PEER-TO-PEER NETWORK

February 2008

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary 2

I. Introduction 3

II. Management Considerations 5

Trends and Impact 5

Governance and Regulations 6

III. Security Considerations 8

Classification of P2P Networks 8

Security Threats 9

Best Practices for Organisations and End-Users 11

IV. Conclusion 14

SUMMARY

In a peer-to-peer (P2P) network, every machine plays the role of client and server at the same time. Although a P2P network has a number of advantages over the traditional client-server model in terms of efficiency and fault-tolerance, additional security threats can be introduced. Users and IT administrators need to be aware of the risks from propagation of malicious code, the legality of downloaded content, and vulnerabilities within peer-to-peer software. Security and preventative measures should be implemented to protect from any potential leakage of sensitive information and possible security breaches. Within corporate networks, system administrators need to ensure that peer-to-peer traffic complies with the corporate security policy. In addition, they should only open a minimal set of firewall ports to allow for such traffic. For end-users and/or home users, precautions must also be taken to avoid the possible spread of viruses over peer-to-peer networks.

I. INTRODUCTION

Peer-to-peer (P2P) is an alternative network model to that provided by traditional client-server architecture. P2P networks use a decentralised model in which each machine, referred to as a peer, functions as a client with its own layer of server functionality[1]. 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 deteriorate 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 organise 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-organisation of group peer members is transparent to end-users.

Another characteristic of a P2P network is its capability in terms of fault-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 BitTorrent 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

[1] http://www.intel.com/technology/magazine/systems/it02012.pdf

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.

II. MANAGEMENT CONSIDERATIONS

TRENDS AND IMPACT

The first appearance of open source systems such as Napster in 1999 radically changed file-sharing mechanisms. The traditional client-server file sharing and distribution approach using protocols like FTP (File Transfer Protocol) was supplemented with a new alternative — P2P networks. At the time, Napster was used extensively for the sharing of music files. Napster was shut down in mid-2001[2] due to legal action by the major record labels.

The shutting of Napster did not stop the growth of P2P applications. A number of publicly available P2P systems have appeared in the past few years, including Gnutella, KaZaA, WinMX and BitTorrent, to name but a few. From analysis of P2P traffic in 2007, BitTorrent is still the most popular file sharing protocol, accounting for 50-75% of all P2P traffic and roughly 40% of all Internet traffic[3].

P2P technology is not just used for media file sharing. For example, in the bioinformatics research community, a P2P service called Chinook[4] has been developed to facilitate exchange of analysis techniques. The technology is also used in other areas including IP-

[2] http://www.oecd.org/dataoecd/55/57/32927686.pdf

[3] http://torrentfreak.com/bittorrent-dominates-internet-traffic-070901/

[4] http://smweb.bcgsc.bc.ca/chinook/

based telephone networks, such as Skype[5], and television networks, such as PPLive[6]. Skype allows people to chat, make phone calls or make video calls. When launched, each Skype client acts as a peer, building and refreshing a table of reachable nodes[7] in order to communicate for chat, making phone calls or video calls. PPLive shares live television content. Each peer downloads and redistributes live television content from and to other peers[8].

GOVERNANCE AND REGULATIONS

In the U.S., a number of politicians have raised concerns about possible threats to national security due to P2P network technology. The possibility of accidental leaks of classified information by government officers to foreign governments, terrorists or organised crime via P2P file sharing programs has prompted a view that "*new laws and rules should be enacted to protect personal information held by federal agencies and other organisations*". The proposal does not restrict P2P networks as a whole, but attempts to strike "*a balance that protects sensitive government, personal and corporate information and copyright laws*"[9].

A P2P network itself is only a form of technology, and is not related to disputes over content and intellectual property rights. However, there have been court cases in Hong Kong against illegal P2P activities. In 2005, a Hong Kong resident was convicted of

[5] http://www.skype.com/products/explained.html

[6] http://www.pplive.com/en/about.html

[7] http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf

[8] http://eeweb.poly.edu/faculty/yongliu/docs/pplive.pdf

[9] http://www.news.com/Congress-P2P-networks-harm-national-security/2100-1029_3-6198585.html

breaching the Copyright Ordinance by uploading illegal copies of copyrighted works to the Internet using the BitTorrent peer-to-peer file sharing program, and making files available for download by other Internet users[10].

[10] http://www.customs.gov.hk/eng/new_release_20070518_bt_e.html

III. SECURITY CONSIDERATIONS

CLASSIFICATION OF P2P NETWORKS

P2P networks can be roughly classified into two types — “pure P2P networks” and “hybrid P2P networks”. In a pure P2P network, all participating peers are equal, and each peer plays both the role of client and of server. The system does not rely on a central server to help control, coordinate, or manage the exchanges among the peers[11]. Gnutella[12] and Freenet[13] are examples of a pure P2P network.

In a hybrid P2P network, a central server exists to perform certain “administrative” functions to facilitate P2P services. For example, in Napster, a server helps peers to “*search for particular files and initiate a direct transfer between the clients*”[14]. Only a catalogue of available files is kept on the server, while the actual files are scattered across the peers on the network. Another example is BitTorrent (BT), where a central server called a tracker helps coordinate communication among BT peers in order to complete a download.

The central distinction between the two types of P2P network is that hybrid P2P networks have a central entity to perform certain administrative functions while there is no such

[11] http://www.intel.com/technology/magazine/systems/it02012.pdf

[12] http://www.gnutella.com/

[13] http://freenetproject.org/

[14] http://opennap.sourceforge.net/

server in pure P2P networks[15]. Compared to the hybrid P2P architecture, the pure P2P architecture is simpler and has a higher level of fault tolerance. On the other hand, the hybrid P2P architecture consumes less network resources and is more scaleable than the pure P2P approach.

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:

1. TCP ports issues:

   Usually, P2P applications need the firewall to open a number of ports in order to function properly. BitTorrent, for example, will use TCP ports 6881-6889 (prior to version 3.2). The range of TCP ports has been extended to 6881-6999 as of 3.2 and later[16]. 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.

2. 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

[15] http://www.iu.hio.no/~frodes/rm/trond.pdf

[16] http://www.dessent.net/btfaq/#ports

sharing network by making and sharing a copy of itself in the Gnutella program directory[17].

Trojan horses have also been found over P2P networks. An example is W32/Inject-H, which contained an IRC backdoor Trojan that utilised P2P networks to propagate itself. The Trojan would open a backdoor in a user's Windows PC to allow a remote intruder access and control of the computer[18]. Theoretically speaking, sensitive and personal information stored in the infected computer could be copied to other machines on the P2P network.

3. 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. Untrusted sources induce another security threat.

4. 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, or even launch a enial of ervice attack. It was reported in

[17] http://www.symantec.com/security_response/writeup.jsp?docid=2000-121813-5230-99

[18] http://www.sophos.com/security/analyses/w32injecth.html

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[19].

In addition to general security risks, the use of P2P applications in a company network situation could generate an unnecessarily large amount of network traffic, monopolising network bandwidth that should be available for other business applications. The time spent by employees in dealing with the effects of P2P download or upload will affect employee productivity and the organisation's bottom line.

BEST PRACTICES FOR ORGANISATIONS AND END-USERS

In light of these security threats, appropriate security and preventive measures should be implemented to protect against any potential leakage of sensitive information and breaches of security. The following are best practices for organisations and end-users when considering the use of P2P technologies.

Organisational Networks

To mitigate the risks associated with exposing TCP ports, the organisation should review the need for P2P technologies in supporting their day-to-day business operations. If a P2P network is not required, security policies should be established to block off unnecessary port ranges across the network. Regular reminders should be sent to users not to download and install P2P applications on company machines. If a P2P network is necessary for certain business operations, the use of all P2P software should be controlled

[19] http://ca.com/tw/securityadvisor/vulninfo/Vuln.aspx?ID=7098

and approved on a case-by-case basis. Users should be educated about proper use of P2P networks, as well as the dangers associated with file sharing. In particular, a P2P network is not a recommended channel for the sharing of sensitive or personal information because communication links in P2P networks are not usually encrypted, and any content is at risk of sniffing by external parties.

In addition, all organisation network traffic should be monitored by an IDS / IPS (Intrusion Detection System / Intrusion Prevention System). Any unauthorised P2P network traffic detected (e.g. by reviewing firewall / IDS log, when diagnosing for a sudden drop in network performance) should be investigated and blocked. A clear firewall policy should be defined to block network ports used by common P2P applications (such as the ports mentioned for Bit-Torrent in the previous section) so as to deny P2P network traffic from entering or leaving the internal network.

In addition, users should have adequate protections against any attacks that may be bought on by P2P technology. Anti-virus programs with the latest virus definitions, regular patch management at the users' desktop PC and appropriate personal firewall configuration is a must in securing an organisation's network.

End-users / Home Network

Similarly, security controls such as personal firewalls, anti-virus programs with latest virus definitions, the latest security patches and system administrative rights restrictions need to be implemented to avoid potential security breaches and system misuse in end-users/home networks. If file sharing is not needed, blocking unnecessary port ranges is suggested.

The advice regarding the security of desktop PCs is also applicable to home users. For young people sharing files over the Internet, they must be educated on the dangers of downloading files from untrustworthy or suspicious sources. If a P2P download is necessary, it is advisable to quit the P2P client application after completion of the download. Child pornography and other illegal material, including pirate software, should never be downloaded.

IV. CONCLUSION

While P2P networks open 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 fulfil 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.