Interested in learning more about security?

SANS Institute InfoSec Reading Room

The Real Cost of Free Programs such as Instant Messaging and Peer-to-Peer File Sharing Applications

As it is becoming ever easier for even a novice computer user to access and use freely available Instant Messaging programs, the security risks to all networks and need for public education increase dramatically. Without the awareness of the public as well as IT Managers, and the implementation of strict policies in regards to these programs, everyone is vulnerable. This paper discusses specific technical details and security risks of the four most popular Instant Messaging clients as well as several peer-to-peer file ...

The Real Cost of "Free" Programs such as Instant Messaging and Peer-to-Peer File Sharing Applications

Sigrun Grabowski
GSEC Practical Assignment V. 1.4b Option 1
July 1, 2003

Abstract

As it is becoming ever easier for even a novice computer user to access and use freely available Instant Messaging programs, the security risks to all networks and need for public education increase dramatically. Without the awareness of the public as well as IT Managers, and the implementation of strict policies in regards to these programs, everyone is vulnerable.

This paper discusses specific technical details and security risks of the four most popular Instant Messaging clients as well as several peer-to-peer file sharing programs. It then examines specific threats that are present for both these types of programs. Last but not least, it provides steps to ensure network security, and discusses the added vulnerability of not having policies in place.

Introduction

The most common Operating Systems (e.g. Microsoft Windows XP) and web browsers (e.g. Netscape) automatically install their own versions of Instant Messaging on a PC. A user actively has to turn off the automatic launching of either MSN Messenger or AOL Instant Messenger (AIM). Incidentally, these two products are also the most widely used Instant Messaging products, along with Yahoo Instant Messenger and ICQ.

The most common file sharing programs currently available are based on three different protocols. Fasttrack, used by KaZaA and others; Gnutella, which is both a protocol and a client; and WinMX. In addition to the threats below, these programs often come loaded with spyware. Since these products are not developed or published by major companies like Netscape, Microsoft and Yahoo, like the Instant Messaging clients mentioned, the download sources cannot easily be verified and the integrity of the installation or program file itself can be questionable.

Among the multitude of threats encountered in these products, these are the most prevalent and dangerous ones:

- Lack of Security
- Lack of Encryption
- Lack of Policy
- Lack of Education / Awareness
- Employee Productivity Loss when used in an office environment
- Legal / Copyright Infractions (file-sharing)
- Social Engineering Threats

[1]Osterman Research conducted surveys on Instant Messaging in March 2002 and September 2002. In March 2002, 29% of respondents said they were using Instant Messaging in their company. By September of 2002 that figure had increased to 42% of respondents. Once you added in unofficial use of Instant Messaging in the workplace, that figure jumped to 84% (in both the March and September surveys). Unfortunately, the surveys did not address the question of whether or not these companies have any policies regarding Instant Messaging in place, however, it is telling that 77% (again, same figure for both surveys) do not make any attempt to block Instant Messaging traffic.

[2]IDC forecasts the number of corporate IM application users to grow from under 20 Million in 2002 to over 200 million by 2006.

"IT managers are finding themselves in an environment where public Instant Messaging clients are prevalent, and thus they have inherited a non-corporate communications system that is insecure and unmanageable".

When looking at another survey, this one done by [3]Central Command in 2002 regarding Computer Security, it becomes apparent that file sharing programs are perhaps an even greater threat.

Question	**Total Number of People Surveyed**	**Total Responses to Question**	**Response**	**Percentage**
All Questions	943,026	66,296		
Current Use of Instant Messaging	943,026	40,994	Yes No	**39%** 61%
Acceptance and download of a file transfer from an unknown source	943,026	11,674	Yes No	**15%** 85%
Use of File Sharing Programs	943,026	46,850	Yes No	**48%** 52%
Aware of Risks of File Sharing	943,026	17,695	Yes No	39% **61%**

[1] Osterman Research Survey on Instant Messaging
[2] Emerging Threats to the Employee Computing Environment
[3] Central Command Annual Computer Security Survey Results for 2002

1. A look at the technical details

The purpose of this technical analysis of the services is intended to let the reader better understand how each program's methodology can be used to develop exploits and where the vulnerabilities lie.

1.1 Instant Messaging

Three companies offer the four free, popular Instant Messaging products: AOL owns both AIM and ICQ, Microsoft owns Windows Messenger / MSN Messenger, and Yahoo owns Yahoo Instant Messenger. None of these products are currently able to interact with each other, in other words, an AIM user cannot chat with a Yahoo IM user and vice versa.

[4]Each of these three vendors has their own, proprietary protocol that is used to facilitate the features of Instant Messaging.

- AOL uses a binary protocol named OSCAR for their popular AIM product. This same protocol with minor variations is also used in their ICQ service since 1998, when AOL purchased Mirabilis and decided to abandon the original ICQ protocol.

  AOL has a second protocol that is able to access AIM called TOC. AOL offers this less functional protocol (it only allows chatting and restricts maximum packet size) to allow third party vendors to write their own clients, and to aid the development of clients for non-Microsoft operating systems such as Linux. Contrary to OSCAR, AOL makes the TOC specifications publicly available.

  Besides chat, AIM offers the following main features: Inline Image Transfer in IM conversations (AIM only), Voice Chat, Game requests (AIM only), File transfers, File Sharing.

- Yahoo also uses a binary protocol, which is called YMSG.

  Yahoo Messenger allows for Voice/video chat, file transfers and file sharing besides chat.

- Microsoft, finally, uses an ASCII protocol called MSNP. The difference of using an ASCII vs. a binary protocol is that ASCII sends everything in human readable text.

  MSN has built in capabilities for Voice/Video Chat, Application sharing, File transfers, remote assistance and whiteboard in addition to Chat.

[4] [4] Hindocha, Neal - Threats to Instant Messaging (References used throughout this section)

AIM OSCAR Protocol

[5]Neal Hindocha of Symantec Security actually reverse engineered the AIM protocol to examine the packets, and gives header information for all three of the above protocols in his paper titled "Threats to Instant Messaging". The following details are comprised from the Header information in his paper and analysis of the header packets based on the SANS Security Essentials course material using Ethereal.

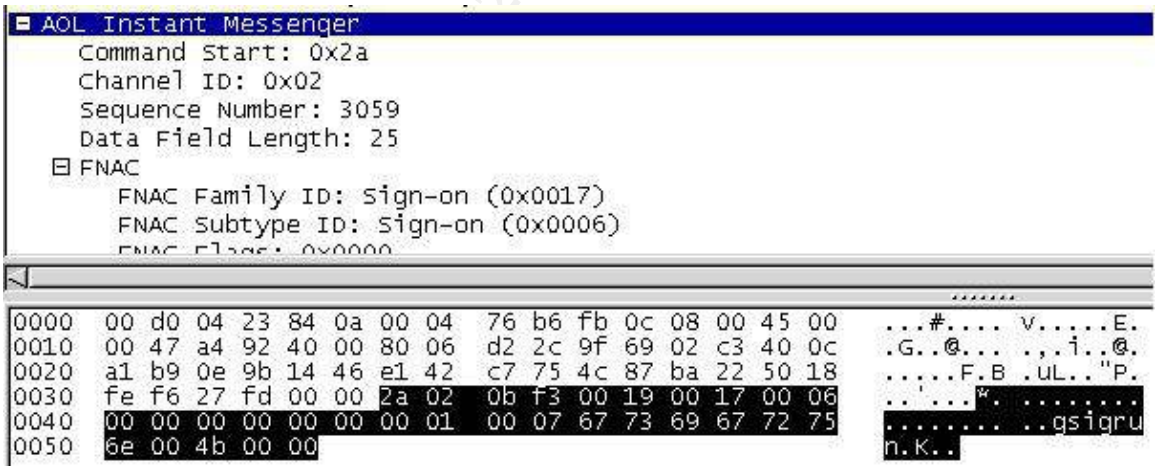
The OSCAR protocol's packets are called FLAP. There is a FLAP header in each FLAP packet. Within the FLAP packets are SNAC packets, which is the format most commands are sent in. The first 6 bytes of every AIM command are generally made up by a FLAP packet.

Note: SNAC packets are what these are identified as in Neal Hindocha's White Paper. The packets I captured with Ethereal designate the entire frame of the session below as "SNAC data, Family: Sign-on Username: gsigrun" and then show FNAC packets inside these SNAC packets.

The example below shows an AIM header captured by Ethereal with the individual elements highlighted. For each element, the type, identification and value is shown (e.g. BYTE, Start, 0x2A for the Command Start).

Entire AIM Header:

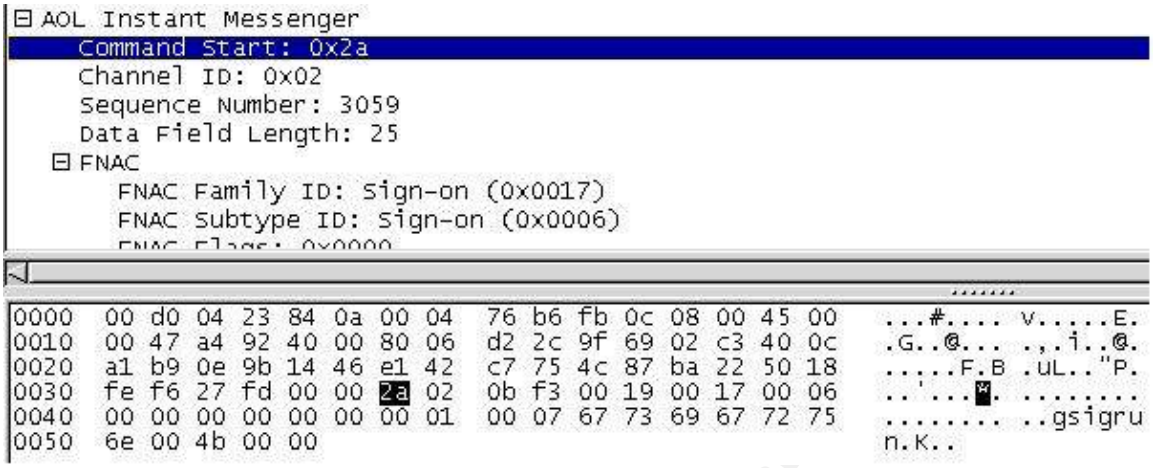
The AIM Header consists of 4 elements – the Command Start, Channel ID, Sequence Number and Data Field Length. Each of these elements is further explained below.



[5] Hindocha, Neal - Threats to Instant Messaging

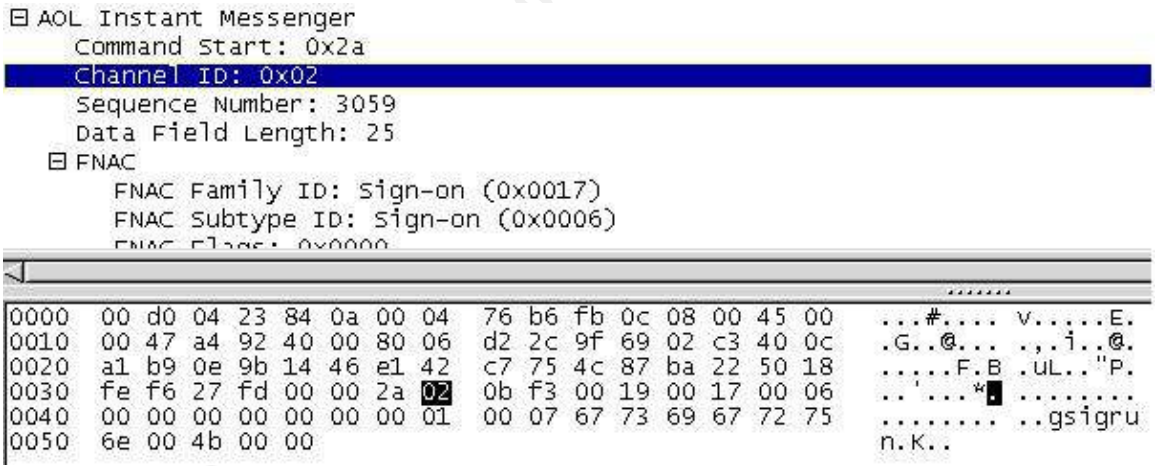
Type: BYTE ID: Start Value: 0x2A

The Command Start is always the same value – 0x2A.



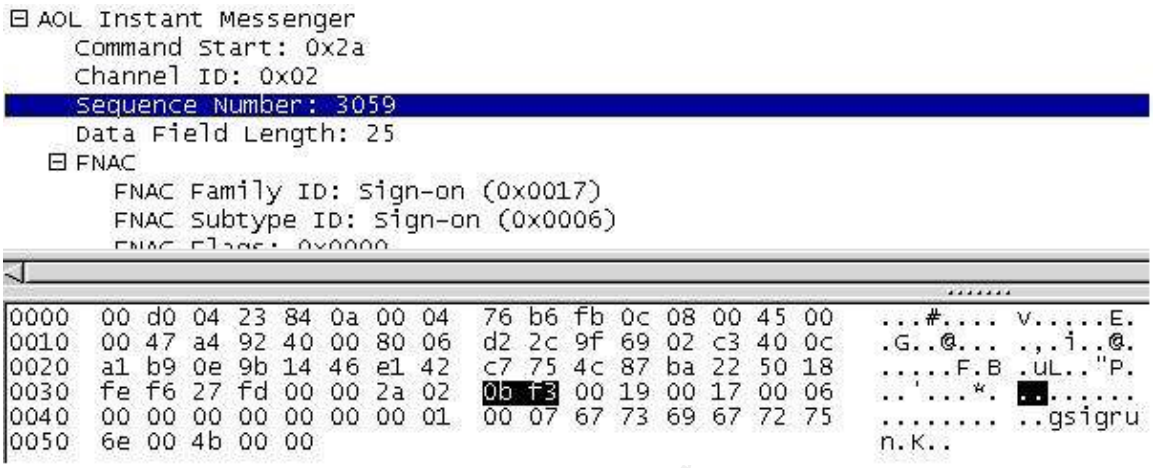
Type:BYTE ID: Channel Value: 0x01 (New connection)
0x02 (SNAC data)
0x03 (FLAP-level Error)
0x04 (Close Connection)
0x05 (Purpose unknown)

This indicates that the package carries SNAC data.



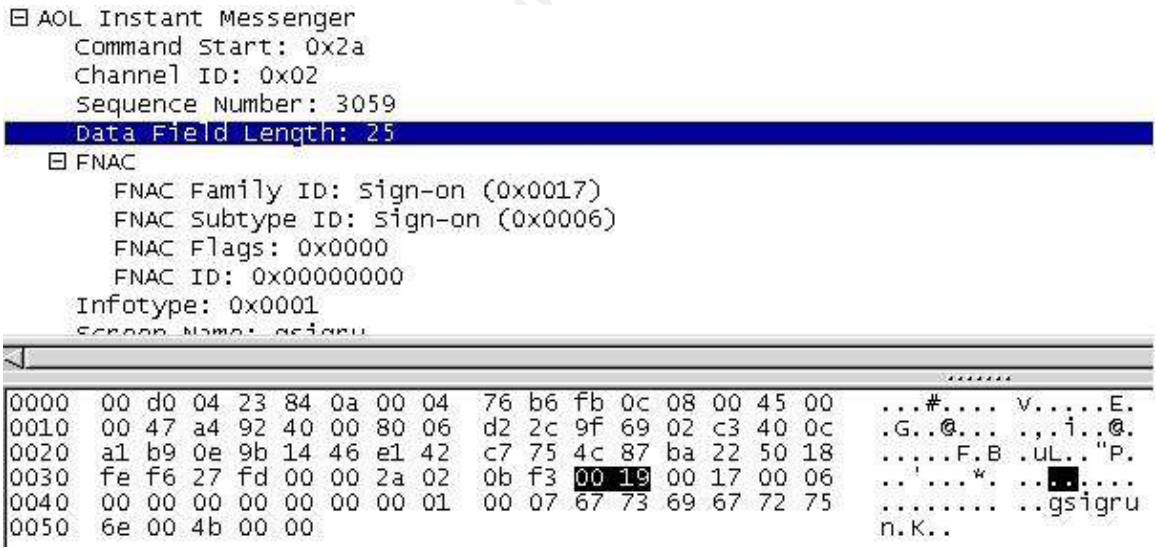
Type: WORD ID: Sequence Number Value: Variable

The sequence number of the first header sent by each the client and the server is a different random number, for each additional FLAP package, this number is incremented by one. The next package sent from the client to the server in this example session would be 3060.



Type: WORD ID: Data Value: Size

The data field of the FLAP header indicates the size of the data following the FLAP header. In this example, the size of the data is 25 bytes.

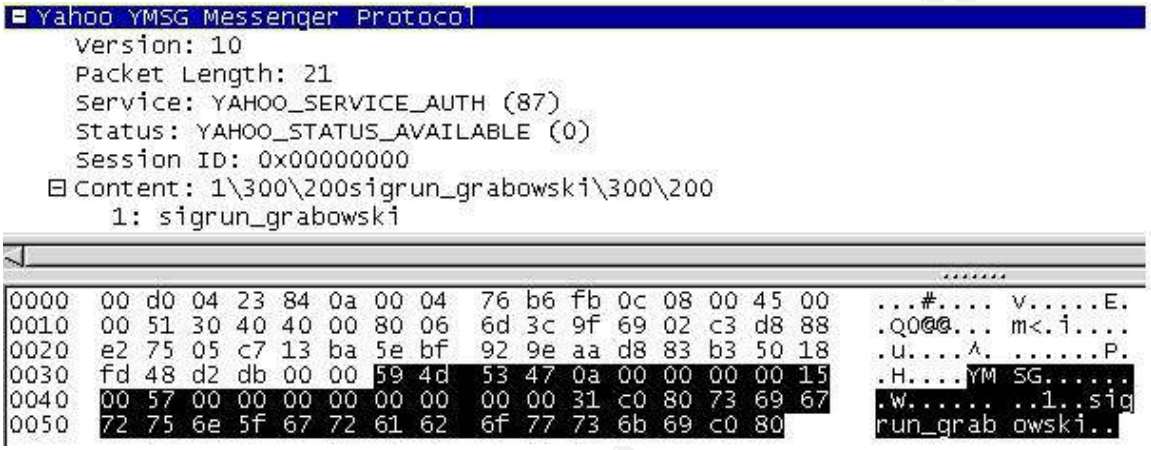


Yahoo YMSG Protocol

Again using information from Neal Hindocha's White Paper, "Threats to Instant Messaging", and the SANS course material, I have analyzed a session in Yahoo Instant Messenger that I captured with Ethereal.

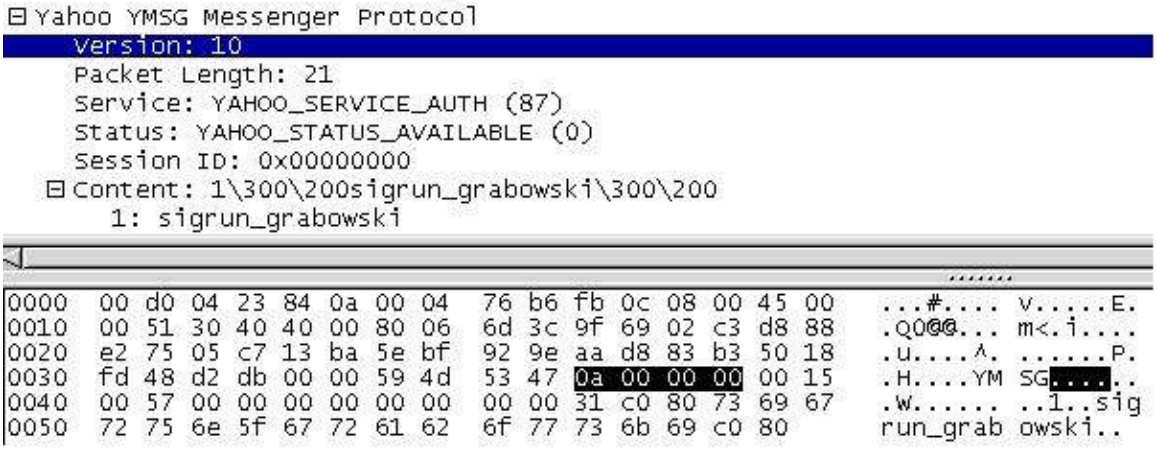
Entire YMSG Header

The YMSG Header consists of Version, Packet Length, Service, Status and Session ID.



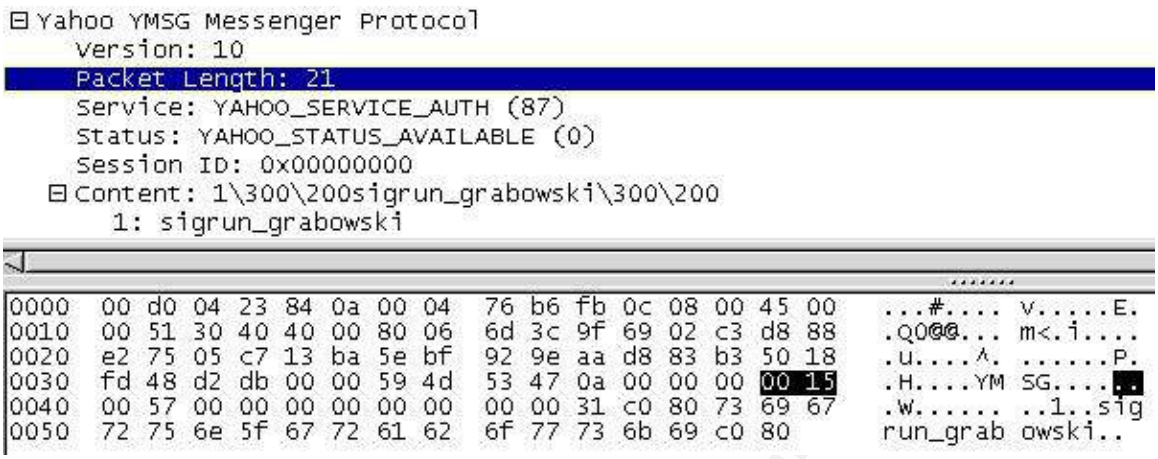
Type: BYTE ID: Protocol Version Value: 10

When sent from client to server, this value is the protocol version number (current Protocol Version Number is 10 for Yahoo Pager Version 5.5). If it is sent from the server to the client, the value is 0.



Type: WORD ID: Length Value: 21

Length of the data following the header (similar to the “Data” field in OSCAR).

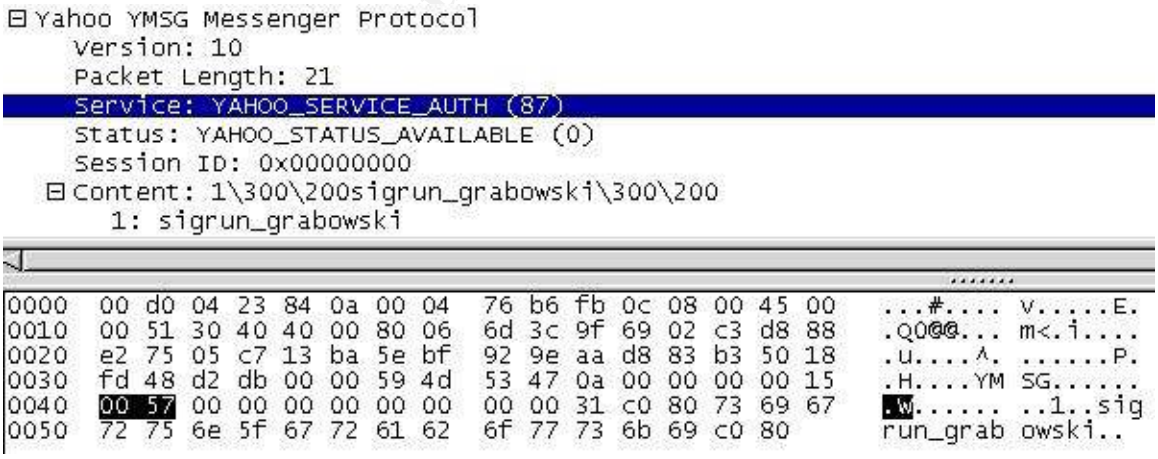


Type: BYTE ID: Service Value: 87

Specifies the specific service of the frame – in this case it is “Authentication” (87). Some of the services I have identified through Ethereal are:

(1) Logon	(6) Message
(21) Unknown	(22) Passthrough
(75) Service Notify	(76) Service Verify
(84) Authentication Response	(85) Service List
(87) Authentication	

In all, there are between 45 and 49 services (the exact number varies by source).

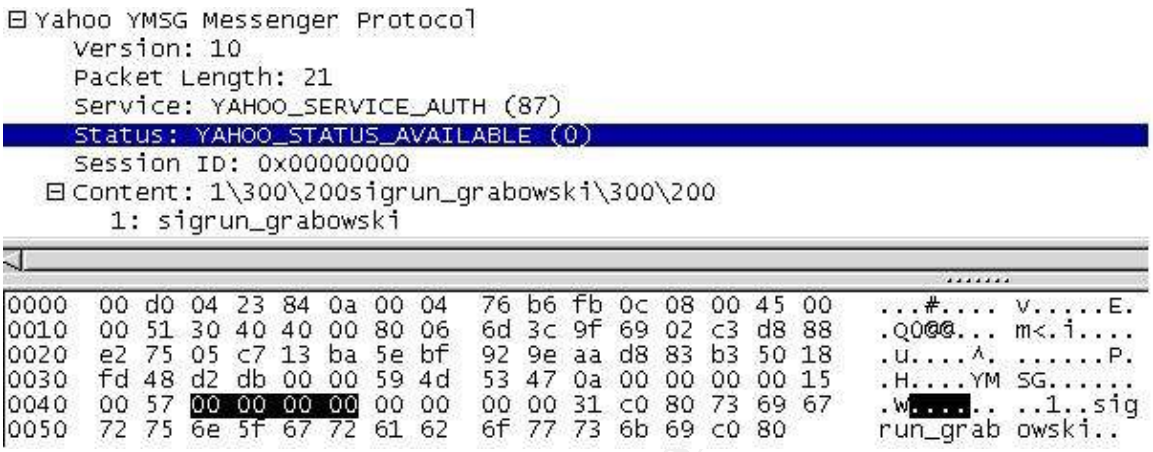


Type: BYTE ID: Status Value: 0

Shows the status of the service – in this case (0) Available.

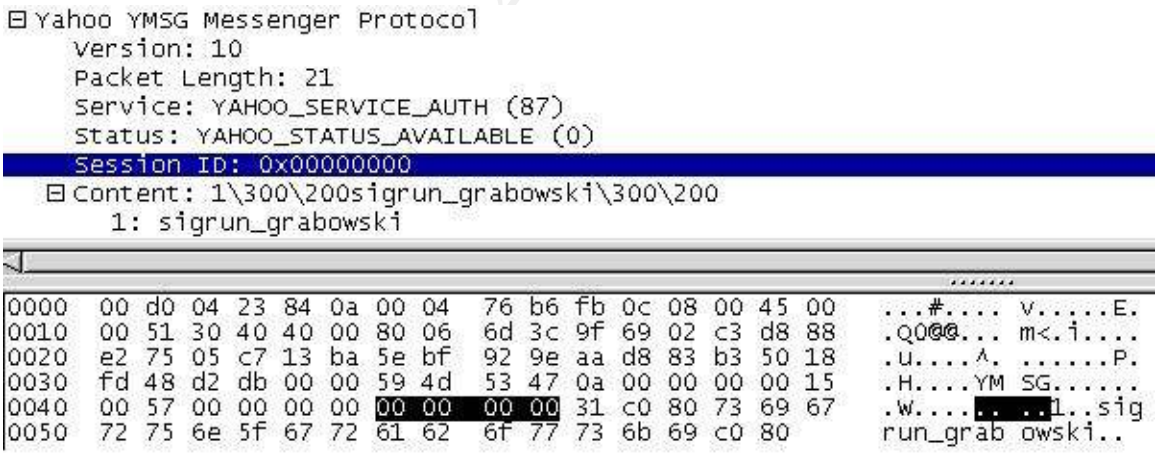
Status Codes I have been able to identify:

(?) Available	(1) BRB (Be Right Back)
(?) Busy	(22) Typing



Type: DWORD ID: Identifier Value: 0x00000000

The last piece of the header is the Identifier, or Session ID. The identifier is pseudo-random and is assigned at the beginning of a session, during which it remains a constant. The next session will have a different identifier.



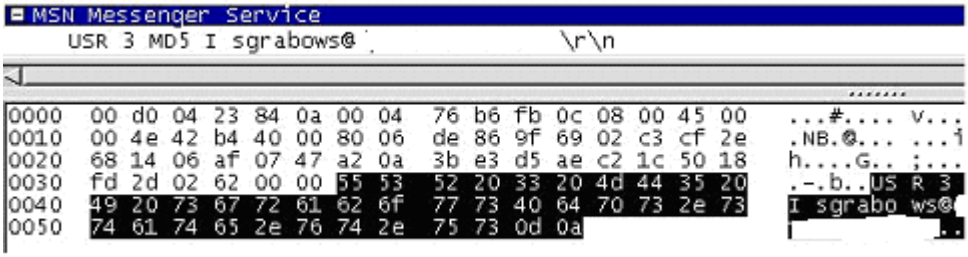
Windows/MSN Messenger MSNMS Protocol

As mentioned earlier, MSNMS is an ASCII based protocol. The sign-on session captured in Ethereal does not break down the header as it did in the previous examples.

Entire MSNMS Header

As you can see from this screenshot, it sends the following information in human readable text:

USR 3 – User ID
Md5 – MD5 hash of the password
Finally the username itself (*sanitized*)



Password Encryption

The following are the password encryption mechanisms used by each service:

- AIM/ICQ – challenge response method with a random challenge string sent from the server, which will be appended to the password by the client. The password and appended challenge string are hashed, and the hash is then sent to the server for verification.

- Yahoo Pager – challenge response method similar to AIM/ICQ.

- MSN Messenger – challenge response method using MD5 algorithm.

All of the services also generate and send a cookie that gets invalidated after the session.

1.2 Peer-to-Peer File Sharing

[6]There are three basic technologies used for these programs:

The simplest technology is based a one-to-one relationship, such as a file transfer from PC to PC. The now defunct Napster used a one-to-many relationship. Gnutella protocol based clients use a many-to-many relationship, enabling highly automated resource sharing among multiple nodes.

- "First generation" P2P used a centralized framework consisting of a centralized server maintaining directories of shared files stored on each node. This directory would be updated every time a client logs on or off the network. Performance-wise, this type of centralized network is most efficient, by requiring every client in the network to be registered, thus ensuring that searches are accurate, quick and efficient. No actual file is ever stored on the server; it maintains a pointer system to the actual location of the file. However, this centralization ultimately caused Napster's downfall due to legal implications.

File Transfer

- Second generation P2P networks started using a decentralized framework – the first version of the Gnutella protocol, for example. In this model, there is no server, and each PC connected to the network has equal status as a server and client. BearShare, Limewire and Gnucleus, among others, use this technology. While the robustness of this method is greater, since there is no danger of central server failure (if one client "falls off" the network, no one will notice), the performance of searches declines dramatically. The only thing that prevents a search sent via this protocol to go on to an infinite number of networked peers is the TTL – "time to live" constraint that is built into the client software. A query starts out with a typical range of 4-6, which is decremented and forwarded by

[6] Sandvine – Peer-to-Peer File Sharing (References used throughout this section)

each node. Once the TTL field is 0, the query will not be forwarded further. The replies from the nodes are then sent back to the originator via the same travel path.

- The current and third generation of file sharing applications still uses a decentralized framework; however, by adding some control to this framework, it essentially becomes a hybrid of the central server and decentralized methods. The latest version of the Gnutella protocol uses this technology, as do KaZaA, Grokster and Groove, which are based on the Fasttrack protocol. The way this works is by designating certain nodes within the framework as “super nodes”, which then act as traffic cops for the other nodes. These “super nodes” are appointed dynamically, based on bandwidth and network topology. A client now only has to keep a small number of connections open and each of these is to a super-node. Thus the network is scaled and lessens the number of nodes involved in message handling and routing, thereby reducing traffic volume. The speed of queries is much closer to the performance of the centralized framework in this model.

There are some other forms of peer-to-peer applications:
Direct exchange of services, such as disk storage, information and files;
Grid computing, which channels unused CPU cycles towards a common purpose (the SETI@Home project is a popular example of this);
Distributed information infrastructure, which brings together all information assets and resources of an organization and then forms a "Virtual Organization" (used typically in the healthcare industry or in scientific research and development).

Regardless of which type of P2P application is used, here is what a typical session will look like:

A P2P application will connect to a number of other P2P nodes on start-up. These nodes can be located anywhere on the network, and are rarely ever on the same network. Bandwidth is used on these connections in 2 ways – the actual client connection to the network and the downloading/transfer of files from one P2P host to another anywhere on the Internet. In addition, P2P connections generate so-called "protocol chatter" which is intended to keep the connections alive longer to aid in resolving searches quickly. Even when hosts are idle and not actively sharing files, protocol chatter takes up a notable share of bandwidth.

[7]Resnet did a study of bandwidth usage of several P2P file sharing programs. Gnutella based clients (tested with BearShare) had the highest overhead at startup, for a total consumption of 150-200 MB. Running the client for two days (without transferring files), produced consumption of about 3.4 GB a day. There is still a small amount of bandwidth consumed during and after shutdown of the client, until other hosts on the network remove the IP address from their cache. Comparatively, Fasttrack based clients (tested with KaZaA) used minimal bandwidth during the actual startup, but during

[7] RESNET

the next 28 hours used about 480 MB. In the steady state, daily traffic was 2.5 GB per day. Once the client was shut down, it continued to run in the system tray, and needed to be shut down again from there. After that, traffic ceased after about 2 minutes. Last but not least, WinMX used about 100KB during Startup. It was tested running for 8 days in Steady State (again without any file transfers), and generated about 550 MB of traffic during that time period. WinMX also did not truly shut down right away, but rather went to the system tray, and once shut down from there ceased all traffic.

2. THREATS

Now that we have learned about the way Instant Messaging and P2P programs connect and send their messages across a network and the Internet, we will take a look at some specific threats that are exploiting a number of weaknesses in these protocols.

2.1 Instant Messaging Threats

Few people realize how many threats there lurk in using a "simple" program like AOL Instant Messenger.

The widespread use of Instant Messaging has prompted hackers and virus writers to look for specific vulnerabilities in these programs for them to target.

Virus/Worm Threats

[8]Instant Messaging is vulnerable to Worms (a type of virus), however, no current Anti-Virus programs on the market are able to directly monitor instant messaging traffic, and only a very small number are able to plug into Instant Messaging to catch infected files when they are received. A lot of this is due to the continued evolution of Instant Messaging clients and protocols, as well as the difficulty of monitoring IM traffic. Thus, most server-based security products let these threats pass undetected.

Trojan Horses

Trojan horses are another danger. All popular Instant Messaging programs have file sharing capabilities, if not built in, at least attainable through patches or plug-ins. Instant Messaging uses already open, unsuspicious ports on the network, which makes it a lot easier for a hacker to access a system undetected. Thus, a desktop or perimeter firewall will let this traffic happen. With a Trojan Horse targeting Instant Messaging, a hacker will automatically be notified every time the victim is online and connected, opening the door for the hacker to do his destructive work. Some of these Trojans are able to modify configuration settings so the victim's entire hard drive is shared. [9]There is a small number of Trojans that will harvest things such as system information, cached passwords and IP addresses and then send that information back to the author of the Trojan, giving him information about other potential vulnerabilities of a user's system.

[8] Hindocha, Neal – Threats to Instant Messaging
[9] Hindocha, Neal – Instant Insecurity

Account Hijacking / Impersonation

Hijacking and Impersonation is another emerging threat to Instant Messaging. [10]Hackers can steal account information fairly easily either by using a password-stealing Trojan horse, or, connections can be hijacked via man-in-the-middle attacks, as none of the four Instant Messaging protocols encrypt their traffic. Since the server connection is kept open, the hacker can easily impersonate the victim. Having access to a user account also instantaneously gives the intruder access to the "buddy list", which eliminates the need to harvest IP addresses for further attack targets. While a user's IP address may change dynamically every time a user logs on, the username associated with Instant Messaging will likely never change.

Denial of Service Attacks

[11]While they are not really dangerous in this instance, Denial of Service attacks can also be easily launched against Instant Messengers, and are often used in conjunction with hijacking attacks.

Lack of Encryption

The lack of encryption of Instant Messaging traffic should also raise a red flag to companies whose employees may be using Instant Messaging to communicate sensitive data, which could be easily accessible to hackers. In addition, if IM is used for business purposes, also bear in mind other requirements regulating your industry – such as HIPAA in the healthcare industry, where Public Instant Messaging becomes a threat to the confidentiality of patient medical information.

The biggest threat for the future in Instant Messaging probably still lies in worms, which propagate ever more quickly after they manage to infect one system and the increase in worms targeting Instant Messaging is a threat. [12]Email, however, remains the number one target for worms and other malicious code. One of the factors holding back a more widespread attack on Instant Messaging through worms and Trojan Horses is the fact that proprietary protocols are in use at all four of the big Instant Messaging clients, which means a worm can only target one system. However, either interoperability between clients or market-share increase in one particular product may make Instant Messaging worms more prevalent in the future.

Bugs/Holes in Software

All of the Public IM clients have had major security related bugs in the software, mostly buffer-overflow vulnerabilities, that will leave targets wide open to attacks. While patches are usually provided by the companies, application and use of the patches is up

[10] Hindocha, Neal – Threats to Instant Messaging
[11] Hindocha, Neal – Threats to Instant Messaging
[12] Hindocha, Neal – Threats to Instant Messaging

to the individual user. In addition, not all holes are sufficiently patched the first time and new holes are usually not discovered until an exploit emerges.

New vulnerabilities are announced frequently. Below is a sampling of headlines that have circulated, encompassing all four of the popular Instant Messaging Products:

01/02/2002 Flaw May leave AIM Open to Attack
02/11/2002 MSN Messenger Security Hole Found
03/20/2002 Social Hacking hits IM
05/05/2002 AIM Vulnerability Resurfaces
05/29/2002 Security Bugs Squashed in Yahoo IM
06/06/2002 Holes Still Linger in Yahoo Messenger
12/12/2002 Shutting the Door on NetBIOS Spam
05/16/2003 Viruses Learn How to IM

There are efforts underway in the Public Instant Messaging market to make products interoperable, offer more security (for a price), but at the same time they also develop in the way of offering more features, such as video messaging, which no doubt will lead to more vulnerabilities.

2.2 Peer-to-Peer Application Threats

The waters are even murkier when it comes to threats aimed at P2P. Products come and go, and each new product opens up a new vulnerability. According to Websense, there are currently more than 130 unique P2P applications.

Legal Implications

The first risk factor is obviously the legality of downloads through these programs, which is now extending beyond audio files. There is an increasing trend to download popular video games, software programs and whole movies or TV shows. These downloads also exponentially increase the amount of bandwidth used. Use of one of these applications in a corporate environment can make the company liable for any damages should illegal file sharing happen through its equipment, in addition to using up valuable network resources.

[13]Using these programs in the workplace is very commonplace, as employees with slow home internet connections (less than 17% have high-speed access at home) will much rather download a full-length movie in a hour using the office's high-speed connection than the doing it at their homes with the download taking 23.5 hours on a 56k dial-up connection.

[13] Websense Press Release

Spyware

[14]Most every downloadable P2P application (KaZaA, AudioGalazy, BearShare, iMesh, and others) comes bundled with "spyware", a software that automatically installs when you install the P2P application, and gathers information about you and your surfing habits so it can then offer you specifically targeted pop-up ads. The programs also send back personal information to their creators. One particular spyware program, SAVENOW, while not sending back information, is the predominant marketing plague distributed. It will always run in the background on your computer, whether or not you are running the P2P application, and can use up as much as 28% of your CPU power and 8MB of RAM. While it can be uninstalled separately, or not installed if custom setup is selected, most users will just click through the setup and install the spyware programs unknowingly. ALTNET, which also comes with KaZaA, can NOT be uninstalled separately.

Another, even worse program, comes with Audiogalaxy. The Gator "Offer Companion" slowly downloads once Audiogalaxy is installed. Once Gator is complete it begins sending your personal information such as your e-mail addresses and Internet surfing interests back to the parent company who responds with pop-up adds and Spam e-mail to you and your friends.

There are removal and detection tools for spyware available, one of the more popular ones being Adaware. It is probably a good practice to install and run one of the products on a regular basis if you have used or are using P2P file sharing products.

Worms

Peer-to-Peer file sharing programs and networks are easily targeted by worms, but worse than that, the advertising software that comes with most of them can be a worm in itself. The behavior of these programs is worm-like, and the code of a lot of them is buggy enough to be able to cause damage to a user's system that would resemble that of a virus infection.

Denial of Service Attacks, file sharing of confidential documents, credit card fraud, child pornography are additional security risks associated with P2P file sharing.

For example, many parents think their children are safe because they use Internet Filtering to protect them from undesirable web sites, emails, etc. However, most filters do NOT filter peer-to-peer networking traffic. [15]Statistically, 35% of peer-to-peer downloads are pornographic in nature, including illegal child pornography. It is difficult to trace the origin of these files back and prosecute the offenders. In February 2003, Palisade Systems collected 22 million requests and searches conducted on the Gnutella network over a three week period, and then analyzed a randomly selected 400,000 of those. 97% of those searches could result in some sort of business or

[14] Spyware, P2P, and the Recording Industry
[15] Peer-to-Peer Pornography – Kids Know, Do Mom and Dad?

criminal liability, with 56% relating to copyright infringement, and 35% with possible grounds for sexual harassment charges. 42% of all requests monitored were for adult or child pornography, and 38% for copyrighted audio files.

[16]Another study made a fake e-mail inbox and a Microsoft Excel spreadsheet containing credit card numbers available through a peer-to-peer file sharing network. This often happens to users inadvertently when they open up their PC for sharing beyond the music files that they may want to share. Within a short period, users started downloading these files, and were obviously conducting specific searches for such material.

3. SECURITY MEASURES

There are a number of security measures that can be taken. It goes without saying that a firewall and Antivirus protection should be present and up-to-date, as well as managed properly. In addition to that, in an enterprise environment, the first decision you have to make is whether to allow these products at all.

Based on that decision, a policy can then be developed. That policy will be backed and strengthened by your physical security measures and level of enforcement. A signed user agreement acknowledging the policies are a good starting level to support enforcement.

3.1 Securing Instant Messaging

A defense in depth approach to secure Instant Messaging will include all of the elements listed below:

- Various levels of blocking at the firewall
- Anti-Virus Protection
- User Education
- Implementation of an Enterprise IM solution offering encryption (optional based on business need)
- Desktop Management
- Well defined Policies
- Intrusion Detection

Here is a more detailed description of these items:

Blocking at the firewall

You can attempt to block Instant Messaging completely by using your perimeter firewall. Even then, it is not possible to completely block any possibility of Instant Messaging being used in your enterprise.

[16] Kazaa & Others Expose Your Secrets

You would, of course, start by blocking the standard port Instant Messaging utilizes.

Default ports and services used for Instant Messaging are:

Application	Service	Port / Site
AIM / ICQ	IM, Voice/Video Chat, File Transfer, File Sharing	TCP 5190 (in) TCP 4099 (in) (but can use any open port)
	Image Transfer	TCP 4443 (in and out)
	Site for all services	login.oscar.aol.com
MSN Messenger	IM, Voice/Video Chat	TCP & UDP 1863
	File Transfer, File Sharing	TCP 6891 – 6900 (in and out)
	Application Sharing, Whiteboard	TCP 1503
	Site for all services	msgr.hotmail.com
Yahoo Messenger	IM, Voice/Video Chat, File Transfer, File Sharing	TCP 5050 (in and out)
	Site for all services	cs.yahoo.com

However, for all clients, the ports and servers are easily configurable to use something else, including HTTP port 80 and telnet port 23. All protocols also try a standard range of preconfigured ports if they find their standard ones blocked.

Now, you go a step further, and completely block login.oscar.aol.com or cs.yahoo.com, for example. The clients are smarter than that – they will now utilize an HTTP proxy server, which adds an HTTP header to all packets, thus eluding protocol based rules as well.

Last but not least, if you block the entire site, such as aol.com, there are freely available proxy servers on the Internet that can be used to access Instant Messaging.

Intrusion Detection

Intrusion Detection should be used to identify and log Instant Messaging traffic, which allows you to put a blocking mechanism in place based on the data collected.

Essentially, this means there is no way to block Public Instant Messaging from your enterprise 100%, even when Intrusion Detection is used. This makes it even more important to have sensible corporate policies in place that prevent employees from using Instant Messaging, and to enforce those policies.

Corporate Messaging Solution

On the other side of the coin, there is something to be said for a possible business need of Instant Messaging – it does make communication between employees easier,

especially if a company has multiple locations. If the decision of an enterprise is to sanction use of Instant Messaging as a work tool, then more secure products are available, which are suited for business use. This could be an enterprise Instant Messaging solution, such as Lotus Sametime or Microsoft Exchange Server. Another way would be to go with an add-on product such as Trillian or Akonix which offers monitoring, filtering and implementation of other security features for Popular Instant Messaging clients.

Policies

If you do decide to allow Instant Messaging in the Enterprise, with one of the above security measures in place, you still need a policy. Most companies already have policies in place that regulate e-mail traffic, and this policy can be used as a base model to develop your Instant Messaging Policy.

[17]The Iowa Enterprise Information Security Office has a good draft policy:

"INSTANT MESSAGING PROGRAMS. *An instant messaging program is a type of peer-to-peer program which is loaded on individual workstations that provide a communication method similar to e-mail. These programs are different from e-mail in that they don't store information on a central server. This configuration bypasses current methods of virus detection.*

THREAT *Currently, there are a variety of ways in which a network can be compromised including instant messaging. The risk in these programs is their capability of sending and receiving executable or other infected files directly to the workstations. The current providers of anti-virus software do not currently have a solution to protect instant messaging communications. Industry analysts are predicting that instant messaging will become the next avenue of introducing viruses. Some of these viruses have been known to not only infect the workstation itself, but to use the workstation as a method of propagation. They also may allow another computer to circumvent security controls and gain unauthorized access to the network.*

POLICY. *Effective immediately, all users must discontinue the use of these programs. Instant messaging programs shall not be used on ITD systems or ITD customer systems without the express written approval of the Enterprise Information Security Office. To initiate the approval process, contact the Enterprise Information Security Office. Covered by this policy are all forms of electronic communication, excluding electronic mail, which can transfer an executable file as an attachment or execute embedded code present in the message package. Not included in the above definition is any form of audio, visual, or text communication which cannot, as part of the communication, perform tasks outside of the message presentation or display. Electronic mail is covered in its own separate policy. To insure that installed instant messaging programs have been uninstalled correctly and that all associated files have*

[17] Iowa Enterprise Information Security Office

been removed, a trained information technology (IT) staff member must perform the removal. To initiate removal, contact the ITD Help Desk.

COMPLIANCE. *Systems currently logging any of the above mentioned or similar information shall cease logging this information as soon as possible. New implementations are to follow this policy. Contact the ITD Security Office to ensure that you are in accordance with this policy.*

All state of Iowa employees, interns, volunteers, and contractors of participating agencies that use, develop, implement, or maintain information technology systems covered by the Enterprise Security Policy (see Paragraph I.C) are responsible for understanding and complying with all state of Iowa enterprise information security policies, standards, processes, and procedures. This includes using, building, configuring, and maintaining systems in accordance with these policies, standards, processes, and procedures. Non-compliant situations will be brought first to the attention of the agency or the individual and efforts will be made to bring them into compliance. Depending on the severity, those who intentionally violate these policies, standards, processes, and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal, and/or criminal prosecution.

All necessary exceptions to this policy must be clearly documented and approved by the appropriate supervisor and the Information Security Office. In certain instances, agency head approval may be required."

A sample policy for Instant Messaging Use is offered by Info-Tech at http://www.infotechadvisor.com/solutions/IM/policy.doc.

Desktop Management

Of course, desktop management will also enable you to control what happens. It is customary for groups of users to have access to certain programs during the performance of their job duties, and these sets of programs will vary depending on your user group. Few companies include Instant Messaging into this category, they will provide the user with standard word processing software, the standard browser and e-mail program, but will happily let the user go to download AIM or Yahoo Messenger. If Instant Messaging is allowed in the enterprise, incorporate it in your standard set of desktop software; decide which product to go with and how to secure it.

3.2 Securing Peer-to-Peer File sharing

The following elements are all part of a good defense in depth approach to protect your enterprise from P2P File sharing Application security risks:

- Firewall blocking
- Spyware detection and removal
- Anti-Virus Protection

- User Education
- Desktop Management
- Well defined Policies
- Intrusion Detection

Contrary to Instant Messaging, there really is no justifiable business need to have one of these programs installed on your corporate desktop. So, how do you deal with this? As mentioned earlier, there are already over 130 different clients available, so how do you block them all?

Blocking at the firewall

Of course, you can access a list of all the current programs, their server addresses, if there is one, the ports they use and other information that you can than utilize to write a firewall rule that blocks this traffic. This list, however, will always be dynamic, and probably out of date by the time you implement the rule.

Using the principle of least privilege, it makes more sense to block everything that is not explicitly permitted. You will have to deal with occasional requests for legitimate access to a specific website that you may need to open up for someone to perform a job function. The other problem, however, is that if you implement this after users have already downloaded file sharing applications, the spyware that comes with them will continue to operate. So in addition to the firewall rules, you also need to implement desktop auditing and remove this software where it does not belong.

Similar to Instant Messaging, file sharing applications also have measures to reach their destination if their default ports and sites are blocked. KaZaA, for example, can be configured by a user with direct web access to use an external SOCKS 5 proxy server. Similar circumvention techniques are available in almost all clients. So, just as with Instant Messaging, there is no way to completely block all traffic unless Intrusion Detection is used.

Policies

Again, the best thing you can do is to have a good policy in place. A policy can be implemented in any organization, regardless of whether you would actually have the ability to block all unnecessary traffic. Many universities, for example, have this predicament, they can't justifiably block users from a variety of services, but doing that also leaves them open to the file sharing programs.

A well written policy, such as the one drafted by the [18]Iowa Enterprise Information Security Office can help protect your resources.

[18] Iowa Enterprise Information Security Office

*"**PEER-TO-PEER PROGRAMS.** A peer-to-peer program is a type of network in which programs or files loaded on individual workstations give equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads and have a security risk which allows for the misuse or abuse of another workstation on the network.*

***THREAT** Currently, there are a number of peer-to-peer programs that can be downloaded from the Internet. One example of these programs provides free music (NAPSTER) while another provides an opportunity to help use the local workstation as a slave to perform certain computations (SETI - Search for Extra Terrestrial Intelligence). Other programs have more legitimate purposes, such as the capability to collaborate on projects. Some of these products have been known to transmit and deliver viruses to not only the workstations installed with the program but other workstations that are in the same network environment. They also may allow another computer to circumvent security controls and gain unauthorized access to the network.*

***POLICY** Peer-to-peer programs shall not be used on ITD or ITD customer systems without the express written approval of the Enterprise Information Security Office. These systems will be installed and tested in a controlled environment and properly configured to ensure an adequate level of assurance. If an adequate level of assurance cannot be established, such programs will not be approved and an alternative method must be employed. To insure that currently installed programs have been uninstalled correctly and that all associated files have been removed, a trained information technology (IT) staff member should be notified to remove all pieces of the program and make any necessary registry changes. Contact the ITD Help Desk to facilitate this.*

***COMPLIANCE.** Systems currently logging any of the above mentioned or similar information shall cease logging this information as soon as possible. New implementations are to follow this policy. Contact the ITD Security Office to ensure that you are in accordance with this policy.*

All state of Iowa employees, interns, volunteers, and contractors of participating agencies that use, develop, implement, or maintain information technology systems covered by the Enterprise Security Policy (see Paragraph I.C) are responsible for understanding and complying with all state of Iowa enterprise information security policies, standards, processes, and procedures. This includes using, building, configuring, and maintaining systems in accordance with these policies, standards, processes, and procedures. Non-compliant situations will be brought first to the attention of the agency or the individual and efforts will be made to bring them into compliance. Depending on the severity, those who intentionally violate these policies, standards, processes, and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal, and/or criminal prosecution.

All necessary exceptions to this policy must be clearly documented and approved by the appropriate supervisor and the Information Security Office. In certain instances, agency head approval may be required."

[19]The Northern Illinois University has a different type of policy that actually allows the use of P2P file-sharing programs, but educates the users on the dangers and includes a clause relating to copyrighted materials.

In addition a policy regarding the use of illegal files – be it software, music or videos, should be a part of every employee's handbook – remember, the company can and will be held liable.

CONCLUSION

The risks of Public Instant Messaging and P2P File Sharing Applications are real and prevalent. What's more, most users are unaware of the multitude of dangers and threats associated with these programs.

IT Managers still ignore the threat of these products to a large extent and do not have proper policies in place. [20]In a survey done by SurfControl, 89% of IT Managers questioned acknowledged the serious risk to businesses caused by the use of IM and P2P, however, almost half of the companies surveyed did not have any technology or policy in place to deal with IM or P2P in the workplace.

There is still a lot of work to be done on this. The growth and evolution of the industry in both the Instant Messaging and P2P File Sharing sector presents new challenges every day. More research needs to be done to find out how to effectively block this traffic which is eluding firewall and IDS systems.

The time to take protective action is now. I am hoping this paper will raise awareness and provide a starting point for both IT Managers and users to secure their systems.

[19] File sharing programs secretly use your bandwidth
[20] Companies ignore IM risks

Bibliography

Bennett, Madeline. “Companies ignore IM risks.” May 12, 2003.
http://www.vunet.com/News/1140820

Burke, Brian; Christiansen, Chris; Kolodgy, Charles. “Emerging Threats to the Employee Computing Environment.” An IDC White Paper.
http://www.websense.com/products/resources/wp/emergingthreats_idc.pdf

Costello, Sam. “Akonix secures instant messaging, peer-to-peer.” June 10, 2002.
http://archive.infoworld.com/articles/hn/xml/02/06/10/020610hnakonix.xml

Couch, William. “Peer-to-Peer File Sharing Networks: Security Risks.” September 8, 2002. SANS InfoSec Reading Room.
http://www.sans.org/rr/policy/peer.php

Derby, Meredith B. “Instant messaging insecurity gains momentum.” May 1, 2002
http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci820928,00.html

Gerard, Mike (IT/CS). “Security Risks of Peer-to-Peer Software across the Internet.”
http://ref.cern.ch/CERN/CNL/2002/001/security/

Glass, Brett. “Kazaa & Others Expose Your Secrets.“
http://www.extremetech.com/article2/0,3973,9219,00.asp

Hindocha, Neal. “Instant Insecurity: Security Issues of Instant Messaging.” January 13, 2003.
http://www.securityfocus.com/infocus/1657

Hindocha, Neal. “Threats to Instant Messaging.” Symantec Security Response. October 2002.
http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf

Krim, Jonathan. “Pornography Prevalent on File-Sharing Services.” Washington Post. March 13, 2003.
http://www.washingtonpost.com/wp-dyn/articles/A17695-2003Mar12.html

Levitt, Jason. “Peer-To-Peer Anarchy: The Next Big Thing? May 15, 2000.
http://www.informationweek.com/author/internet35.htm

Lowe, Scott (MCSE). “Admins: Take control of your organization’s IM services.” Network Tech Review. February 1, 2002.
http://www.techrepublic.com/article_guest.jhtml?id=r00220020129low01.htm&fromtm=e036

Miller II, Stanley. “Peer-to-peer networks can’t be unplugged.” March 24, 2003.
http://www.jsonline.com/bym/tech/news/mar03/128038.asp

Naraine, Ryan. “Security Bugs Squashed in Yahoo IM.” May 29, 2002.
http://internetnews.com/dev-news/article.php/1146281

Reagan, Mike. “P2P shares more than meets the eye.” October 4, 2002.
http://zdnet.com.com/2100-1107-960638.html

Ropelato, Jerry. Peer-to-Peer Pornography – Kids Know, Do Mom and Dad?
http://www.internetfilterreview.com/peer-to-peer-file-sharing.html

Olavsrud, Thor. “Flaw May Leave AIM Open to Attack.” January 2, 2002.
http://www.internetnews.com/dev-news/article.php/10_947531

Saunders, Christopher. “Shutting the Door on NetBIOS Spam.” December 12, 2002
http://www.instantmessagingplanet.com/security/article.php/1556691

Singer, Michael. “Holes Still Linger in Yahoo Messenger.” June 6, 2002.
http://www.internetnews.com/dev-news/article.php/1331311

Woods, Bob. “Half of IM Users Accept Downloads.” September 26, 2002.
http://www.instantmessagingplanet.com/security/article.php/1470691

Woods, Bob. “MSN Messenger Security Hole Found.” February 11, 2002.
http://www.instantmessagingplanet.com/security/article.php/9

Woods, Bob. “Public IM: Are You In or Out?” October 14, 2002.
http://www.instantmessagingplanet.com/security/article.php/1481031

Woods, Bob. “Social Hacking Hits IM.” March 20, 2002.
http://dc.internet.com/news/article.php/994951

“AIM/Oscar Protocol Specification: Section 2: AIM Commands”
http://aimdoc.sourceforge.net/OSCARdoc/section2.html

“Annual Computer Security Survey Results for 2002.” Central Command.
http://www.centralcommand.com/safesurvey2002.html

“Beyond the Music: Peer-to-Peer File-Sharing Web Sites Grow 300 Percent.”
Websense Press Release. January 23, 2003.
http://www.websense.com/company/news/pr/03/012303.cfm

“Clients and Network Security”. CERT Incident Note IN-2000-08. Chat June 21, 2000.
http://www.cert.org/incident_notes/IN-2000-08.html

“File sharing programs secretly use your bandwidth”. Northern Illinois University.
http://www.its.niu.edu/its/helpdesk/bandwidth/allp2p.shtml

"Instant Messaging Security Policy". The Info-Tech Research Group.
http://www.infotechadvisor.com/solutions/IM/policy.doc

"P2P File-Sharing Risks." BizReport. March 24, 2003.
http://www.bizreport.com/article.php?art_id=4253&PHPSESSID=7860a8afd5770

"Peer-to-Peer File Sharing." An Industry White Paper. Sandvine Incorporated. December 2002.
http://www.lightreading.com/wp_redirect.asp?doc_id=24827

"Peer-to-Peer" and "Instant Messaging". Iowa Enterprise Information Security Office. June 7, 2002.
http://www.itd.state.ia.us/security/reading.html#

"Peer-to-Peer Networks Provide Ready Access to Child Pornography." GAO. February 2003.
http://www.gao.gov/new.items/d03351.pdf

Resnet
"Gnutella Bandwidth Usage". http://hf.utexas.edu/trouble/p2p-gnutella.html
'Fasttrack Bandwidth Usage". http://hf.utexas.edu/trouble/p2p-fasttrack.html
"WinMX Bandwidth Usage". http://hf.utexas.edu/trouble/p2p-winmx.html

"Risk Exposure Through Instant Messaging and Peer-to-Peer(P2P) Networks." ISS. April 2002.
http://www.itsecurity.com/papers/iss7.htm

"Securing Instant Messaging." Symantec Enterprise Security. White Paper. "
http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf

"Securing Public Instant Messaging in the Workplace." IM-Age White Paper. October 23, 2002.
http://www.im-age.com/_downloads/productselect.asp

"Social Engineering Attacks via IRC and Instant Messaging." CERT Incident Note IN-2002-03. March 19, 2002.
http://www.cert.org/incident_notes/IN-2002-03.html

"Survey on Instant Messaging March 12-18, 2002." Osterman Research.
http://www.ostermanresearch.com/results/surveyresults_im0302.htm

"Survey on Instant Messaging September 10-28, 2002." Osterman Research.
http://www.ostermanresearch.com/results/surveyresults_im0902.htm

Last Updated: January 22nd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS SEC455: SIEM Design Beta One 2018	Arlington, VAUS	Feb 12, 2018 - Feb 13, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VAUS	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
ICS Security Summit & Training 2018	Orlando, FLUS	Mar 19, 2018 - Mar 26, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Dubai 2018	OnlineAE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced