Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Submitted by: Wei Heong YAP
30th November 2003

Review on P2P Security and Future

Table of Content

Abstract

"P2P" a word that is not foreign for most of the people in the cyber world. P2P is a powerful tool and fast gaining popularity among the virtual world. It is gaining popularity as it is easily available, cost free and the ease of installation. With a few click away, you are ready to be part of the digital sharing community. P2P recently becomes famous in the music and entertainment industry, as user starts to utilize it as a new way to share music files and movie. In view of the rapid growing trend, security of P2P has turned to an important aspect and raising concern among the users and the corporate world.

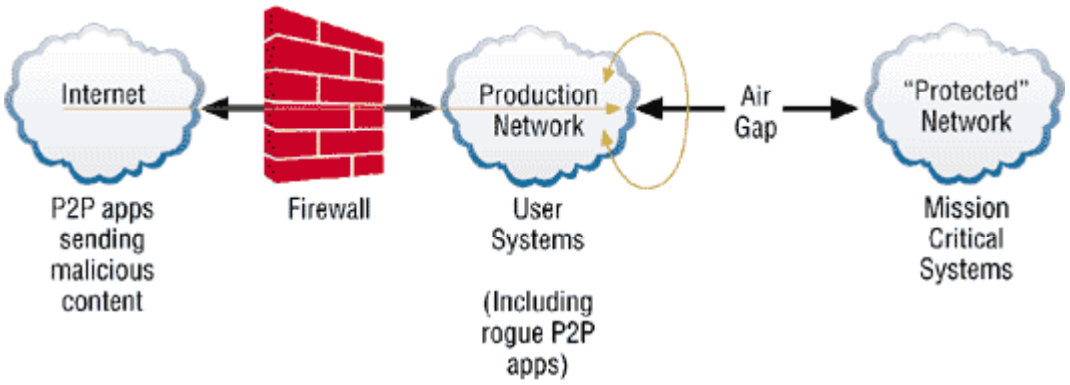
This research paper will put in plain word of how P2P works, its search engine, types of P2P network. It also aims to reveal the potential risk on the security aspects that are faced by the users, the implication to the corporate world as well as academy arena. In addition, this research paper will also discuss the possibility of P2P being exploited for the unauthorized access to the security system, actions to be taken to prevent the unauthorized access, the advantages and disadvantages of P2P implementation and the changes to the virtual world being driven by P2P.

1.0 Introduction - P2P and Security[1]

With the technological advancement in the telecommunication arena, broadband connection within general public has become common in most of the developed nation. As most of the network carriers anticipate the increased adoption of broadband connection, many undersea cables have been laid to better prepare for the increasing demand of the "bandwidth". Today the world has heavily relied on the convenient of "one click away".

Other than shopping online, a new trend has started such as sharing of document, software, picture and most of the things that they are able to digitize online. What is the technology that enables the exchange or sharing of the information globally? Ironically the answer is Peer to Peer (P2P).

In order to ensure the exchange or sharing of information globally being done in the most secured mode, security plays an essential role. The need of security becomes critical especially when there is corporate fraud and loss of revenue as a result of the attacks on their internal networks. The below diagram illustrates the gaps in security when using P2P applications. The security of the secured network is in jeopardy.



[2]

Figure 1: The gaps in the security when using P2P applications

Hence apparently P2P security should be carefully taken care of in order to ensure the invulnerability of the P2P applications. At this moment, security remains the major issue for the continual growth of the P2P. To enable P2P to reach its full potential, users' confident in the ability in the security measurement being utilized to protect them is vital. [3]

[1] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[2] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[3] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

"*Security is a social phenomenon we live with everyday of our lives*"[4]

[4] Bill Yeager, p.16, http://www.jxta.org/docs/p2psecurity.pdf

And 2.0 Definition of P2P

Today, P2P has become a common term for everyone to describe the system that they are having. Naspter, MSN Messenger and Yahoo Messenger claim themselves to be P2P; the labeling of P2P has become a popular trend. Nevertheless there are still groups of people who do not agree with the labeling of the P2P by those companies. For example, there is debate going on for Naspter whereby it is not P2P due to the connection is through a mediated server. Hence if the mediated server is defined as P2P, the argument will go on whereby phone system, email system and all the appliances that work together shall be classified as P2P as well.

As such, below are some extractions of P2P definition from the Internet to provide an overall picture of P2P.

2.1 According to Whatis.com, P2P is "A communication model in which each party has the same capabilities and either party can initiate a communication session. So we could define P2P as direct communication or collaboration between computers, where none are simply client or server, but all machines are equals – peers. [5]

2.2 Peer-to-peer or also known as "Person-to-person" in layman term is a communications model in which each party has the same capabilities and either party can initiate a communication session. Other models with which it might be contrasted include the client/server model and the *master/slave* model. In some cases, peer-to-peer communications are implemented by giving each communication node both server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server. IBM's Advanced Peer-to-Peer Networking (APPN) is an example of a product that supports the peer-to-peer communication model. [6]

2.2 On the Internet, peer-to-peer (referred to as P2P) is 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. Napster and Gnutella are examples of this kind of peer-to-peer software. Corporations are looking at the advantages of using P2P as a way for employees to share files without the expense involved in maintaining a centralized server and as a way for businesses to

[5] Andrew B, Tarun, Andrew C, Bob, p.1(http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p1.html)
[6] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html

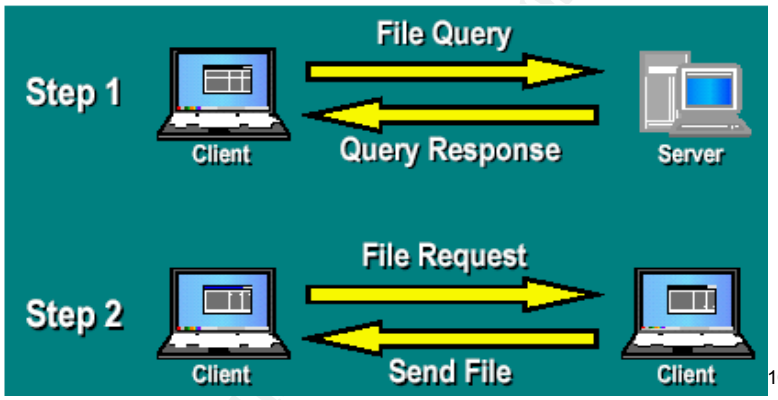
exchange information with each other directly. [7]

"P2P is really just an umbrella covering five areas: file sharing, distributed computing, web services, messaging, and gaming. P2P is not a technology; it is a mindset."[8]

Referencing to all the explanations as stated on P2P, apparently it is really hard to define what is or what is not P2P. As for this research paper, in order to define P2P, the assumption will be made as 2 computers of the same capabilities and resources to perform the same function both as a server or client which is connected directly or indirectly through an intermediate server to perform certain function such as file sharing, messaging and etc.

The example of the 5 components of P2P technology is as follows: [9]

a. File Sharing: P2P file sharing basically enable the capability to share the files over the Internet. It has gained the popularity as the file sharing activities had been dramatically increased between the Internet users to enable a faster delivery of messages or information. For example, Naspter, KazaA and Morpheus are those who do provide the file sharing capability. The below figure is showing the Napster Model for the P2P file sharing.



[10]

Figure 2: Napster Model

b. Distributed computing:P2P distributed system sharing computing power, application and resources across the network. The examples are Distributed.net, Seti@home. Figure 3 illustrates the distributed computing/processing. [11]

[7] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html
[8] Jon Orwant, http://www.openp2p.com/pub/a/p2p/2001/03/27/orwant_security.html
[9] http://www.howstuffworks.com/search-engine.htm
[10] Matt, Gibbs, p.2, http://www.hill.com/archive/pub/papers/2003/03/paper.pdf
[11] Matt, Gibbs, p.7, http://www.hill.com/archive/pub/papers/2003/03/paper.pdf

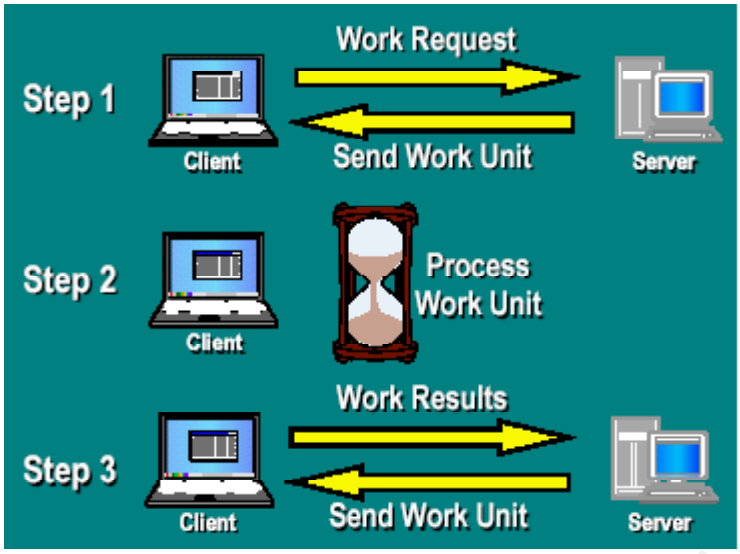


Figure 3: Distributed Computing/Processing

c. Web services: This is an architecture that allows application talking to each other. For example: furnishing of a stock quote, checking on a bid on an auction item online.

d. Messaging: This component allows the users to exchange text, voice, files and messages instantly. The examples are MSN Instant messenger, Yahoo Messenger, AIM as well as ICQ.

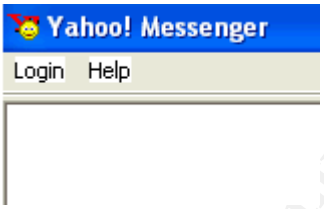


Figure 4: Example of Yahoo Messenger which allows instant exchanging of messages.

e. Gaming: All time famous computer game such as, Counter Strikes, Star Craft and Warcraft. These are game that request user to be connected to a central server to play the online game together.

3.0 Definition of Search Engine in General[12]

Before we start to explore on how the P2P search function work, let's take a step backward, to see how the search engine in the World Wide Web (WWW) works. The World Wide Web figuratively consists of more than billions of web pages, which span across thousand and thousand of servers.

In view of the humongous size of the World Wide Web, it makes it impossible for one to examine and go through the web pages to get information readily. That's why search engine is here to work this out for you. The main "brain" of search engine is called "Spider", which will roam through all the web pages and follow the hyperlink from one document to another to extract the textual information and form a correlated database which consists of the keyword of the web pages for searching purposes.

Most of the search engine today is no longer searching the web directly to obtain the search result. They rely on their central database to feedback to user with the search result. Having said so, we can expect lots of web pages that are still invisible to the spider. Figure 5 illustrates one of the examples of search engine architecture. [13]

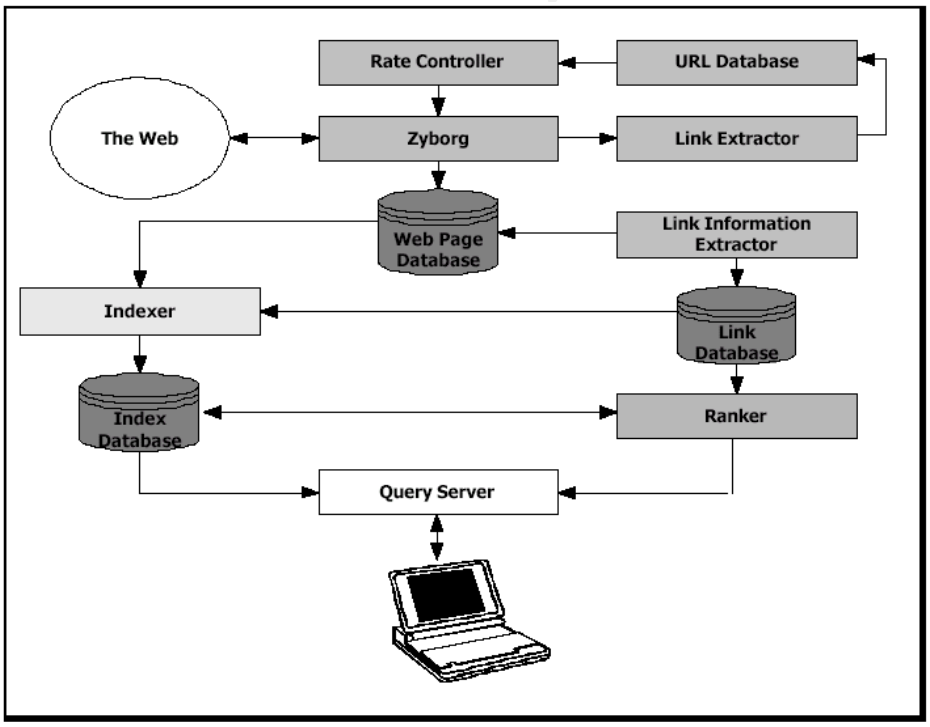


Figure 5: The WiseNut Search Engine Architecture

[12] http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p8.html
[13] http://www.wisenut.com/pdf/WISEnutWhitePaper.pdf

4.0 P2P Search and Discovery Methods[14]

After talking so much about search engine in the World Wide Web, it is time to dive into the search function within P2P. There are many discovery methods being used by the P2P system. For this research paper, we are going to reveal the major 6 categories as follows:

1. Flooding broadcast of query
2. Selective forwarding system
3. Decentralized Hash table networks
4. Centralized index and repositories
5. Distributed index and repositories
6. Relevant driven network crawlers

We will discuss in detail on how those discovery methods work.

4.1 Flooding broadcast of query

Any peer within the P2P network which sends out a query will be broadcasted to the entire peer. If the immediate peer is not able to answer the query, it will proceed to forward the query to its neighbor. It goes on and on until the TTL expired, than the query will be dropped. This type of discovery method does not scale well; as it will quickly run into network saturation as the number of peer connection grow. Therefore, it is only suitable to run across small network.

4.2 Selective forwarding system

Comparatively selective forwarding system is more scalable than flooding broadcast system. A super peer will be selected among the peers, the selection is based on the processing power and bandwidth of the particular peer. If it found that the host processing power and bandwidth is within the requirement, automatically the host will be elected as the super peer. A super peer will be acting as an index directory to reduce the main server processing time and bandwidth consumption. As the super node will be acting like a subset of the main server, most of the P2P network allows their peer to decide whether they wish to participate to be a super node.

4.3 Decentralized Hash table network

Decentralized Hash table networks use a unique ID to identify resources or files within the peer network, regardless the size of the network. It will still be able to locate for the files in the speed in light. However, due to the fact that, the resources are uniquely identified by key, it makes it impossible for searching through keyword or fuzzy. So, in order for a peer to search for a file from one another, they must first obtain the key that uniquely identify the file.

These systems are also subject to malicious activities by peer with ill intention. They may discard the query and send large amount of unsolicited data to clutter

[14] Ed, Michael, Richard, Rob, Sean, p.8, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html

the key space. Or they may flood the network with large amount of queries to degrade the performance of the systems.

4.4 Centralized index and repositories

Napster used Centralized index and repositories system, basically, all peers and resources information is stored within the centralized main server. It will be serving as a single point of reference to locate files. When a query is being sent to the server, it will go through its index and determine whether there is a match. If it matches, it will send the result back to the query sender peer of where it can retrieve the file.

So far, this system works very well in the P2P environment, however the maintenance of the system is expensive. This is due to it required large processing power, storage space and bandwidth to support large base of customer.

There is also risk of single point of failure for the system as Centralized server did the entire job for searching and storing information. However, Naspter uses cluster to minimize the risk, as it will failover to the next server should problem occurred.
Recent court rulings cast a serious doubt about using a centralized server to index resources in the peer to peer based network, the legal precedent requires such type of system to monitor the usage and activity of the system to ensure that no infringement of copyright occurred within the network. To monitor and enforce the requirements is challenging with the size of the network, and it might have too much unpredicted risk involved.

4.5 Distributed index and repositories

The system gets rid of the expensive centralized server, whereby it works like the “super-node” concept. Decentralized node will store the some portion of the index locally, the index includes information about itself and some of the neighboring peers. When the super node receives a query, it will go through its local index to determine whether there is a match, if no match found, it will forward the query according to its local index to the next possible super node that might be holding the information.

It eliminates the risk of single point of failure, as if we lost one of the super nodes, we are only losing a small portion of the index, thus the system will still be functioning properly. This is a strong contrast as compared to the centralized server.

If a file was changed by peer locally, the peer that is storing the index locally might not be aware of the changes, hence it might provide a requester with outdated information. As peer joins and leaves the network, the system might be losing some of it indexes too; this remains a great challenge for the distributed based system.

4.6 Relevant driven network crawlers

This is a totally different approach of carrying out the search. Instead of performing query based of peer request, it uses database that the peer accumulates overtime to determine whether the resources being found might be of interest to the peer.

After a period of time, the information that user accumulates will be used to determine the common element that is relevant to the peer. The crawler will traverse network to search for information, which matches the peer profile based on the previous information.

5.0 Types of P2P Network[15]

There are three major types of P2P network as follows:

5.1 Pure P2P

5.1.1 Peers act as clients and server

5.1.2 There is no central server.

5.1.3 There is no central router.

5.1.3.1 Every node is a Peer. It is a total democratization of the peer group nodes. There are two routing structures – one which is on the distributed catalogue and the other is on direct messaging.

Below is the graphical representation of the Pure P2P. [16]

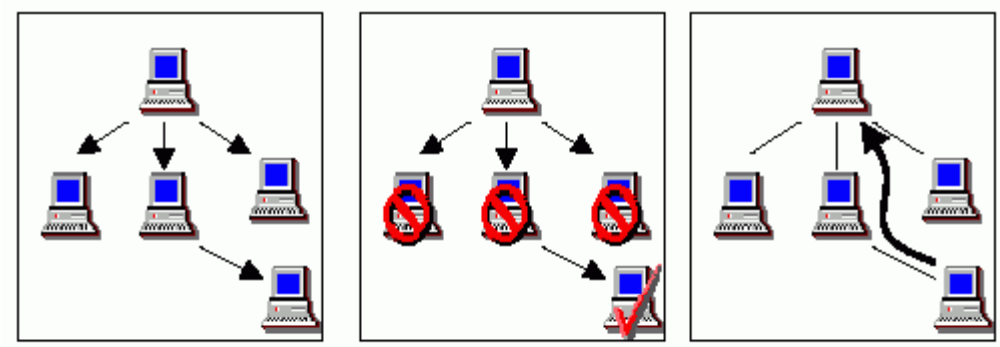


Figure 6: Pure P2P

5.2 Hybrid P2P

5.2.1 Has a central server that keeps information on peers and responds to requests for that information.

5.2.2 Peers are responsible for hosting the information as the central server doesn't store files, for letting the central server know what files they want to share and for downloading its shareable resources to peers that request it.

5.2.3 Route terminals are used addresses, which are referenced by a set of indices to obtain an absolute address.

Figure 7 illustrates the hybrid P2P. [17]

[15] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html
[16] http://wiki.cs.uiuc.edu/cs427/Major+Forms+of+P2P
[17] http://wiki.cs.uiuc.edu/cs427/Major+Forms+of+P2P

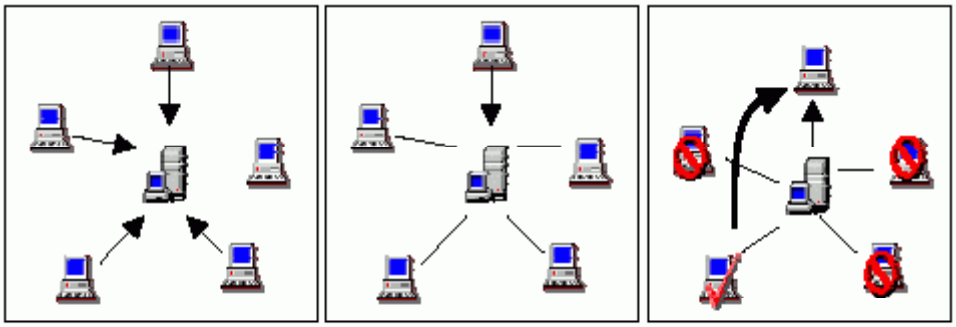


Figure 7: Hybrid P2P

5.3 Mixed P2P

5.3.1 Has both pure and hybrid characteristics. In fact for both pure P2P and hybrid P2P are extremes, thus Mixed P2P is introduced to serve as the middle ground that involves both server and the peer to provide adequate independence.

Below figure is describing the Mixed P2P.[18]

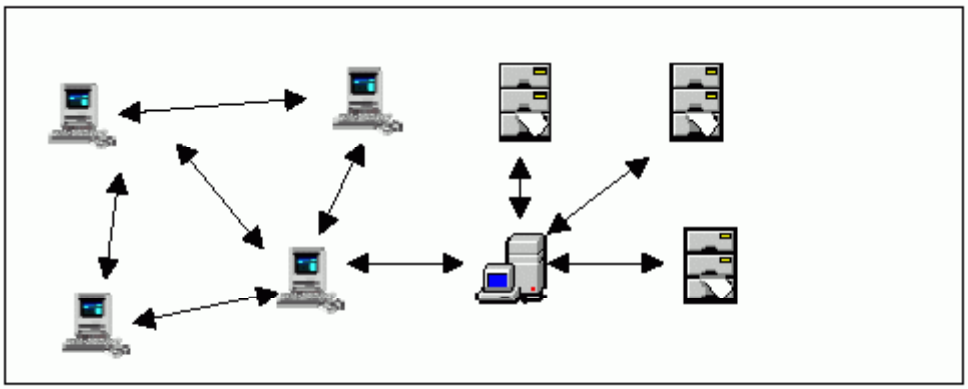


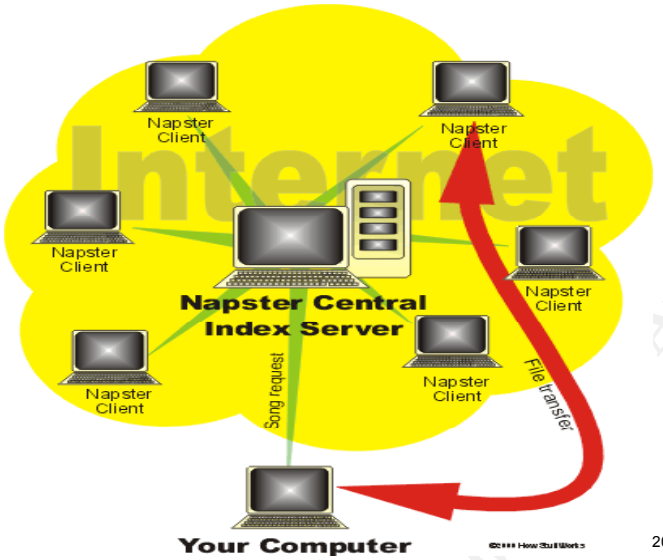
Figure 8: Mixed P2P

[18] http://wiki.cs.uiuc.edu/cs427/Major+Forms+of+P2P

6.0 Example of P2P Applications

In order to further elaborate on the type of P2P networks, this research paper will illustrate 2 examples of the P2P applications. Naspter and Gnutellanet will be further discussed as the 2 P2P systems to enhance the understanding how the P2P applications work to accomplish the various objectives such as file sharing, messaging as well as web services.

6.1 How does Napster work? [19]



20

Napster is an example of a hybrid P2P system. Napster has a centralized directory (actually several) that describes how files reside in Napster and each host registers with this directory when they join the network. The centralized directories therefore have the IP addresses, the names of the files the hosts want to share and other data stored about each computer system connected to it. [21]

1. Users, who wish to use Naspter, must first install the software. Once the software is installed and executed, it will check for network connection.
2. If the software is able to detect network connection, it will establish connection between the client and one of the Central index servers.
3. Central index server, store information of all the connected clients, information such as IP address of the client, login username, bandwidth, ping number file size of the files shared will be stored in its database.
4. User will send request of the file that they wish to find to the Central Index server.

[19] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html
[20] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html
[21] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html

5. Central Index server will go through his database to locate for file for any matches.
6. If there are matches, Central Index server will send the list of matched (if any) which include information like the IP, username, ping number, file sizes and bit rate to the user.
7. User will then choose from the matches list for the desirable file that they wish to download and the client will attempt to establish a direct connection with the designated client that user chosen. The client tries to initiate the connection by sending its own IP address and the file that it wish to download.
8. Once the connection has been established, the client who has the files will be acting as a host and the host will transfer the file to user.
9. Connection will be broken by the host computer, once the transfer is completed.[22]

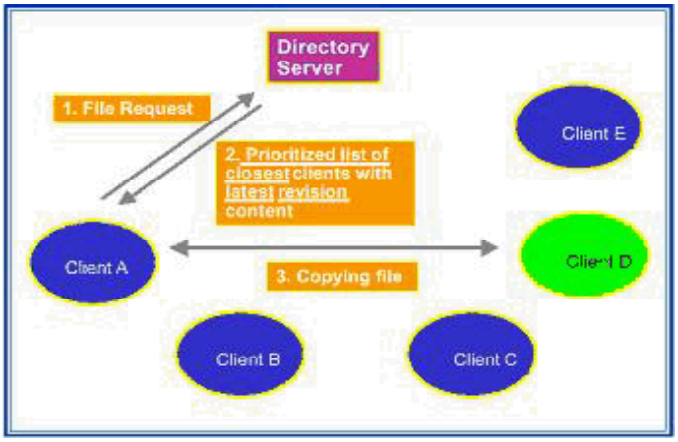
Users can choose how many member connections to seek at one time and determine which files they wish to share or password protect.

6.2 How Does Gnutellanet P2P Work?

In beginning of this paper, we explain that there are a few systems out there that are available to general public user which wish to be part of the P2P community. Gnutellanet is one of the classic examples of P2P. So let's take a look on how Gnutellanet works.

The user must first download and execute a peer-to-peer networking program. (Gnutellanet is currently one of the most popular of these decentralized P2P programs because it allows users to exchange all types of files.) After launching the program, the user enters the IP address of another computer belonging to the network. (Typically, the Web page where the user got the download will list several IP addresses as places to begin). Once the computer finds another network member on-line, it will connect to that user's connection (who has gotten their IP address from another user's connection and so on).

[22] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html



[23]

7.0 Potential Threats to P2P Network[24]

In view of the popularity of the P2P in the internet world, a lot of virus and worm has been written by the "black hat" that will exploit the P2P vulnerability to further utilize them as a way to get personal information, backdoor to gain access corporate services. Academy is also facing challenge as the increase usage of the P2P application, which most of the time student is downloading movie, song and graphic over the internet. This has generated tremendous traffic which might cripple the university network and brought down the system.

7.1 Fertile place for Virus and Worms to grow

Recently, a number of P2P installation software for Audiogalaxy has been found infected by Nimda virus. It is not clear how does this installation software get infected. Nimda virus can spread through email, flaw in Internet explorer and open file sharing environment. Nimda is a virus that not only affecting webserver, but any user PC that is running any version of windows. Once the system is infected. It will attempt copy itself into all the HTML files. Nimda can re-infect a system easily, even if the system is properly patched, this is due to the propagation can be done, especially if user visit a infected site and they are using a vulnerable version of internet explorer.[25]

"Benjamin" a worm that first hits KazaA user, full name of the worm is W32.Benjamin. It is spread through KazaA online file sharing. This virus will convert infected host into a KazaA server, with minimum damage to infect host but the worm will alter the registry of the system and dumps the sys32 folder in to the windows temporary folder. That folder will contain rich media file which will be used as a lure to other online user to download it and get infected. The process then will be started all over again. But the exponential grow has worried most of the security expert. So far, this worm is only infecting KazaA user and the infected rate is relatively low. According to one of the writer of the worm, this

[23] Susan, Elaine, AnneMarie, David, Charles, p.4, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html
[24] http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[25] http://www.unwantedlinks.com/Guntella-alert.htm

virus is only targeting those who try to download copyright material as well as users who try to download child porn via online. [26]

According to Techs report on July 9, 2002, a virus by the name of backdoor .K0wbot.1.3.B infecting KazaA user who unknowingly downloads the infected file. Backdoor also infected user through IRC remote control backdoor component, that's why it was given the name "backdoor". Once the system is infected with backdoor virus, it will gain control of the system, by having the control, it will update the virus itself to a newer version, report out the system information like CPU speed, memory, operating system version, uptime, Internet connection type, local IP address, software installed on the system. Backdoor virus will also execute IRC command to flood other users in chat room.

A quote from the virus researcher show that P2P might form a paradise for virus writer

> "This backdoor is the second virus to successfully attack the popular network in less then two months," said Began Dragu, virus researcher at BitDefender. "Following this trend, peer-to-peer file-swapping networks could soon become a paradise for any virus writer." [27]

P2P networking allows your "secured" network to open up for attack, espionage and malicious mischief. P2P itself actually does not bring any new threats to the network, but the novel threat, Worms and virus attacks.

As it is so easy to set up a P2P file sharing system, employee within a company can easily download file across the internet. If an infected file was downloaded from the P2P network, it will bring potential harmful virus or worm into the corporate environment, which may in turn lead to leak of confidential information. This is due to the worm might plan a backdoor within the company computer system, which will not be detectable by the company firewall rule set or possibly computer services disruption. Hence the virus or worm might perform destructive activities including the deletion of important information, bringing down the server or network services.

7.2 Bandwidth clogging and file sharing

Bandwidth clogging will incur if there is inappropriate use of the company resources, e.g. expensive bandwidth that company is subscribing, hard disk space of the computer and so on. Downloading of the rich movie and song files could cause congestion to the corporate network, as the congestion might cripple the network of the company, it will cause potential revenue loss to the company.

---

[26] http://www.techtv.com/news/securityalert/story/0,24195,3385557,00.html

[27] http://www.techtv.com/news/security/story/0,24195,3390306,00.html

7.3 Legal Risk

Also employee could be violating the intellectual property law by downloading some movie or song over the internet. Recent court ruling allows RIAA to make a lawsuit down to the individual who attempts to download or share copyright files. The entertainment industry has taken aggressive step to pursue copyright violators, RIAA seek legal action against ISPs, who provide Internet connection to both the corporations and individuals. The action also pointed to those employers who do not take necessary action to prevent their employees from engaging in file sharing activities. As they believe that company system which most are connected to high bandwidth connection form a good ground for the employees to be involved with the copyright infringed file sharing activities.

As a result of this, company is facing a high risk of law suit, especially so, if the company has a big pool of employees and control of access to file sharing activities becomes more challenging then ever. Some company has decided to put up security policy and some make their staffs sign an agreement to be responsible for their own act if they happened to be one of person which take part in the illegal activities of sharing copyright song or movie.

This agreement is deemed necessary as the legal implication for copyright violation is heavy.

> "In United State, copyright violations carry a maximum penalty of $150,000 per instance, plus punitive cash damages and possibility of imprisonment. In Canada, the offender may be subject to fine of up to $1,000,000 or to imprisonment for a term of not exceeding 5 years. Or to both at the same time." [28]

In view of the heavy punishment, it is really important for corporation and individual to look into the problem seriously.

7.4 Untested Software bug

In order for the P2P file sharing application to work, appropriate software has to be installed. Most the P2P software is available free of charge which has resulted software quality to be questionable in most of the time, contain lots of bugs and loopholes. This software might have conflict with the existing business application and thus causing the system to crash.

7.5 Spyware Trojon

A lot of the P2P file sharing applications was found to be bundled with spyware Trojan or also known as adware. P2P Software Company depends on the advertisement company as a financial resource. Therefore, most of the time they do not have access over the source code of the software and have very little control over what is the function of the bundled software. Even if a user would deny installation of addition to the program as it can be installed through the

[28] http://www.assetmetrix.com/pdf/p2prisk.pdf

backdoor. It also has been reported that, these addition to the program has the capability of changing the system firewall setting to allow itself from accessing the Internet without permission. It is important to understand though P2P software always claims that users who are using their services should anonymous, this is not the case for the spyware that bundled with it. The spyware Trojan is capable of monitoring and transmitting user information over the internet as it has been programmed. Most of the time, user IP address, keystroke activities, information you enter into online form fields will be monitored and transmit accordingly. Sometime it does contain personal and private information about the user. So user privacy is at risk, some sensitive data like your credit card information, internet banking personal identification number (PIN) will also end up at unknown hand. [29]

7.6 Parents

It has greatly raised the parents concern, as with the file sharing in place, children can now bypassing most of the web filter program, which is only catered to filter web contains that is not suitable for children viewing. But all these products are not capable of blocking porn movie or photo being downloaded through Peer to Peer application. Even with the latest development of tool like Cyber sitter which is used by parents to filter and prevent file sharing, so far there are still no software available to prevent only porn downloading from P2P. However, most of the latest version of the P2P software, like KazaA, has already included a filtering control function, which claims to be able to filter off offensive and adult content. Most of the time, children who is searching for game and music over P2P got expose to hard core porn material. Unfortunately, pornographic seems to be here to stay since attempts to restrict online pornography have been repeatedly found unconstitutional.

Some statistic to show the current stage of the P2P application

P2P App	Total downloaded via download.com	Relative Popularity	# of viruses	3rd Party Malware?
Kazaa	240,759,939	47.90%	68	yes
Morpheus	113,014,928	22.49%	14	yes
Imesh	52,262,345	10.40%	10	yes
AudioGalaxy	31,408,240	6.25%	0	yes
BearShare	19,070,465	3.79%	13	yes
LimeWire	15,420,551	3.07%	9	yes
Grokster	8,445,256	1.68%	12	yes
WinMX	6,191,639	1.23%	3	NO
Blubster	3,361,874	0.67%	0	yes
Xolox	2,290,756	0.46%	2	yes
FileNavigator	1,250,260	0.25%		
2 Find MP3	1,217,585	0.24%		yes
EDonkey	920,180	0.18%	12	

[30]

As we can see from the table, it seems that the popularity of the P2P application does in some manner attract more attention of the virus writer. KazaA which with the highest rate of download coincidently has the highest number of virus.

[29] http://www.wired.com/news/privacy/0,1848,49430,00.html

[30] http://www.assetmetrix.com/pdf/p2prisk.pdf

Also most of the P2P softwares bundled with 3rd party malware.

A quotation obtains from website shown that P2P in corporate environments might be at a stage that is quite worrying.

> "A Canadian company has studied P2P software usage in corporate networks and according to the study 77% of companies have a P2P software installed in their network. Companies with over 500+ employees had at least one P2P installation within the company. The study was targeted to companies with more than 10 employees."[31]

In addition to the copyright violation issues, P2P software is also a significant security risk. There are number cases where employees have been sharing valuable corporate data in the P2P network.

The results highlight the potential risks that corporations and individuals run, as the record industry prepares to file potentially thousands of lawsuits against individuals who offer copyrighted materials online.

> "Corporations are frantic about how to rein in some control over this," said AssetMetrix President Paul Bodnoff. "Like with software licenses, most companies want to be on the right side of the law. The challenge is how they do that." [32]

[31] http://www.assetmetrix.com/pdf/p2prisk.pdf

[32] http://www.afterdawn.com/news/archive/4285.cfm

8.0 Why that is a need for security?

During time of economy downturn, everyone seems turning away their attention from the importance of information security into how to generate more profit and maintaining their cost at low level. This has caused some organizations relating information security as an expense that will lower their revenue/profit and thus concluding it as less important element of the IT requirement. Hence the direct impact will definitely be the hindrance factor to the growth of the cyber world. This behavior is commonly demonstrated by the small business entity. As small business entity is vulnerable to the network hacking, this means an indirect endangered to the larger corporation which is having a business relationship with them.

This possible thread is via the need to the larger corporation to open up their firewall to the small business entity in order to perform certain transaction with them over the net. By compromising the host at the small business entity, it increases the chances of the larger corporation get intruded. Till the recent continuous virus and worms outbreak, it has woken everyone on the need to reinforce and tighten the security of their company network as the attack could result in possible revenue loss and worst which affecting the company reputation. Customer will lose confident over doing business with company that does not have information security in place.

For example of company who takes customer credit card information to perform transaction online. Even with the encryption technology that is currently available, it might be not sufficient to prevent people from accessing illegally through tapping on the network. However most of the time, this company tends to store the credit card information within their local server for a period of time to serve the purpose of marketing and statistics. If the company system is not properly secured, hacker might illegally gain access to steal the valuable information through their server.

The need for P2P security is undeniable as company information plays an important role as the asset of the company. Any information leakage or misuse of the confidential information will definitely cause a jeopardy to the company profile as well as revenue. Thus a serious consideration and measurement should be in place for the P2P security.

9.0 What should we do to reduce the risk?

9.1 Individual

As individual, we must aware the risk that we are facing for downloading files and software through P2P application. All the files are not guaranteed to be virus or worm free. If you would like to get a freeware, it will be recommended to go through site like download.com, which gives you certain level of protection that you are getting a freeware that you required, without additional code attached to it.

We must not make P2P a place to exchange copyright software, movie or song. Other than, infringement of copyright, this increases the chances of one getting infected by viruses and worms, as most of the virus writer will make use of the chances to create virus that pretend to be one of the copyright file that you intend to download. Once you have download and execute it, your PC will be infected.

Malware will be bundled with most of the P2P application. It might be performing activities of which user did not permit. Individual must first go through the download agreement of the software before installing the software into your PC. Most of the time, the software agreement will indicate about the malware that is bundled with your P2P software. Even if the agreement does not mention about the function of the Malware, it will be good to know about the name of the Malware and do some research on what level of security you would have to scarify to install the software.

It is important to bear in mind that, P2P software if not configure properly, it might expose your entire hard disk to the whole Internet world. Sharing of the file is running background until you shut it down completely.

In order to tighten the security of our PC, personal firewall should be installed, so that we are aware of any application that is trying to gain access to the internet without our knowledge.

9.2 Corporation

Corporate system environment often contains sensitive information, hence it is extremely important to make sure that information system in corporate environment is properly secured. P2P software is developed and bundled with unknown Malware, most of the time it is not suitable to run in a corporate environment. But it is difficulty for either big or small company to ensure that their system will be free from P2P software, the big challenge for Medium and Small Corporation is most of the time they do not have a centralized IT department to look into the possibility of user installing P2P application and they do not have someone monitoring their network usage. They are totally relying on the user to perform their own maintenance of the PC. So it is important to educate the user of the potential harm that they could bring to the company,

should they use P2P application within the office environment. It will be good to get the user to sign agreement that he or she will be responsible for his own act, if they choose to run the software and run into legal issue, as a result of copyright issue. Company will then able to lower their risk of being sued.

Large corporation most of the time have their own IT department to oversee the IT system in the corporation. They might be equipped with the network monitoring tools and some software management tools to have a better picture of what is installed in a PC. These give them a better control over the maintenance of the system. Network usage can be monitored for any abnormality, if they see a sudden spike. They can always filter out how is the top 10 users of their network, and it should be easily caught by the IT people, as most of the time P2P user tend to download rich movie and song file. Company firewall policy must always block the port that is common to P2P applications. Even though some of the P2P application is capable of using the standard port that is open by firewall to initiate connection, it lowers the possibility of use connecting to P2P application through the default P2P sharing port.

All PC should be installed with antivirus software and ensure that the virus definition is always up-to-date. This can be enforced by central IT department, all system should be monitored the software management system and to perform necessary push of virus definition to user as needed. System maintenance should also be restricted to the administrator only. This will mean common user should not have the right to install any software to their system.

10.0 The Future of P2P Security[33]

P2P security is frequently associated with “trust”. The trust has to be established with the users who we interact with and the trust with the software suppliers who provide the applications as well as the business partners. The development of P2P is strongly driven by the sense of security or trust level viewed by the community.

Users Gaining Their Own Trust[34]
One very interesting idea recently proposed, is that of users gaining trust within the P2P community. All users would be assigned a unique digital signature, like IP, but per user and not per machine. Associated with this digital signature would be a level of trust. Depending on a users behavior in the past, their trust level would either be promoted on the grounds of valid use of the network, of demoted with acts of malice and misuse.

It is being proposed that the users trust level would rather begin at a relatively low level to combat unwanted users creating new accounts and thus abusing the new trust level. In order to get the trust level to be pushed up to another level, users will have to be active on the network for a certain period.

This idea might not be working fine as in reality, people will find all means to uncover the flaw of this security system and try to hack into some other person’s account which is having higher trust level and act as the owner of the account.

Biometrics[35]
Biometrics involves the use of a person’s unique characteristics to authenticate them. Traits that are commonly utilized include a person’s facial image, signature, fingerprint or retinal pattern. One key feature of biometrics is that the user is no longer required to remember any passwords or store any key data, a major weakness in conventional authentication systems.

Ultimately, the technology could find its strongest role as an integrated and complementary piece of a larger authentication system, perhaps in combination with the cryptographic certificates mentioned above, rather than a stand-alone single point of defense. [36]

[33] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[34] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[35] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
[36] Declan, Jarlath, Keith, John, Dan, p.10, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

In the future, biometrics is foreseen by many experts to play both key roles to enable public key infrastructure deployment, thus protecting public and private keys and residing in smart card technology in line to the effort to support personalized e-commerce.

11.0 Conclusion

If there are advantages, there will be disadvantages. P2P can be a benefit to IT world provided it is being used wisely. Apparently, P2P file sharing has been regarded as a way to exchange copyright software, movies and songs. This created a negative impact to the P2P, as it is now notorious to the entertainment

industries. It also created an environment for the virus writer to test on their virus. Parents are worried that their kids will be in contact with inappropriate contents. However if it is used in a proper way, it will certainly bring convenient to the general public. P2P can be used as a good way to locate for freeware, article which user wishes to share with the world. It will apparently making searching of information much easier.

Security is a process rather than a product, some company thinks security carries the meaning such as firewall, traffic analyzer, software management tools and etc. With all these tools being put in place, security will no longer pose a concern to the company. This is a wrong perception as security besides the tool, the need to define rules set to ensure the equipment work properly is also important. This means all procedures have to be in place and monitoring to ensure all the users are strictly following the procedures. To create the awareness, users must be educated about the possible impact P2P application to the corporate environment, e.g. leakage of company product plan or blue print could cause revenue loss or even loss of company pioneer position in certain arena. It will have chain reaction to the employee, as the company might face a crisis as a result of the information leaked.

To conclude, P2P really changes the way people use Internet. With P2P in place, bandwidth demand has surged to a new high. Users no longer rely solely on physical media to transport the data, files but exchange of information can be done electronically with the digitize capability. Large files are now transferred across the Internet with the technological advancement. Thus the pros and cons of P2P are heavily relying on whether the users are using it in proper manner or misuse it for the ill intention.

Reference

1. Peer to Peer – a searchNetworking definition - URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html

2. OpenP2P.com – P2P concerns miss the P2P point – URL: http://www.openp2p.com/pub/a/p2p/2001/03/27/orwant_security.html

3. Howstuffworks "How Internet Search Engines Work" - URL:
http://www.howstuffworks.com/search-engine.htm

4. Howstuffworks "How napster worked" - URL:
http://www.howstuffworks.com/napster2.htm

5. Serious P2P file sharing security concern - URL:
http://www.unwantedlinks.com/Guntella-alert.htm

6. TechTV | KazaA worm target users. – URL:
http://www.techtv.com/news/securityalert/story/0,24195,3385557,00.html

7. TechTV | Second virus Hits KazaA Users – URL:
http://www.techtv.com/news/security/story/0,24195,3390306,00.html

8. What They Know Could Hurt You - URL:
http://www.wired.com/news/privacy/0,1848,49430,00.html

9. OpenP2P.com: What is P2P… and what isn't [Nov 24, 2000] – URL:
http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html

10. The P2P report – Knowledge Management Research Center –CIO – URL:
http://www.cio.com/research/knowledge/edit/p2p_content.html

11. Wired News:This is your deep link on P2P – URL:
http://www.wired.com/news/politics/0,1283,57230,00.html

12. P2P hide and seek | CNET News.com
http://news.com.com/2100-1025_3-5051627.html

13. Fastrack P2P supernode packet handler buffer overflow vulnerability –URL:
http://securityresponse.symantec.com/avcenter/security/Content/7680.html

14. P2P usage still popular in corporate environment.
http://www.afterdawn.com/news/archive/4285.cfm

15. Wired News: RIAA wants to hack your PC.
http://www.wired.com/news/conflict/0,2100,47552-2,00.html

16. Corporate P2P (Peer to Peer) Usage and Risk analysis
http://www.assetmetrix.com/pdf/p2prisk.pdf

17. Declan, Jarlath, Keith, John, Dan, p.10,
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

[18.] Bill Yeager, p.16,
http://www.jxta.org/docs/p2psecurity.pdf

19. Andrew B, Tarun, Andrew C, Bob, p.1
(http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p1.html)

20 . Matt, Gibbs, p.2,
http://www.hill.com/archive/pub/papers/2003/03/paper.pdf

21. Wisenut search engine white paper, Sept 2001
http://www.wisenut.com/pdf/WISEnutWhitePaper.pdf

22. Ed, Michael, Richard, Rob, Sean, p.8,
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html

23. Major Forms of P2P
http://wiki.cs.uiuc.edu/cs427/Major+Forms+of+P2P

24. Susan, Elaine, AnneMarie, David, Charles, p.4,
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html

25. Declan, Jarlath, Keith, John, Dan, p.10,
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

26. P2P Search Engines URL:
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p8.html

27. P2P Security URL :
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html