



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Managing Peer-to-Peer Applications in Dormitory Networks

Network security for dormitory networks have similar but special network security implications than the typical network. Most universities are less restrictive on user policy and dormitory networks are even less restrictive because it is a semi-private network, since the dorm residents own the workstations but the universities own the network. This makes it hard for universities to control what applications are installed and running on a dorm resident's computer. There is a need to manage the usage of P2P apps because ...

Copyright SANS Institute
Author Retains Full Rights

AD



Managing Peer-to-Peer Applications in Dormitory Networks

Abstract

This paper will focus on the issue of peer-to-peer application (P2P app) management in university dormitory networks. Dorm networks are usually not tightly secured as an ordinary network and thus special procedures need to be used to either block or restrict the use of P2P apps for illegal file swapping. Most universities have experienced or are currently experiencing problems in dealing with P2P app management. This paper will start out with an overview of the typical P2P apps used in dorm networks. The paper then discusses the problems associated with P2P apps in dorm networks. Then there is a brief discussion of how a dorm network security policy can be used for P2P app management. The bulk of this paper focuses on the tools for P2P app management. Then issues with P2P monitoring are discussed in the higher education environment. Throughout the paper, examples of actual universities and vendor tools are included. The paper concludes with the outlook of P2P management for dorm networks.

Introduction

Network security for dormitory networks have similar but special network security implications than the typical network. Most universities are less restrictive on user policy and dormitory networks are even less restrictive because it is a semi-private network, since the dorm residents own the workstations but the universities own the network. This makes it hard for universities to control what applications are installed and running on a dorm resident's computer. There is a need to manage the usage of P2P apps because it is used illegally by a majority of the dorm users to illegally trade copyrighted material, which could make the users liable and possibly the universities liable. Though the Recording Industry Association of America (RIAA) does not have an estimate of how much of the illegal P2P music files are downloaded by dorm residents, a significant amount of the 2.5 billion downloads that occur each month are from dorm networks (Mark). Back on October of 2002, the RIAA with other trade groups, sent letters to approximately 2,300 higher education institutions requesting their network administrators to eradicate illegal P2P file

sharing (Cox). In April 2003, the RIAA sued four students separately for using P2P apps to download and share MP3 song files. The lawsuits could have had the students each pay up to \$100 million, but each student settled with making payments totaling \$12,000 to \$17,000 that would be paid between 2003 and 2006 (Borland, "Campus"). The RIAA was also asking universities to hand over the students' names that used universities' networks to illegally share files using P2P apps. In July 2003, Loyola University Chicago was the first university to comply with RIAA's request to hand over the names of students suspected of violating the Digital Millennium Copyright Act of 1998 (Vance). However, the RIAA has made mistakes in identifying potential violators in universities. In May 2003, the RIAA withdrew a notice (not a subpoena) to Penn State University's astronomy and astrophysics department, which made the central computing office at the university threaten to cut off Internet access for the department if the illegal music files were not found and deleted. The RIAA's automated program made a mistake by identifying a folder in one of the department's computer having a legal MP3 within a folder named "usher"—and made the assumption that there was an illegal copy of an MP3 by the musician Usher (McCullagh). As of December 2003, a federal appeals court ruled RIAA is illegally issuing subpoenas to ISPs seeking the contact information of alleged users who download or share copyrighted music. The ruling would require the RIAA to file a "John Doe" lawsuit against each anonymous illegal file trader that requires a judge's supervision; this would require more manpower and time for the RIAA to sue each individual (Borland, "Court"). Even though it might be harder right now for the RIAA to subpoena a university to give out students' names, universities cannot ignore illegal file swapping in their dorm networks.

Overview of typical P2P apps used in dorm networks

Dorm networks are less restrictive than a typical network since students own the computers. Universities are usually less restrictive because of the academic environment and budget limitations limit the choice of what they can do to enforce any policies that are in place. This combination has made students at universities contribute a significant amount of illegal P2P file sharing. In a study conducted in September 2003 by the Business Software Alliance, close to two-thirds of surveyed college students would download copyrighted software if they had the opportunity. The study also showed that only 8% of the 69% of students have paid for downloaded music (Harrison).

P2P apps allow the use of decentralized, dynamic, and anonymous networks for file exchange over the Internet (P-Cube Inc., p. 2). There are many P2P apps available and some of them are listed here:

2 Find MP3, Aimster, Audio Galaxy, AudioGnome, BearShare, Blubster, Direct Connect, Earthstation 5, eDonkey 2000, FileNavigator, Filetopia, Flipr, Gnotella, Gnucleus, Grokster, Imesh, KaZaa, LimeWire, Mactella, Morpheus, Napigator, Ohaha, Rapigator, Real MP3 Finder, Songspy, Swaptor. WinMX, Xolox (SurfControl plc.).

The two most popular P2P network architectures are FastTrack and Gnutella. Kazaa, iMesh, and Grokster are the P2P clients that use the FastTrack architecture. The FastTrack architecture utilizes a central server for user authentication and locating files for users. The central server automatically chooses “SuperNodes”, which are users’ computers that have very high-speed connections. When a user submits a query, the central server directs the user to the closest SuperNode for file searching and initiates user-to-user file transfers. This method speeds up file searches and reduces traffic generated by file searches (Piccard, p. 22). SuperNode traffic is encrypted and by default, all FastTrack protocol connections use TCP port 1214 (Piccard, p. 23).

The Gnutella architecture is a true peer-to-peer network with no central servers. Users (servants) have to connect to one of several prearranged IP addresses, which relays other servants’ IP addresses for file searching and transfers. When a servant starts a file search query, the query is passed to the known IP addresses of other servants, and if necessary passed along to other servants in a hierarchal fashion (Piccard, p. 25). Morpheus, Limewire, BearShare, and Gnucleus are the most popular Gnutella architecture clients (Piccard, p. 26). Gnutella clients can use any port for communications, such as ports 21,25, 80, and 143, which are generally open on a firewall. Due to the extensive configuration parameters of Gnutella clients, a network monitoring tool may perhaps be the most effective method to detect these clients (Piccard, p. 27). The eDonkey architecture is rather common in Europe and has a growing user base in the United State. EDonkey2000, eMule, MLDonkey, and xMule2 are clients that use the eDonkey architecture. The eDonkey architecture is semi-centralized because it uses servers set up by users. For a user to connect to the eDonkey network the eDonkey client needs to connect to the IP address of at least one server; a server list is stored on a Web page and is downloaded by the eDonkey client. eDonkey offers a feature called “the horde” that allows clients to work together for faster file transfers. Another feature, called swarming, breaks up each file into smaller parts to allow them to be independently distributed (Piccard, p. 29).

The P2P apps problem in dormitory networks

Typical dorm networks are usually designed to handle large downstream applications such as e-mail and web browsing. P2P file sharing increases the upstream to downstream traffic ratio, causing upstream link congestion. The typical dorm network is designed to handle peak hours of traffic, but P2P apps download or upload many large multi-megabyte files that are queued to be transferred on students’ computers, causing high bandwidth utilization throughout the day (P-Cube Inc., p. 3). Recent statistics estimate that P2P traffic makes up 60% of all Internet traffic (P-Cube Inc., p. 3). However, dorm networks have a higher amount of P2P traffic, as P2P traffic may use up to 90% utilization of the available campus bandwidth—which the University of Florida has experienced (Gasior).

Although the Recording Industry of America has filed lawsuits against students but not at educational institutions, there still is a potential liability for education institutions. Educational institutions may perhaps face contributory or vicarious liability from the activities of their students. The chances are low that an educational institution would be faced with such a lawsuit as it would depend on the institution's knowledge of illegal file sharing, contribution to illegal file sharing, ability to control the illegal file sharing, and whether the institution acquires monetary benefit from the illegal file sharing. Contributory infringement liability is described as "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another..." Vicarious liability can be brought upon defendants who "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities" (Remington, P. 6). Therefore, it is important for educational institutions to not ignore the legal liability of illegal file sharing in dorm networks.

P2P file sharing programs exposes the campus' network and students' computers to hackers, viruses, worms, and Trojan horses. Since P2P apps uses direct connections between two users for file sharing across the Internet, hackers have taken advantage of this by attaching Trojan Horses to files that log keystrokes or set up IRC backdoors to the victims' computers (Falcon I.T. Services). For example, Fizzer was the most recent Kazaa worm that installs a keyboard logger and transmits the information through backdoor utilities via IRC, HTTP, or Telnet protocols. The Fizzer worm also had the capability of disabling anti-virus programs (Piccard, p. 23). In general, there is a very high risk that files downloaded from P2P apps contain malicious code that could endanger the students' computers, which could then be used to attack the university's network. P2P apps can penetrate firewalls, which would weaken a university's firewall. P2P apps also reveals internal network information such as IP addresses which could allow potential hackers to target the user's network--such as owning the user's computer for a distributed denial of service (DDoS) attack (Cole et al., p. 693).

Most universities have budget limitations to employ the optimum amount of network staff for their network operations let alone to manage P2P usage. Without specialized tools, P2P apps are using elusive methods to escape detection from administrators by using port hopping, port masquerading, and encrypted P2P traffic. With port hopping and port masquerading, if a firewall blocks a P2P app's default port it will switch to open ports such as port 80 and as a result disguise as Web traffic (Messmer). One P2P app using encryption is Earthstation 5, which uses SSL (Secure Sockets Layer) encryption to shield the identity of data being shared (Borland, "Refugee"). P2P apps can utilize proxy servers to hide file-sharing activity. For example, KaZaa can use an external SOCKS 5 proxy server to route file transfers if the default TCP port 1214 is blocked (Piccard, 24).

P2P Network Security Policy

Every university should use a dorm network security policy for peer-to-peer application management. The content of a dorm network security policy should contain an issue-specific policy regarding the issue of P2P app use. In Sans Security Essentials with CISSP CBK, an issue-specific policy should contain these details:

- Purpose—this should explain the reason for having a policy regarding P2P app usage.
- Related documents—includes any documents or policies that affects the policy; laws such as United States Copyright Law and the Digital Millennium Copyright Act might be included here.
- Cancellation—states any existing policy that is terminated when this policy is in use; most universities would not have any cancellation of any existing policies since they probably never had an issue-specific policy regarding P2P app usage.
- Background—provides further reasons on the need for this policy; this should explain the need for the P2P app usage policy such as the unlawfulness and prosecution of illegal file sharing, and the necessity for bandwidth management.
- Scope—indicates who and what the policy applies to; the policy could apply to all students on campus or dorm residents regarding P2P app usage.
- Policy statement—lists the actual rules; this should include an explanation that illegal P2P file sharing is prohibited and violators would be punished.
- Action—states what procedures are required and when they are to be completed; this should explain any network usage restrictions that have been implemented to enforce this policy, such as a bandwidth cap on all P2P apps.
- Responsibility—indicates who is accountable for what. Probably the IT personnel in charge of the dorm network are the first line of enforcement and then flows up to the CIO of the university for appeals.
- Ownership—need to specify who sponsored the policy and where authority was derived from, and who may make changes to the policy. Usually it is IT upper-management who sponsors this policy and authorizes changes, and authority is derived from the United States copyright law (Cole et. al, 341).

A partial sample of a policy regarding P2P use is from Azusa Pacific University (the entire policy can be found at <http://www.apu.edu/imt/peer-to-peer-file-sharing.php>):

Purpose

The primary purpose of this policy is to inform, educate and set expectations for the members of the university community of their individual and corporate responsibilities towards the use of Peer-to-Peer applications using the University's network.

Scope

This policy addresses the issues, impacts and concerns with file sharing aspects of Peer-to-Peer networking applications using the University's network.

Background

While the definition itself is controversial, generally a peer-to-peer (often referred to as P2P) computer network refers to any network that does not have fixed clients and servers, but a number of peer nodes that function as both clients and servers to the other nodes on the network. This model of network arrangement is contrasted with the client-server model. Any node is able to initiate or complete any supported transaction. Peer nodes may differ in local configuration, processing speed, network bandwidth, and storage quantity. Put simply, peer-to-peer computing is the sharing of computer resources and services by direct exchange between systems. Many researchers are looking into the practical uses of this technology.

This policy intends to make it clear that P2P architecture, itself, is not in question. What is a concern, however, is one of the most prevalent uses of this technology, P2P File Sharing applications used for the distribution of copyrighted content. Morpheus, KaZaa, Aimster, Madster, AudioGalaxy and Gnutella, are examples of the kinds of P2P File Sharing software, which can be used inappropriately to share copyrighted content. Note, that some of these applications are not pure peer-to-peer architectures, further reinforcing that the issues with File Sharing applications have more to do with risk of abuses, than in the technology itself. Along with copyright infringement, other concerns of P2P File Sharing applications include network resource utilization, security, and inappropriate content. For a more in-depth definition of peer-to-peer and the various types (hybrid vs. pure) and peer-to-peers relationship with distributed networks, please refer to the footnotes.

For the purposes of this policy, a Peer-to-peer file sharing application is any application that transforms a personal computer into a server that distributes data simultaneously to other computers.

Issues

Copyright Infringement

Downloading or distributing copyrighted material, e.g. documents, music, movies, videos, text, etc., without permission from the rightful owner violates the United States Copyright Act and several

university policies. While it is true that a number of artists have allowed their creative works to be freely copied, those artists remain very much the exception. It is best to assume that all works are copyright-protected except those that explicitly state otherwise.

Those who obtain or distribute copyrighted material should be aware that if found liable for copyright infringement, the penalties can be severe, depending upon the amount and the willfulness of the infringing activity. In a civil lawsuit, one found liable for copyright infringement can be ordered to pay damages of as much as \$30,000 per copyrighted work infringed. This penalty can be increased to \$150,000 per infringed work in cases of particularly flagrant infringement. In the most serious and widespread cases of copyright infringement, criminal prosecution is possible.

Additionally, students, faculty and staff who may be in violation of copyright law place not only themselves at risk - they may be exposing Azusa Pacific University to liability as an institution, for contributory or vicarious infringement, e.g., using the University network resources to obtain the material and/or to store the material on University computers and/or servers

The results of a recent on campus survey, although not an extensive sample, indicates a lack of recognition by students that downloading and uploading MP3 files may infringe on the copyrights of musicians. In other words, obtaining copyrighted material without the permission of the owner of the work is stealing.

(part of the policy omitted)

Policy

It is the policy of APU that the university's network connections may not be used to violate copyright laws. The unauthorized reproduction of copyrighted materials is a serious violation of APU's Internet Acceptable Use Policy, as well as the U.S. Copyright Laws, as discussed above.

IMT has placed into effect a limit of 1 megabit per second (Mbps) on the inbound and outbound traffic generated by Peer-to-Peer file-sharing applications. For comparison purposes, the outside Internet connection for the University is 15Mbps between 7AM and 10PM and 25 Mbps between 10PM and 7AM (that bandwidth is used for both incoming and outgoing connections).

This restriction is necessary to support the primary usage of the network: academic and enterprise computing. The data network must be available for APU's students, faculty, and staff to use for academic research and essential daily operations. While IMT does have the option to entirely shut off access to Peer-to-Peer applications, that option is not currently being exercised.

APU realizes this can result in the delay of downloading files from the Internet; however, Peer-to-Peer applications are an incredible consumer of bandwidth and will take as much bandwidth as available, constricting available bandwidth for other applications.

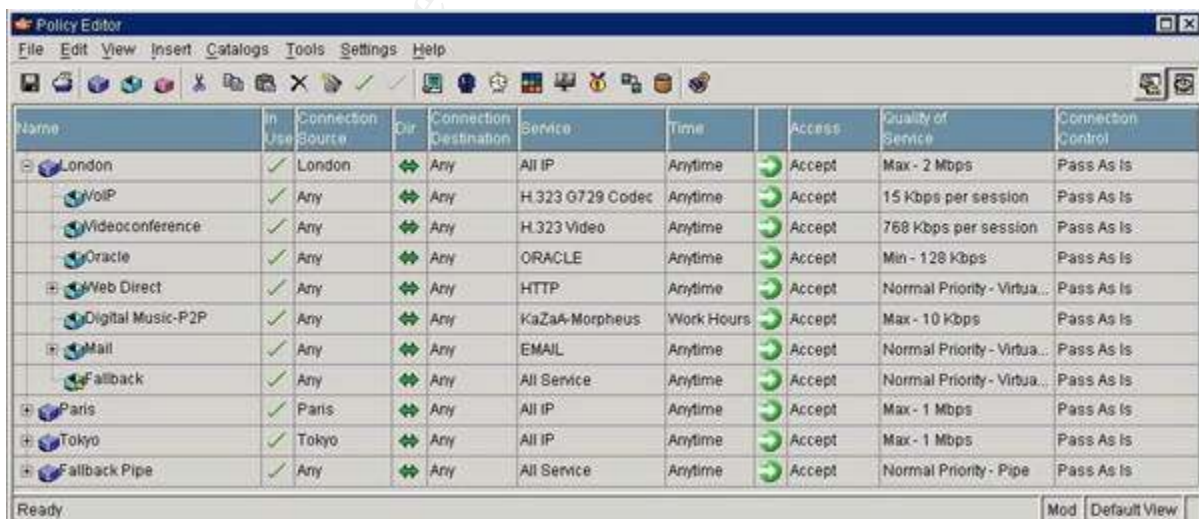
If an artist, author, publisher, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), or a law enforcement agency notifies the University that a Faculty/Staff member or Student is violating copyright laws, IMT will provide to the relevant offices within the University information in the form of Internet Protocol (IP) address information and any information from logs to assist in the investigation of the complaint. If appropriate, action will be taken against the violator in accordance with University policy. In some cases, violations of University policy can result in suspension or revocation of network access privileges without refund of network access fees and/or civil or criminal prosecution under state and federal statutes. (Azusa Pacific University).

For a security policy to be effective, it must be enforced. There is no standard yet of what procedures should be used when a student is caught illegally using a P2P app to share files in a dorm network. As an example--for Azusa Pacific University--if the RIAA, law enforcement agency, or the university's internal reporting system detected illegal file sharing activity, the student would first have his or her Internet access cut off immediately and be notified via a written warning. The student has to sign the written warning acknowledging the warning and promising not to conduct any further illegal file sharing activity and then the student is allowed Internet access. On the second offense, the student is immediately denied access for one year and another written warning is sent. Some universities, such as Temple University are considering including in their policy the refusal of any hardware or support for students' computers if they contain disallowed P2P programs or illegal files (King, p. 3). From the announcements by universities about the legal and ethical issues of illegal file trading and with the cooperation from university network administrators in managing illegal P2P file sharing, there is a continuing trend of decreased illegal P2P file sharing in dorm networks (Borland, "Colleges").

Tools for peer-to-peer application management

A relatively ineffective method that many university IT staff use to block P2P traffic is by blocking P2P traffic ports using a packet filtering-firewall such as ipchains and iptables in Linux, ISA Server in Windows 2000 Server, or Cisco ACLs (access control lists). P2P apps usually connect to a central server on a default port before connecting to peer computers for actual file sharing, but P2P apps can use port hopping to overcome port blocking (Govindarajan). For example, Kazaa uses the default port of 1214 to connect to the Kazaa network, and the incoming and outgoing TCP and UDP needs to be blocked.

There are many bandwidth management products that can help detect and stop P2P traffic. One method to help identify potential P2P abusers is to identify the top talkers on the dorm network using a network monitoring tool such as Network Instruments Observer (http://www.networkinstruments.com/products/observer_statistics.html). P2P abusers will generally consume more bandwidth than users who just check e-mail and surf the Web. There are also bandwidth management appliances that can limit bandwidth usage, provide bandwidth rate limits, and provide traffic shaping. One such product is Allot Communications NetEnforcer (http://www.allot.com/html/products_netenforcer_enterprise.shtml), which includes Layer 7 protocol monitoring and application signature identification to control P2P apps. NetEnforcer monitors traffic and can create policies to enforce quality of service (QoS) by user, application, protocol, bandwidth usage, and time of day. NetEnforcer allows administrators to group applications into categories and guarantees and prioritizes traffic based on the application (Allot Communications Ltd).



The screenshot shows the 'Policy Editor' window in NetEnforcer. The window has a menu bar (File, Edit, View, Insert, Catalogs, Tools, Settings, Help) and a toolbar. Below the toolbar is a table with the following columns: Name, In Use, Connection Source, Dir, Connection Destination, Service, Time, Access, Quality of Service, and Connection Control. The table contains several rows of policies, including 'London', 'VoIP', 'Videconference', 'Oracle', 'Web Direct', 'Digital Music-P2P', 'Mail', 'Fallback', 'Paris', 'Tokyo', and 'Fallback Pipe'. Each row has a green checkmark in the 'In Use' column and a green arrow in the 'Access' column. The 'Quality of Service' column contains various settings like 'Max - 2 Mbps', '15 Kbps per session', '768 Kbps per session', 'Min - 128 Kbps', 'Normal Priority - Virtua...', 'Max - 10 Kbps', 'Normal Priority - Virtua...', 'Max - 1 Mbps', and 'Normal Priority - Pipe'. The 'Connection Control' column contains 'Pass As Is' for all rows.

Name	In Use	Connection Source	Dir	Connection Destination	Service	Time	Access	Quality of Service	Connection Control
London	✓	London	↔	Any	All IP	Anytime	→ Accept	Max - 2 Mbps	Pass As Is
VoIP	✓	Any	↔	Any	H.323 G729 Codec	Anytime	→ Accept	15 Kbps per session	Pass As Is
Videconference	✓	Any	↔	Any	H.323 Video	Anytime	→ Accept	768 Kbps per session	Pass As Is
Oracle	✓	Any	↔	Any	ORACLE	Anytime	→ Accept	Min - 128 Kbps	Pass As Is
Web Direct	✓	Any	↔	Any	HTTP	Anytime	→ Accept	Normal Priority - Virtua...	Pass As Is
Digital Music-P2P	✓	Any	↔	Any	KaZaA-Morpheus	Work Hours	→ Accept	Max - 10 Kbps	Pass As Is
Mail	✓	Any	↔	Any	EMAIL	Anytime	→ Accept	Normal Priority - Virtua...	Pass As Is
Fallback	✓	Any	↔	Any	All Service	Anytime	→ Accept	Normal Priority - Virtua...	Pass As Is
Paris	✓	Paris	↔	Any	All IP	Anytime	→ Accept	Max - 1 Mbps	Pass As Is
Tokyo	✓	Tokyo	↔	Any	All IP	Anytime	→ Accept	Max - 1 Mbps	Pass As Is
Fallback Pipe	✓	Any	↔	Any	All Service	Anytime	→ Accept	Normal Priority - Pipe	Pass As Is

Figure 1. The Policy Editor in NetEnforcer is used to configure network traffic policies (Allot Communications Ltd).

Many universities have seen much benefit from P2P management with NetEnforcer. Louisiana State University faced a problem of P2P traffic using 60 to 80% of the university's bandwidth. Using NetEnforcer, the university was able to guarantee a minimum and maximum amount of bandwidth for a specific application or user. NetEnforcer also allowed the university to guarantee constant bit rates for VoIP and videoconferencing, which are crucial for latency-sensitive applications (PR Newswire).

Another popular bandwidth management appliance is Packeteer's PacketShaper (<http://www.packeteer.com/prod-sol/products/packetshaper.cfm>), which allows administrators to set policies that enforce:

- **Per-App Minimum and Maximum:** Provide a limit and a cap on the bandwidth usage on an application type. PacketShaper can parse streams of data to identify specific P2P app traffic. This allows the separation of each application's traffic and allows the distribution of the appropriate bandwidth according to the importance of the application.
- **Per-Session Minimum and Maximum:** Provide a minimum bandwidth rate for latency-sensitive applications and allow prioritized excess bandwidth usage. Provide a cap for the bandwidth rate for a traffic session such as an FTP download. This prevents large sessions from affecting sessions that are more important.
- **Dynamic Per-User Minimum and Maximum:** Provides dynamic allocation of bandwidth per user without detailed and time-consuming per-user configuration, and allow unused bandwidth to be loaned to others.
- **Denial-of-Service Attack Avoidance:** Detects and stops SYN floods, detects and blocks ICMP variants that can install malicious instructions (Packeteer, Inc., "PacketShaper").

PacketShaper also has built-in centralized reporting called ReportCenter that details network utilization and application performance analysis so that the policies can be refined (Packeteer, Inc., "4-Steps").

© SANS Institute

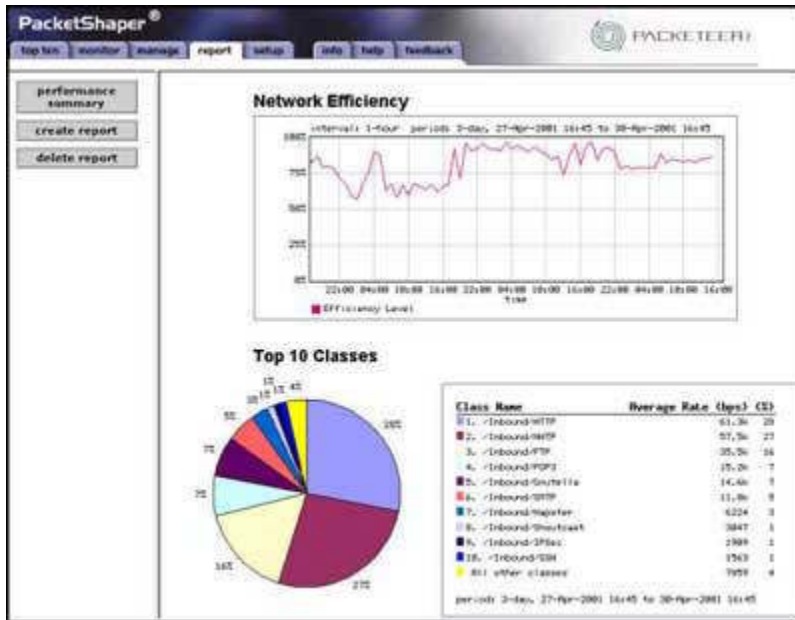


Figure 2. A screen shot of PacketShaper showing network monitoring statistics (Packeteer, Inc., “4-Steps”).

The University of California, Irvine (UCI) is one university that has PacketShaper in use to control P2P traffic on the dorm network. The network staff found that over 50% of the network traffic going outbound to the Internet came from one P2P app. UCI started using PacketShaper in the Fall of 2002 to identify and prioritize network traffic by applications, so that P2P apps are given a significantly lower priority than e-mail and web browsing. In addition, any traffic to any official campus computer is not managed by Packeteer because UCI assumes that traffic as “educational” traffic. P2P apps are limited to 10 Mbps of bandwidth if it is available out of the 60 Mbps of total bandwidth for the dorm network. UCI made it clear to their dorm residents that PacketShaper is used only for network performance management and would never invade the privacy of the residents--such as finding out what Web sites are visited (The Regents of the University of California).

There are new P2P detection tools that can detect encrypted P2P sessions such as P2P WatchDog (<http://www.p2pwatchdog.com/home.html>), which uses stateful packet inspection to detect which users are using P2P apps even if the P2P file transfer sessions are encrypted. Currently P2P Watchdog can detect SSL-encrypted P2P file transfer sessions on any port, tracks sessions that are hiding behind HTTP proxies, and can integrate with many popular firewalls to block file transfers. P2P WatchDog can be used without a firewall and is capable of blocking many P2P sessions by remotely resetting the TCP connection. P2P WatchDog is able to identify encrypted P2P sessions by using special techniques for identifying encrypted data streams and determining their origin (MesoCom, LLC).

One P2P management tool fingerprints music files is Audible Magic’s CopySense Appliance (http://www.audiblemagic.com/copysense_appliance.html), which can log, limit,

filter, and block P2P traffic. What is unique about this tool is that it utilizes a database of file signatures for copyrighted media (Audible Magic Corporation, "Audible"). Audio Magic uses its proprietary technology to dynamically identify "audio content by using psycho-perceptual measures of the content itself for recognition." The CopySense Network Appliance is integrated with the world's largest reference database music, which can identify over 3.5 million recorded songs (Audible Magic Corporation, "Content").

Some universities are developing their own tools to manage P2P traffic. At the University of Florida, they had a record 3,500 Kazaa file transfer sessions in 2002. The university faced with distinguishing legal and illegal P2P file transfers and stopping the illegal transfers. The university's IT staff developed a homegrown network tool named Icarus and within an hour of putting it into production, they saw an 86% drop in illegal P2P uploads from the dorm network to the Internet. They also noticed overall downloads dropped by 30% to the dorm network (King, p1). Icarus stands for Integrated Computer Application for Recognizing User Service and it combines data from the university's various different network management systems so that the data can be examined as a whole in a database. When Icarus detects P2P activity on the dorm network, it sends a pop-up message to the user's computer. First-time violators are directed to the university's network usage policy Web page and shown specific details about the violation. Second-time offenders are cut off from the Internet for five days, but are able to access the university's Intranet resources. Third-time violators are cut off from all network connectivity and then referred to the university's judicial affairs office. Since September 2003 to December 2003, Icarus has caught 919 first-time violators and 9 second-time violators. The university plans to release Icarus as an open-source project in spring 2004 (King, p. 2). When Icarus becomes available to the public in spring of 2004, it can be downloaded at <http://www.icarus.ufl.edu/> (the Web site is still being built). Icarus will be compatible across many platforms such as FreeBSD, Linux, and Windows. The hardware requirement for Icarus depends on how many users are on the LAN and the greatest overhead is the database. Icarus requires Perl support because it uses Perl as its main engine. Icarus supports many types of database packages because it is SQL 99-compliant. According to Rob Bird, network services supervisor at the University of Florida, it is normal if Icarus collects 2 to 5 GB of data per day on a 10,000-user enterprise LAN. The current Icarus software at the University of Florida uses a dual-processor Intel server with 225 GB RAID 10 storage (Betts). Icarus might be a good tool for universities that have a tight budget but need a tool to manage their P2P traffic problems.

Issues with P2P Monitoring

When creating a plan to manage illegal P2P file transfers, there are some issues to consider that are brought up by the Electronic Privacy Information Center (EPIC). EPIC, a non-profit research center that focuses on privacy and civil liberties rights, wrote a letter in response to the RIAA letter that was sent to

2,300 universities. The EPIC letter raises the questions of the proper role of colleges and universities regulating private conduct. The EPIC letter told the higher education institutions to review the concerns of network logging, privacy issues, and security risks in the higher education environment:

- **Network monitoring can affect students' ideas**—the RIAA wants university administrators to detect illegal P2P file sharing which could mean network administrators might have to look into the content of communications. Studies show that monitoring can make students worry and affect their creativity. Academic settings are supposed to be open and not have someone “look over your shoulder.” EPIC is concerned that that network monitoring system will evolve from logging illegal P2P activity into general data surveillance of students. In addition, before a policy is implemented there should be student input for the policy to be effective. The policy should take into student's views of academic freedom versus copyright law enforcement.
- **Monitoring students' network usage requires data protection requirements**—the Federal Educational Rights and Privacy Act (FERPA) and a 1997 CAUSE report (Association for Managing and Using Information Resources in Higher Education) requires protection of student records that are result from network monitoring. This would include only collecting the least amount of data that is necessary, notification of policies, limits on secondary use, nondisclosure and consent, authorization before allowing third parties to access data, data accuracy, inspection, review, information security, integrity, education, and accountability.
- **Network monitoring and enforcement can impair overall network reliability and performance**—universities should leave the judgment of innocence or guilt to the courts, and not use scarce university staff and resources to “prosecute” students. It might be better to not block the default P2P ports because P2P clients would easily bypass that and use port 80 or encrypted traffic, forcing universities to analyze the content of the traffic. If the university allows reasonable use of P2P apps, they can more easily identify P2P traffic for fair bandwidth allocation and would not need to use any techniques that may invade students' privacy (Pruitt).

Conclusion: The outlook of P2P management for dorm networks

Since higher education institutions are in an academic setting, they will face more problems with illegal P2P file sharing than corporations will. There has already been lawsuits filed against students and subpoenas issued to universities. Although recently the court has made it more difficult for the RIAA to issue subpoenas, nobody can predict if the courts will change their minds in the future and force universities to increase the level of monitoring of students' P2P file sharing habits. Until then, it is still important for universities to manage P2P apps on their dorm network because of bandwidth, ethical, and potential legal issues. With the combination of dorm network security policies to inform

students of the rules and enforcement of the policies, it should deter many students from using P2P apps for illegal file sharing. Many tools can be used to manage the usage of P2P apps including port blocking and bandwidth management appliances such as Allot Communication's NetEnforcer and Packeteer's PacketShaper. However, precautions need to be evaluated to preserve the academic freedom of a university setting and avoid invading students' privacy rights.

The problem of illegal P2P file sharing in dorms will probably continue until students find an alternative method of downloading music. The Joint Committee of the Higher Education and Entertainment Communities was formed in fall of 2002 to create solutions for music piracy in higher education institutions. The organization is launching a test project in spring of 2004 for legal online music downloads. Dorm residents would be charged a fee with their room and board fee, much like cable TV fees for their dorm rooms (Mark). The effectiveness of this service is unknown until the test results of this legal online music downloading service in dorm rooms are available. However, the results will probably be on the positive side as online music services such as iTunes have sold 20 million songs in less than 7 months (Michaels). Hopefully, the future of illegal P2P file sharing will be displaced by legal music downloads in university dorm networks.

© SANS Institute 2004, Author retains full rights.

References

Allot Communications Ltd. "NetEnforcer Data Sheet." Allot Communications Web Site. URL: http://www.allot.com/html/products_netenforcer_enterprise.shtm. (1 Jan. 2004).

Audible Magic Corporation. "Audible Magic CopySense Network Appliance." 1999-2003. URL: http://www.audiblemagic.com/copysense_appliance.html. (2 Jan. 2004).

---. "Content Aware Technology For Next Generation Solutions." 1999-2003. URL: <http://www.audiblemagic.com/technology.html>. (2 Jan. 2004).

Azusa Pacific University. "Peer to Peer File Sharing Policy." URL: <http://www.apu.edu/imt/peer-to-peer-file-sharing.php>. (1 Jan. 2004).

Betts, Michelle. "Sidebar: FAQ about the Icarus program for restricting P2P file sharing." 8 Dec. 2003. URL: <http://www.computerworld.com/news/2003/story/0,11280,87791,00.html>. (2 Jan. 2004).

Borland, John. "Campus File Swappers to Pay RIAA." 1 May 2003. URL: <http://news.com.com/2100-1027-5070407.html>. (3 Jan. 2004).

---. "Court: RIAA Lawsuit Strategy Illegal." 19 Dec. 2003. URL: <http://news.com.com/2100-1027-5129687.html>. (3 Jan. 2004).

---. "Colleges Making Dent in Campus P2P." 2 Sept. 2003. URL: <http://news.com.com/2100-1027-5070407.html>. (3 Jan. 2004).

---. "In Refugee Camp, a P2P Outpost." 14 Aug. 2003. URL: <http://news.com.com/2100-1027-5063402.html>. (3 Jan. 2004).

Cole, Eric, et al. Sans Security Essentials with CISSP CBK, Volume 1. Version 2.1. United States of America: The SANS Institute, 2003. 341, 693.

Cox, Beth. "RIAA Trains Anti-Piracy Guns on Universities." 30 Jan. 2003. URL: <http://www.internetnews.com/bus-news/article.php/1577101>. (30 Dec. 2003).

Falcon I.T. Services. "Kazaa Peer to Peer File Sharing & Security Issues, Miami, Dade County, Florida." URL: http://www.miguelfra.com/services/documents/kazaa_security_issues.htm. (1 Jan. 2004).

Gasior, Geoff. "Icarus blocks P2P on campus network." 3 Oct. 2003. URL: <http://www.tech-report.com/onearticle.x/5727>. (31 Dec. 2003).

Govindarajan, Shekhar. "Block Kazaa, Morpheus, LimeWire." 12 Sep. 2002. URL: <http://www.pcquest.com/content/p2p/102091201.asp>. (3 Jan. 2004).

Harrison, Ann. "Are lawsuits intimidating students?" 25 Sep. 2003. URL: <http://www.nwfusion.com/newsletters/fileshare/2003/0922p2p2.html>. (30 Dec. 2003).

King, Julia. "Preventing P2P Abuse." 8 Dec. 2003. URL: <http://www.computerworld.com/managementtopics/management/story/0,10801,87789,00.html>. (2 Jan. 2004).

Mark, Roy. "College File Swapping: Making the Illegal, Legal?" 2 Sep. 2003. URL: <http://dc.internet.com/news/article.php/3071331>. (30 Dec. 2003)

McCullagh, Declan. "RIAA Apologizes for Erroneous Letters." 13 May 2003. URL: <http://news.com.com/2100-1025-1001319.html>. (3 Jan. 2003).

MesoCom, LLC. "P2P WatchDog: Monitor and Block P2P (Peer-to-Peer) File Sharing." URL: <http://www.p2pwatchdog.com/home.html>. (1 Jan 2004).

Messmer, Ellen. "Tricky Worm Triggers New P2P Alarms." 19 May 2003. URL: <http://www.nwfusion.com/news/2003/0519fizzer.html>. (1 Jan. 2004).

Michaels, Philip. "iTunes Music Store: 20 million served and growing" 9 Dec. 2003. URL: <http://maccentral.macworld.com/news/2003/12/09/lowe/>. (30 Dec. 2003).

P-Cube Inc. "Controlling Peer to Peer Bandwidth Consumption." 1999-2003. URL: http://www.pcube.com/doc_root/products/Engage/WP_Controlling_P2P_Bandwidth_Use_31403.pdf. (31 Dec. 2003)

Packeteer, Inc. "4-Steps to Application Performance." 1996-2003. URL: http://www.packeteer.com/prod-sol/products/packetshaper_steps.cfm - analyze. (3 Jan. 2004).

---. "PacketShaper Datasheet." 11 Nov. 2003. URL: <http://www.packeteer.com/prodsol/resources/?attrvalue=7&subhead=Datasheets>. (1 Jan. 2004).

Piccard, Paul. "Risk Exposure: Instant Messaging and Peer-to Peer Networks v2.0." URL: http://documents.iss.net/whitepapers/X-Force_P2P.pdf. (2 Jan. 2004).

PR Newswire. "Leading Universities Implement Allot's NetEnforcer to Manage Network Traffic and Control Music Downloads; Louisiana State University and the University of Miami Select High-Performance NetEnforcer AC-1000." 7 Oct. 2003. URL: http://www.findarticles.com/cf_dls/m4PRN/2003_Oct_7/108581067/p1/article.html. (1 Jan. 2004).

Pruitt, Scarlet. "Privacy Group Warns Colleges against P2P Monitoring." 8 Nov. 2002. URL: <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,75758,00.html>. (3 Jan. 2004).

The Regents of the University of California. "Bandwidth! How the Residential Network is handling it." 1 Oct. 2002. URL: <http://resnet.uci.edu/bandwidth.html>. (1 Jan 2004).

Remington, Michael J. "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks." 8 Aug. 2003. URL: <http://www.acenet.edu/washington/legalupdate/2003/P2P.pdf>. (31 Dec. 2003).

SurfControl plc. "Peer to Peer (P2P) File Sharing." 2003. URL: <http://www.cyberpatrol.com/resources/p2p.aspx>. (30 Dec. 2003).

Vance, Ashlee. "Did Loyola University Chicago Lose Its Innocence to the RIAA?" 1 Aug. 2003. URL: <http://www.theregister.co.uk/content/6/32126.html>. (3 Jan. 2004).

© SANS Institute 2004, Author retains full rights.



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS India 2010	Bangalore, India	Feb 22, 2010 - Feb 27, 2010	Live Event
SEC540 VoIP Security Debut, San Antonio	San Antonio, TX	Feb 22, 2010 - Feb 27, 2010	Live Event
RSA Conference 2010	San Francisco, CA	Feb 28, 2010 - Mar 01, 2010	Live Event
SANS 2010	Orlando, FL	Mar 06, 2010 - Mar 15, 2010	Live Event
SANS Wellington 2010	Wellington, New Zealand	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS Dublin 2010	Dublin, Ireland	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS 507 Norway 2010	Oslo, Norway	Mar 15, 2010 - Mar 20, 2010	Live Event
SANS at FOSE, GovSec and US Law 2010	Washington, DC	Mar 23, 2010 - Mar 25, 2010	Live Event
SANS UAE 2010	Dubai, United Arab Emirates	Mar 27, 2010 - May 06, 2010	Live Event
SANS Northern Virginia Bootcamp 2010	Reston, VA	Apr 06, 2010 - Apr 13, 2010	Live Event
SANS 503 Norway 2010	Oslo, Norway	Apr 12, 2010 - Apr 17, 2010	Live Event
The 2010 European Community Digital Forensics and Incident Response Summit	London, United Kingdom	Apr 14, 2010 - Apr 20, 2010	Live Event
SANS Geneva CISSP at HEG Spring 2010	Geneva, Switzerland	Apr 19, 2010 - Apr 24, 2010	Live Event
SANS Toronto 2010	Toronto, ON	May 05, 2010 - May 10, 2010	Live Event
SANS Security West 2010	San Diego, CA	May 07, 2010 - May 15, 2010	Live Event
SANS Phoenix 2010	OnlineAZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced