks, such as Gnutella Net in the first place.

Even if an inside user does not initiate a session with an external client, one can still be established. Assuming the P2P software is Gnutella and the client has already connected to the Gnutella Net, following is a description of how external clients are allowed to connect to a client in the internal network.

An external Gnutella client attempting a connection (download) first initiates the connection with a "pull" request to an internal client behind a firewall. Because the client is behind a firewall and the packets are not allowed to pass, the connection is refused. The problem lies in the fact that Gnutella clients are configured to initiate a "push request" if this initial "pull request" has been rejected. When the client within your network receives this push request, they then proceed to initiate the connection with the external client. If this outbound traffic is allowed to pass the firewall, a connection is then established.[3] It is at this time that an internal user has become part of a separate peer to peer network, completely bypassing your firewall and you now have an uninvited guest with a connection established within your network. And your company paid how much for that firewall?

Viruses/Trojans/Malware

One of the greatest threats regarding file sharing that must be mentioned is the propagation of viruses, and downloading of trojans and malware. P2P software serves as the perfect vector for infection and subjects your network to the risk of confidentiality, availability and integrity attacks. The opportunity for one of these threats to make their way into your network is staggering. Of course, the inherent danger results from the fact that when a user is downloading a file, they really don't know what they are getting. A user may believe they are actually downloading a genuine music file or a software program, however, just because it has an authentic looking title, does not mean it is so.

On May 18, 2002 the Benjamin virus was discovered within the Kazaa network. This virus posed as popular music files, movies and games in an attempt to trick people into downloading them. Once executed, the worm created a directory called %windows%\temp\sys32 and changed the settings so that this folder was accessible to other Kazaa users, thereby allowing propagation to continue. It then displayed a fake error message:

"Access error #03A: 94574: Invalid pointer operation
File possibly corrupted." [4]

Once this was completed, the virus stays resident waiting for the next victim to download it.

Luckily for many corporations, this was a low profile virus that was written in an attempt to allow its writer to generate money.[5] It did not cause much damage, but the threat still exists. This was not the first virus to circulate via P2P networks and it is certain that it will not be the last.

These programs also provide a perfect platform to initiate the fast propagation of trojans or malware. According to Symantec, some of the malicious code that is currently circulating the Kazaa network is:

- W32.Kwbot.Worm – a backdoor trojan that with its own IRC (Internet Relay Chat) channel. It opens a random port to connect to the hacker which can provide access to system/network information, allow propagation of trojan to other IRC channels, use the machine as an agent in Dos attacks and remove itself from the registry. [6]
- W32.HLLW.Kazmor – a backdoor trojan which can allow a hacker to spoof IP packets, perform port scans, steal host information and launch attacks.[7]

These are just two of many tools that a hacker could use to gain access to the network. A user may believe they are simply downloading a copy of popular music, but in reality they are erroneously allowing malicious code to be installed on their machine, just waiting to be awakened by its owner. Once the machine has been compromised, it may be used to attack your own network or somebody else's.

File Sharing

Music sharing was pioneered by Napster and served as a means for sharing only MP3's. It introduced many to the peer to peer technology and served as most peoples first experience with file sharing. Because of this, along with the introduction of multimedia sharing, many users today still believe that the only files that get shared out are multimedia files like music, videos, software, etc. What they don't understand is that most file sharing software these days allow the sharing of all files. This can lead to users unknowingly sharing out private files, which is dangerous to the corporation and could possibly result in corporate espionage, stolen passwords, or serve as a tool in the recon phase of an attack.

A recent study was conducted by Nathaniel S.Good of HP Laboratories – Information Dynamics Lab and Aaron Krekelberg from the Office of Information Technology at the University of Minnesota entitled "Usability and privacy: a study of Kazaa P2P file-sharing" and was based on Kazaa's 1.7.1 release. In their research it was discovered that many users inadvertently shared out private files due to design flaws within the application. Some of the things they were able to establish are:

- It is difficult for a user to determine what types of files are actually being shared, and it is not apparent that every file type is a prospect for sharing, as opposed to just sharing multimedia files.
- During configuration of the program, it is not obvious to the user that folders selected for sharing are done so in a recursive manner, i.e. if a user has selected C:\, it is not obvious that this will share every folder beneath it. The software also assumes that the user has an in depth knowledge of file sharing pertaining to the hierarchy of folders.
- The program makes it very difficult to configure the program to stop sharing files once they have been shared. If a user wants to remove the sharing of files, they have to be deselected one at a time - a significant task if the entire drive has been shared!

One very interesting point of their discovery is the fact that some users have a definite interest in other's private files, assuming a user has mistakenly shared them out. In order to make this establishment, they ran a dummy client that shared out dummy files like: Credit Cards.xls, Inbox.dbx and Outlook.pst and allowed the client to run for 24 hours. In that time four users downloaded the Credit Cards.xls file and two users download the inbox.dbx. [8] Obviously certain people are very attracted to these files.

This is potentially very dangerous to the corporation as confidentiality problems can arise if the user has any sensitive data stored on their machine, which could potentially lead to corporate espionage. What type of information may be residing on an executive's desktop? Serious privacy issues could definitely result if access is allowed to private files containing confidential data, cookie's, email files, and password files to mention a few. Also, it is important to include VPN and laptop

users in this equation, as they are more likely to have data stored locally on their hard drive.

Theft of Intellectual Property – Copyright Infringement

Music

The RIAA (Recording Industry Association of America) won its ongoing battle against Napster regarding the illegal sharing of music files. It is continuing its pursuit in attempting to stop the theft of intellectual property by starting to focus on corporations. In April of this year, it reached a settlement with IIS (Integrated Information Systems), an Arizona based company that ironically provides security services. The company apparently provided a server to its internal users as a platform for storing MP3's. When the RIAA became aware of these activities via an e-mail informant, they quickly took action. The cost to the company totaled a million dollars in settlement fees, and Matt Oppenheim, the Senior Vice President of Business and Legal Affairs (RIAA) stated that it "sends a clear message that there are consequences if companies allow their resources to further copyright infringement". [9] There is a definite risk to a company allowing copyright infringement to take place in it's internal network and can possibly result in a damaged reputation along with a high price tag attached to it.

Non-compliant licenses

Unfortunately sharing is not strictly limited to music files, as many people also share out software programs. Some of these software packages can be very expensive to purchase. Although most users these days have a fairly good knowledge as to what pirating software entails, for some reason the desire to download seems to prevail over common sense. In order to address the threat it is necessary to look at the human aspect for that is what puts us at risk to begin with.

For some unknown reason people these days take the theft of intellectual property very lightly. It could be that pirated software is so readily available that it generates a high temptation to download illegal software. Or they may believe that the software companies "make enough money already". Or maybe they associate stealing with physical objects, and have difficulty relating theft with things they cannot touch.

Consider this scenario: Suppose an honest person is on their way to work one day and happens upon a wallet lying in the street. As soon as they get to work, they proceed to call its owner and happily report that "yes of course, all the money is still in it" and arrangements are made to return the wallet. Then the person goes about their work very proud of their good deed. And so they should be. However, lunch time comes and this same person logs on to iMesh, sees that copy of software that was just denied approval for purchase last week. Well before you know it, that same honest person has suddenly sprouted horns and proceeds to double click. They have just committed theft but don't really consider the seriousness of their actions.

They may have convinced themselves that they will only use it for a couple of days or that they aren't really hurting anybody. The bottom line is that they have just committed a crime and they don't understand the risk they have introduced to the company.

Software piracy is a rising problem and it is continuing to grow. Caast (The Canadian Alliance Against Software Theft) and the Business Software Alliance (BSA), have released the seventh annual study regarding global piracy, which indicates that 38 percent of business software applications in Canada were pirated in 2001. Caast, which includes members like Adobe, Autodesk, Macromedia, Microsoft, Symantec Corp., also warns that companies not complying with copyright laws should be prepared to face the consequences.[10] And they sound serious. If your company falls in this category, Caast has also graciously implemented a "truce" program that allows a non-compliant company to come forward and get legal.[11]

Caast has just recently partnered with a company called Mediaforce.[12] They are responsible for developing MediaSentry, a sophisticated tool that searches the web for piracy via "advanced heuristics, self-adapting searched, neutral search algorithms, and probability ranking formulas, permitting an unprecedented ability to successfully locate and identify infringing material". Basically, copyright owners provide MediaSentry with a list of "works". Then MediaSentry's sophisticated agent patrols the internet at regular intervals searching for violations. Any confirmed infringements results in them contacting the perpetrators ISP and notifying them to block their access to the network until the material is removed, or a license is purchased. Mediaforce then requests that the ISP restore access, and then your company continues to be monitored for repeat infringement.[13] Obviously this sounds like a solution that is very effective in reducing copyright infringement and it appears that they are not taking this task lightly. Can your company afford to be blocked by your ISP? Or possible a hefty fine for non-compliance?

Adware/Spyware & Bandwidth

Adware is software that comes bundled together with the peer to peer software and it is virtually impossible to download a file sharing program these days without it - in fact, many programs come with more that one. Bearshare is bundled with Savenow and Nowbox and Kazaa and iMesh comes with Cydoor, just to mention a few. These are the programs that are responsible for the annoying pop-up ads that occur after installing the primary application and they usually run as their own entity.

They are designed to provide advertisements, typically in the form of pop-ups or banners as a trade-off for downloading the file sharing software at "no cost to the user". The goal is to provide the user with personalized ads and some deliver these ads to the desktops based on the URL's visited by the user. Many of these programs report demographic information back to central servers or prompt users to fill out surveys which can then (depending on the conditions of the EULA), be shared with third party companies. Some track users based on their IP addresses.

The reader is strongly encouraged to view the link provided below. It links to the privacy agreement of Nowbox; a package bundled with Bearshare.[14]
URL: http://www.nowbox.com/privacy_policy.html

Upon inspection of some of these adware agreements, it is surprising that many people would actually agree to their conditions! The problem is - how often do end users actually read the agreement? Very rarely, I would guess. It has become second nature for people (hopefully not network administrators) to bypass these agreements, and just click on the "I agree" button. Also, the fact that these programs will be installed is usually not done so in a secretive manner - they are simply checked at the time of setup. However, if the agreement hasn't been read, the user simply has no idea what they are putting on their machines. This must change. Although internal users should not be allowed to install software on the company's computers without proper approval in the first place, users still must be educated to read the EULA.

Another consideration is the confidentiality issues pertaining to the information that is gathered and where it is stored. Although these companies claim that the personal information is not shared, there is no way of knowing what type of information a user is actually entering when filling out a survey, or what are the questions relate to. Could internal users be giving a way information that could possibly fall in the wrong hands? How secure the servers are on which this information is it is stored? It is fair to assume that information not shared cannot then be hacked and potentially used against you in the recon phase of an attack.

Installing peer to peer software introduces a significant threat to the corporation and the user alike, by bundling the software with what is commonly referred to as adware or spyware. The tasks they perform, (other than providing the peer to peer companies with revenue), is varied depending on the software. Most of these programs perform some form of tracking of the users and at the same time, consume internal resources posing a threat to availability and confidentiality to users and the network alike.

Bandwidth Considerations

If there are more than a couple of users within the enterprise performing downloads as well as uploads, a significant amount of the network's bandwidth can be exhausted. Of course this expenditure of network resources continues to increase with the number of people logged on and sharing. This creates serious issues regarding the availability of resources and is definitely a serious problem on its own. But then couple this with the adware applications that may be running within the enterprise and your users may have significant performance issues. Regrettably, with the fast approaching implementation of Altnet, it is most definitely going to get worse.

When adware runs on a machine the program may consume the user's desktop resources – particularly if they have more than one installed. Users may notice that their computer has slowed down notably as the CPU cranks away running processes they did not initiate. These processes may involve querying the ad servers or downloading new content to the hard drive. The way in which this task is performed varies according to the application.

Once again, the reader is strongly encouraged to view the link provided below. It links to the privacy agreement of Savenow; a package bundled with Bearshare. URL: http://www.whenu.com/about_savenow.html [15]

Beware the Coming of Altnet

In April of this year, the computer industry was astounded to learn that a program created by Brilliant Digital Entertainment had been included in the Kazaa download. (Doesn't anybody read the "terms of service")? The program, b3d Projector, has been installed on millions of computers and will soon be remotely awakened allowing each computer to serve as a node in an enormous peer to peer network known as Altnet.[16] When implemented in July, Altnet will use the processing capability and resources of the client's desktops to not only provide real-time ads, but also to distribute various forms of content like music, games and video streaming.[17] Users will have the choice as to whether or not they "opt in", and if they do, they will receive rewards in trade for their computer power. They will then be able to redeem the rewards to buy content of their choice.[18] Even though Altnet could prove to be an effective solution in ensuring that content providers receive payment for their goods, it has no place in the enterprise. And corporate users certainly have no right to allocate company resources for their personal benefit.

Resolution

There are many threat vectors that these peer to peer programs serve as carriers and the dangers associated with them are sure to increase as time passes. Now that some of the threats have been addressed, you may be asking yourself, "What now"? There is one simple answer to that question. In order to mitigate the threat, you must make every attempt to get these programs out of your enterprise! What follows now are some suggestions you may want to consider implementing keeping in mind the requirements specific to your organization.

- Develop and implement security policy.

If you have established that your network is at risk, the first step to addressing the issue is to develop a policy. This provides everybody with a clear and concise objective. Be sure to define the purpose for the policy, any other relating policies, the reason that the policy is being implemented, a clear statement, and what actions must be performed. In order for the policy to be effective a person in high authority should sign it, like at the executive or senior management level. This will give the policy a significant amount of "clout" and you have more of a chance of it being

respected and followed. Some policies to be considered may include: firewall policy, acceptable usage policy, antivirus policy, theft of intellectual property, audit policy and desktop policy. These are only listed as suggestions as every policy is unique to the organization.

- Educate the users.

Most users simply don't understand the risks that are involved when they install these programs on their desktops. Some people don't take corporate policies seriously enough. For whatever the reason, it is pertinent to get these people on your side. Educate them about the risks that they are introducing to the network. Tell them that, not only are they affecting their own resources, but that they are wasting resources of the entire network. Teach them to read EULA's. Inform them that these programs may be tracking their actions. Let them know they are committing theft, which is a serious crime!

Unfortunately these programs are decentralized and unless you are going to implement a group policy that does not allow them to install software on their desktops (which could be an administrative nightmare in some enterprises), it is vital that internal users share in your security objectives.

- Block ports used by P2P software on the firewall.

Assuming that a firewall security policy suited to your organization's requirements has been put into place, it is worthwhile to consider blocking ports that these programs use. Some of them are listed below.

Port	Program
80	BadBlue
80	hotComm
80	INoize
1044	Direct File Express
1045	Direct File Express
1214	Grokster
1214	KaZaA
1214	Morpheus
4661	EDonkey 2000
4662	EDonkey 2000
4665	EDonkey 2000
5190	SongSpy
5500	Hotline Connect
5501	Hotline Connect
5502	Hotline Connect
5503	Hotline Connect

6346	Gnutella Protocol
6347	Gnutella Protocol
6666	Yoink
6667	Yoink
7788	BuddyShare
8080	hotComm
8888	AudioGnome
8888	OpenNap
8888	Swaptor
8889	AudioGnome
8889	OpenNap
28864	hotComm
28865	hotComm

It should be noted that this would only block the default ports used by the P2P services on the firewall.[19] Since some of these applications can be configured to run off any port, it is no guarantee that you are eliminating the threat, but it is one positive step towards defense in depth. Also, proceed with care when blocking traffic as some of these programs rely on ports that may be necessary to keep open (i.e. some travel on port 80).

Once your firewall ruleset has been tightened, continue to monitor the traffic that passes the firewall so that traffic travelling on ports other that the default ports will not go unnoticed. Pay close attention to your firewall logs and the occasional use of a sniffer may notify you that one of your users is not following policy.

- Ensure that an Antivirus solution is implemented and definitions are kept up to date.

Every enterprise should have an antivirus solution already implemented. If not, you are vulnerable to one of the top threat vectors: viruses, trojans and malware. Because desktop scanners on their own are very difficult to administer, it is recommended that a network scanning solution also be used to complement them if at all possible. These solutions can provide effective coverage for the firewall, servers and desktops alike. They can provide real time protection and they also allow for centralized administration, which can be very effective in pushing out updated virus definitions and monitoring. This can prove to be very efficient in keeping clients up to date when weekly definitions become available. Also, in times when there is a high - risk outbreak, these definitions must be propagated throughout the entire network as soon as possible.

Ensure that you have a process in place that makes you aware of these outbreaks as soon as they are discovered! It can be as simple as visiting an antivirus site a couple of times a day. A few helpful links are provided below.

URL: http://securityresponse.symantec.com/ [20]

URL: http://wtc.trendmicro.com/wtc/ [21]

- Invest in audit software and perform audits regularly on the network.

A good investment to protect your enterprise from intellectual property theft as well as maintaining licensing compliance may be software that performs auditing. A good tool will allow auditing to be performed over the network as opposed to manually visiting every machine, making it very easy for the administrator to execute. The auditing information is then gathered into a central database. This information can then be used to verify if any users have these P2P programs on their desktop to begin with, as well as inform you of any illegal software or music that may also exist on their machine. Most allow you to generate reports that may be used to easily keep track of the task at hand. An important note to remember is to perform audits regularly in order to assure that compliance is being maintained. Caast has a link on their website to a program called GASP, which is located at:
URL: http://www.caast.com/audit_tools/ [22]

Conclusion

These are just a few general suggestions to be considered. Unfortunately, each individual program has issues unique unto itself, which could definitely be further analyzed. The intent within this paper was to provide the reader with an overview of the problems that exist with all peer to peer software – bar none, and to show why it has no place within the enterprise.

Citations

[1] Wirednews."Napster's Not Up (or Down) Yet". July 19,2001
http://www.wired.com/news/business/0,1367,45364,00.html

[2] Cisco Tech Notes."Context-Based Access Control: Introduction and Configuration". Jun 18, 2002
http://www.cisco.com/warp/public/110/32.html

[3] Gnutella News. "Gnutella & Firewalls". May 21, 2000
http://www.gnutellanews.com/information/firewalls.shtml

[4] Symantec Security Response."W32.Benjamin.Worm". July 19, 2002.
http://securityresponse.symantec.com/avcenter/venc/data/w32.benjamin.worm.html

[5] Singer, Michael. Siliconvalley.Internet.Com. "Benjamin Worm Plagues KaZaA". May 20, 2002.
http://siliconvalley.internet.com/news/article.php/3531_1141841

[6] Symantec Security Response."W32.KwBot.Worm". June 19, 2002.
http://securityresponse.symantec.com/avcenter/venc/data/w32.kwbot.worm.html

[7] Symantec Security Response."W32.HLLW.Kazmor". June 25, 2002.
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.kazmor.html

[8] Good, Nathaniel S.; Krekelberg, Aaron. HP Labs Technical Reports. "Usability and privacy: a study of Kazaa P2P file-sharing". June 13, 2002.
http://www.hpl.hp.com/techreports/2002/HPL-2002-163.html

[9] Harrison, Ann. Network World. "Watch out: The RIAA is watching you".
April 15, 2002
http://www.nwfusion.com/newsletters/fileshare/2002/01311294.html

[10] Caast. "Canada Losing Millions to Software Piracy". Jun 10, 2002
http://www.caast.org/release/default.asp?aID=74

[11] Caast. "Truce Campaign".
http://www.caast.org/truce/

[12] Caast. "Canadian Alliance Against Software Theft Announces Deployment of Mediaforce Online Anti-Piracy Services". Jun 19, 2002
http://www.caast.org/release/default.asp?aID=76

[13] Mediaforce. "MediaSentry". © 2002 MediaForce, Inc., All Rights Reserved.
http://www.mediaforce.com/services/mediasentry.asp

[14] Nowbox. "Privacy Policy".
http://www.nowbox.com/privacy_policy.html

[15] WhenU.com. "About Savenow".
http://www.whenushop.com/about_savenow.html

[16] Coursey, David. ZDNet Anchordesk. Brilliant responds: Now YOU be the judge.
April 9, 2002
http://www.zdnet.com/anchordesk/stories/story/0,10738,2860521,00.html

[17] Douglas, Jeanne-Vida. ZDNet Australia. "Bermeister's way: Altnet's plans for P2P technology".
http://www.zdnet.com.au/newstech/ebusiness/story/0,2000024981,20265404,00.htm

[18] Altnet. Users. http://www.altnet.com/users.asp

[19] UKERNA.Janet-Cert. November 2001
http://www.ja.net/CERT/JANET-CERT/prevention/peer-to-peer.html.

[20] Symantec Security Response."Security Response".
http://securityresponse.symantec.com/

[21] Trend Micro. “Trend World Virus Tracking Center”.
http://wtc.trendmicro.com/wtc/

[22] Caast. “Audit Tools”.
http://www.caast.com/audit_tools/