PEER-TO-PEER NETWORK SECURITY

Mrs. PADMAPRIYA .G (M.SC., M.PHIL)

Rathinam College of Arts and Science, Coimbatore, India.

ABSTRACT: *Peer to Peer networks in general refers to the setup in which all computers have equal status. In other way, this allows communication between two systems, where each system is considered equal. Peer-to-peer networking is an alternative to the client-server model. Under the peer-to-peer model, each system is both a server and a client, commonly referred to as a servant. Recently, however, peer- to- peer networks have gained momentum with searchable peer-to-peer network file databases, increased network connectivity, and content popularity. In this article, will discuss the malicious threats, privacy concerns, and security risks of three common peer-to-peer network systems.*

The threats discussed will include how these can harness existing peer-to-peer networks, and how peer-to-peer networking provides an additional (potentially unprotected) degree of delivery for malicious code. Each protocol will be discussed, as well as the advantages and disadvantages of such models in regard to privacy and potential security risks by their usage. Many other peer-to-peer networking systems exist (for example, Microsoft Networking), and while this is explicitly discussed, conclusions can be applied to these systems as well.

I. INTRODUCTION

Peer to peer networking has created tremendous interest worldwide among users. Many of the business units have promoted "peer to peer" technology as the future of Internet networking. Peer-to-peer well known as P2P is an alternative network model to that provided by traditional client-server architecture. P2P networks use a decentralized model where each machine, referred to as a peer, functions as a client with its own layer of server functionality1. A peer plays the role of a client and a server at the same time. That is, the peer can initiate requests to other peers, and at the same time respond to incoming requests from other peers on the network.

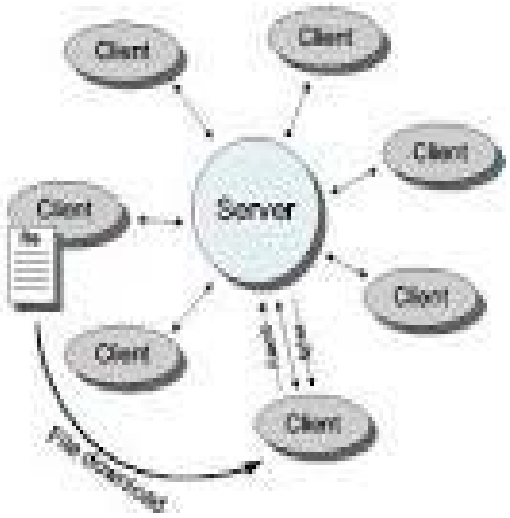
It differs from the traditional client-server model where a client can only send requests to a server and then wait for the server's response. With a client-server approach, the performance of the server will reduce as the number of clients requesting services from the server increase. However, in P2P networks overall network performance actually improves as an increasing number of peers are added to the network. These peers can organize themselves into ad-hoc groups as they communicate, collaborate and share bandwidth with each other to complete the tasks at hand (e.g. file sharing). Each peer can upload and download at the same time, and in a process like this, new peers can join the group while old peers leave at any time. This dynamic re-organization of group peer members is transparent to end-users.

Another characteristic of a P2P network is its capability in terms of error-tolerance. When a peer goes down or is disconnected from the network, the P2P application will continue by using other peers. For example, in a Bit Torrent system, any clients downloading a certain file are also serving as servers. When a client finds one of the peers is not responding, it searches for other peers, picks up parts of the file where the old peer was, and continues the download process. Compared to a client-server model, where all communication will stop if the server is down, a P2P network is more fault-tolerant. A P2P network implements search and data transfer protocols above the internet protocol.

A peer-to-peer (P2P) network in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system.

II. ARCHITECTURE

A peer-to-peer network is designed around the idea of equal peer nodes simultaneously functioning as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server. A typical example of a file transfer that uses the client-server model is the file transfer model (FTP) service in which the client and server programs are different: the clients initiate the transfer, and the servers satisfy these requests.



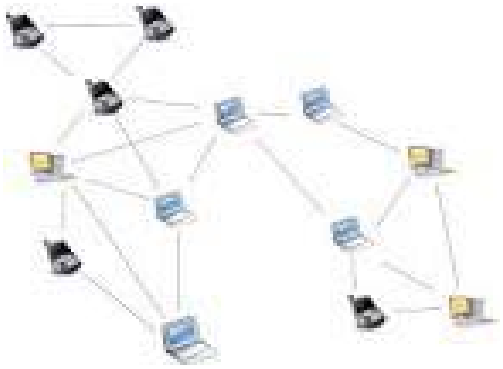
1.1, Routing and resource discovery

Peer-to-peer networks generally implement some form of virtual overlay network on top of the physical network topology, where the nodes in the overlay form a subset of the nodes in the physical network. Data is still exchanged directly over the underlying TCP/IP network, but at the application peers are able to communicate with each other directly, via the logical overlay links (each of which corresponds to a path through the underlying physical network). Overlays are used for indexing and peer discovery, and make the P2P system independent from the physical network topology. Based on how the nodes are linked to each other within the overlay network, and how resources are indexed and located, we can classify networks as *unstructured* or *structured* (or as a hybrid between the two)

1.2, Unstructured networks

Distributed hash tables

However, in order to route traffic efficiently through the network, nodes in a structured overlay must maintain lists of neighbors that satisfy specific criteria. This makes them less robust in networks with a high rate of *churn* (i.e. with large numbers of nodes frequently joining and leaving the network) More recent evaluation of P2P resource discovery solutions under real workloads have pointed out several issues in DHT-based solutions such as high cost of advertising/discovering resources and static and dynamic load imbalance.



1.3, Hybrid models

Hybrid models are a combination of peer-to-peer and client-server models. A common hybrid model is to have a central server that helps peers find each other. There are a variety of hybrid models, all of which make trade-offs between the centralized functionality provided by a structured server/client network and the node equality afforded by the pure peer-to-peer unstructured networks. Currently, hybrid models have better performance than either pure unstructured networks or pure structured networks because certain functions, such as searching, do require a centralized functionality but benefit from the decentralized aggregation of nodes provided by unstructured networks

1.4, Network neutrality

Peer-to-peer applications present one of the core issues in the Network neutrality controversy. Internet service providers have been known to throttle P2P file-sharing traffic

due to its high-bandwidth usage. Compared to Web browsing, e-mail or many other uses of the internet, where data is only transferred in short intervals and relative small quantities, P2P file-sharing often consists of relatively heavy bandwidth usage due to ongoing file transfers and swarm/network coordination packets. Critics point out that P2P networking has legitimate legal uses, and that this is another way that large providers are trying to control use and content on the Internet, and direct people towards a client -server based application architecture. The client-server model provides financial barriers-to-entry to small publishers and individuals, and can be less efficient for sharing large files.

Advantages

Easy and simple to set up only requiring a hub or a switch to connect all computers together. You can access any file on the computer as-long as it is set to a shared folder. If one computer fails to work all the other computers connected to it still continue to work.

III. SECURITY THREATS

A P2P network treats every user as a peer. In file sharing protocols such as BT, each peer contributes to service performance by uploading files to other peers while downloading. This opens a channel for files stored in the user machine to be uploaded to other foreign peers. The potential security risks include:

TCP ports issues

Usually, P2P applications need the firewall to open a number of ports in order to function properly. Each open port in the firewall is a potential avenue that attackers might use to exploit the network. It is not a good idea to open a large number of ports in order to allow for P2P networks.

Propagation of malicious code such as viruses

As P2P networks facilitate file transfer and sharing, malicious code can exploit this channel to propagate to other peers. For example, a worm called VBS. Gnutella was detected in 2000 which propagated across the Gnutella file sharing network by making and sharing a copy of itself in the Gnutella program directory. Trojan horses have also been found over P2P networks. The Trojan would open a backdoor in a user's Windows PC to allow a remote intruder access and control of the computer18. Theoretically speaking, sensitive and personal information stored in the infected computer could be copied to other machines on the P2P network.

Risks of downloaded content

When a file is downloaded using the P2P software, it is not possible to know who created the file or whether it is trustworthy. In addition to the risks of viruses or malicious code associated with the file, the person downloading the file might also be exposed to criminal and/or civil litigation if any illegal content is downloaded to a company machine. Also, when downloading via a P2P network, it is not possible to know what peers are connected at any one time and whether these peers are trustworthy or not. Un trusted sources induce another security threat.

Vulnerability in P2P software

Like any software, P2P software is vulnerable to bugs. As each peer is both a client and a server, it constantly receives requests from other peers, and if the server component of the P2P software is buggy, it could introduce certain vulnerabilities to a user's machine. Intruders could exploit this to spread viruses, hack into a machine. It was reported in 2003 that a bug in the P2P software Kazaa Media Desktop could cause a denial of service attack, or allow a remote attacker to exploit arbitrary code.

IV. FUTURE

The current peer-to-peer model appears to be moving toward a true peer-to-peer model without a centralized server, which Microsoft Networking uses today. The current peer-to-peer model's advantage over Microsoft Networking is its ability to perform fast searches and exchange data through firewalls. Future models of peer-to-peer networking will combine aspects of Microsoft Networking and Napster's protocols to allow for easy search capabilities and the ability of open Data Stores. For example, in Microsoft Networking you can allow for Full Control, meaning that a remote user cannot only download, but also upload and modify data stored in the shared space. Imagine departmental groups in a corporation who need to share and update each other's files. A

peer-to-peer networking model that does not require that a file be downloaded in order to be executed, and allows write-ability to remote shares will increase the ability of a malicious threat to propagate. Threats that infect network shares, such as W32.FunLove, demonstrate the difficulty of containment in environments that utilize central file servers (along with personal shares). A peer-to-peer networking model that incorporates uploading as well as downloading increases the propagation and difficulty of containment of network infectors.

Such a model allows simpler two-way communication of malicious threats. Virus writers may be able to update their threats via a peer-to-peer network. For example, an infected machine may send an update to all other nearby nodes of a peer-to-peer network.

V. SUMMARY

Peer-to-peer networks obviously pose a danger as an additional degree of delivery. Their impact on security will depend on the adoption of peer-to-peer networks in standard computing environments. If systems use peer-to-peer networks as email is used today, then they will be significant methods of delivery of harmful code. The use of two-way network communication also exposes the system to potential remote control. More importantly, the usage of a peer-to-peer network creates a hole in a firewall and can lead to the exporting of private and confidential information. Therefore, administrators should begin analyzing their networks for peer-to-peer network usage and configure firewalls and systems accordingly to limit or prevent their usage.

VI. CONCLUSION

While P2P networks opens up a new channel for efficient downloading and sharing of files and data, users need to be fully aware of the security threats associated with this technology. Security measures and adequate prevention should be implemented to avoid any potential leakage of sensitive and/or personal information, and other security breaches. Before deciding to open firewall ports to allow for peer-to-peer traffic, system administrators should ensure that each request complies with the corporate security policy and should only open a minimal set of firewall ports needed to fulfill P2P needs. For end-users, including home users, care must be taken to avoid any possible spread of viruses over the peer-to-peer network.

REFERENCES

[1] Rüdiger Schollmeier, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).

[2] D. Barkai, Peer-to-Peer Computing, Intel Press, 2002.

[3] Oram, A. (Ed.). (2001). Peer-to-peer: Harnessing the Benefits of a Disruptive Technologies. O'Reilly Media, Inc.

[4] Host Software, S. Crocker, IETF Working Group (April 7, 1969)

[5] Berners-Lee, Tim (August 1996). "The World Wide Web:Past,Present,Future". Retrieved 5 November 2011.

[6] Steinmetz, R., & Wehrle, K. (2005). 2. What Is This "Peer-to-Peer" About? (pp. 9-16). Springer Berlin Heidelberg.

[7] Walker, Leslie (2001-11-08). "Uncle Sam Wants Napster" The Washington Post. Retrieved 2010-05-22.