Global Information Assurance Certification Paper

Instant Messaging Security Concerns and Recommended Best Practices SANS Security Essentials GSEC Practical Version 1.4b

Francis J. Reiss
May 19, 2003

Abstract

Instant messaging is a popular tool that was primarily used by the personal user for chatting. Instant messaging has found its way into the corporate setting for inter-office communication because people can send a brief message to each other when both are online at the same time. There security concerns related to instant messaging that revolve around web based instant messaging. Instant messages are usually not encrypted and can easily be intercepted, spoofed or modified using various means that are available to hackers. Interception of instant messages can be a major concern to corporations who may be using web based instant messaging to exchange confidential or business proprietary messages. This paper discusses the popular instant messaging programs and their features, the security risks the instant messaging programs presents and will present methods to mitigate the risks associated with instant messaging based on best practices recommended for securing instant messenger services.

I. Introduction

Instant messaging has become an extremely popular and convenient communication tool that is not only in vogue with the personal user but has become entrenched in the corporate setting. In 2002, there were 80 million instant messaging users in the United States, and 25 million were business users, according to The Yankee Group. Those numbers are only going up: instant messaging is expected to post a compound annual growth rate of 150 percent through 2005, according to the latest Yankee Group forecast [1]. The instant messenger programs can be effective tools for communicating and sharing information, as they are easy to use and work across multiple platforms. According to Lee Smith, chief operating officer for Internet research company InsightExpress,

> "Instant messaging [is] a growing communication tool that is fast becoming a substitute for traditional methods of communication. Instant access helps people to do their jobs more efficiently than waiting for someone to call them back on the phone or find their e-mail from a week ago" [2]

While e-mail has virtually replaced traditional letters and even telephone calls as the choice for correspondence, with e-mail there is no way of knowing if the person being sent the e-mail to is online at that particular moment or not. Also, if multiple e-mails are being sent back and forth with the same person, there are normally a few steps needed to read, reply and send the e-mail. Instant messaging has gained popularity for inter-office communication because people can send a message to each other when both are

online at the same time because the user can maintain a list of contacts and see whether or not they are on line and then messages can be sent to any of the contacts on-line.

II. Instant Messaging Architecture

The majority of instant messaging systems employ client-server architecture. In the client-server architecture, the client is installed on a particular computer by the end user and provides the interface for the user's communication with other users who use the same system. The instant messaging server manages and relays all client/user communication and is not only responsible for delivering messages to the intended recipients, but is also responsible for authenticating users and verifying their online status. All users that sign up for instant messaging are given a unique identifier, which can be either a name or a number. The user then gives out the unique identifier to people that he or she wants to communicate with via the instant messaging network.

In most instances, users are not directly connected to each other and the messages are not sent from one user's computer directly to his or her buddy, but rather from the first user to an instant messaging server over the public Internet, and then down to the recipient. In almost all instant messaging systems, messages sent between users are plainly visible (unencrypted) and susceptible to eavesdropping. Messages and connection information are maintained on servers controlled by the provider of the instant messaging utility [3].

There are some instant messaging programs the use a peer-to-peer network architecture. The peer-to peer networks use an architecture in which all parties are considered equals. There is no central server and peers can associate and connect with each other directly. All peers can deliver messages and files without the aid of a centralized server. These peers can have multiple connections to other peers at any given time, and can communicate and send files to many different users simultaneously. The peer-to-peer scheme can offer better security than the client-server-client scheme when both users are on the same local area network because messages do not travel over the Internet. However, if one user is located outside the corporate network, messages sent between machines are exposed to potential eavesdroppers, just as in the client-server-client scheme [4].

III. Instant Messaging Capabilities

AOL Instant Messenger (AIM), MSN .NET Messenger, Yahoo Messenger, and ICQ are the more popular client-server based instant messaging programs. These instant messaging programs provide similar kinds of capabilities. Table 1 summarizes the capabilities of the different instant messaging programs and a brief description follows.

Table 1 – Instant Messaging Program Capabilities

Features	AOL	MSN	Yahoo	ICQ
Instant Messaging	X	X	X	X

Voice Chat	**X**	**X**	**X**	**X**
Video Chat		**X**	**X**	**X**
Application Sharing		**X**		
File Transfers	**X**	**X**	**X**	**X**
File Sharing	**X**		**X**	**X**
Game Requests	**X**			
Remote Assistance		**X**		
Whiteboard		**X**		
IM Images	**X**			

Instant Messaging

Instant messaging is simply the passing of HTML-encoded clear text messages from one user to another. These messages are not encrypted and are always routed over the Internet.

Voice/Video Chat

A direct connection must be stabled between the two users to enable Voice/Video Chat. The data is typically transferred via UDP connection. AIM only has voice chat and is handled in a manner similar to its instant messaging Images capability.

Application Sharing (NET Messenger)

Application sharing gives a remote user access to programs installed on a computer. Optionally, a user can give control of a program to a remote user. If a user accepts the invitation to share an application, the initiating user may select which of their own programs they wish to share with the other user. To achieve application sharing, a direct TCP connection is established between clients.

File Transfers

File transfers require a direct connection to be established between users. However, once a file transfer is complete the direct connection is closed.

File Sharing (AIM, Yahoo and ICQ)

File sharing allows a user to browse a selected directory structure and to download files. File sharing is optional capability that must be enabled in AIM and ICQ before any sharing can take place. However file sharing is enabled by default in Yahoo. The connection method for file sharing is the same as for a regular file transfer.

Game Requests (AIM only)

Game requests are simply requests for remote users to execute certain external programs, usually games. During game requests, no direct connection is made with

users via AIM. If the external application or game requires a direct connection, one may be set up. This is beyond the scope of AIM.

Remote Assistance (.NET Messenger)

Windows XP Professional and Home Editions contain the Remote Assistance utility, which allows a remote user to control another computer. The Remote Assistance feature in .NET Messenger launches this utility.

Whiteboard (.NET Messenger)

Whiteboard sharing is a way to share a Microsoft Paint document over a direct connection. It is identical to Application Sharing. Starting a whiteboard session with another user is a shortcut of invoking Application Sharer, then selecting Microsoft Paint as the application to share.

IM Images (AIM only)

IM images are sent via a direct connection with another user. The request is sent to the AIM server and is relayed to the target user. The request packet for direct connection contains the TCP/IP address and port information of the requester. These direct connections reveal the IP address of each participant.

IV. Vulnerability/Exploits/Threats to Messaging Programs

The majority of security concerns related to instant messaging revolve around web based instant messaging or instant messages being exchanged over the Internet. These messages can easily be intercepted, "spoofed" or modified. This is of major concern to corporations who use this web based instant messaging to exchange confidential or business specific messages [5]. Because instant messaging networks provide the capability to transfer text messages and to also the transfer files, instant messengers can also transfer worms and other malware. Instant messengers can also provide an access point for backdoor Trojan horses and allow a hacker to gain backdoor access to computers without having to open a listening port. This effectively bypasses desktop and perimeter firewall implementations. In addition to user-initiated file transfers, most of the major instant messaging networks support peer-to-peer file sharing where one can share a directory or drive. This means that all the files on a computer can be shared using the instant messaging client, leading to the spread of files that are infected with a virus or other malware [6].

Infected files

E-mails spreading infected files are a common occurrence and some of the worms have great success in spreading their infection due to social engineering or due to the usage of security exploits. Most of these e-mail threats can be dealt with swiftly due to antivirus products that monitor e-mail traffic, as well as the normal user being more

aware of them. The threat also exists to instant messengers programs from the transfer of infected files.

The number of instant messaging worms is rising steadily, but there are still no antivirus applications that directly monitor instant messaging traffic and only a few exist that directly plug in to instant messaging clients, notifying a user when a file is received. This is partly due to the difficulty in monitoring instant messaging traffic, as well as the constant modifications to the clients and the protocols that they use [1].

Some successful worms that have already infected instant-messaging clients, include Aplore, which spreads via AOL Instant Messenger (AIM); Goner, which takes advantage of ICQ; and CoolNow, Message from Jerry (also known as Hello), and Choke, which are all spread via MSN Messenger. Blitzdung is a mass-mailing worm that tries to send itself to all users found from Yahoo! Messenger log file. In addition to spreading itself the worm copies itself to windows root directory, tries to drop Elkern.C virus and Y3KRat backdoor and on certain dates tries to overwrite windows system files [7]. In the early part of 2002, the security organization w00w00 (www.w00w00.org) reported two buffer overflows in AIM that made it possible for an attacker to steal the buddy list and spread malicious code throughout the entire AIM community--as well as run malicious code on the person's computer [8].

There are also a handful of Trojan horse programs that target instant messaging. Some modify configuration settings so file sharing is enabled for the entire hard drive. These types of Trojan horses pose a large threat, as they allow anyone full file access to the computer. The benefit for a hacker using an instant messenger to access files on a remote computer instead of installing a backdoor Trojan horse is that even if the computer is using a dynamic IP address, the screen name will probably never change. Furthermore, the hacker will receive a notification each time the victim computer is online making much easier for the hacker to keep track of and access infected computers.

These backdoor Trojan horses may be harder to discover than the classic backdoor Trojan horses. Classic backdoor Trojan horses open a listening or outgoing port on the computer, forming a connection with a remote machine and can effectively be blocked by a desktop firewall. The backdoor Trojan horse, operating via the instant messaging client, does not need to open a new port and is not blocked by traditional desktop firewall products. The hacker does not need to open a new suspicious port for communication, but does so via already open instant messaging ports.

Unencrypted Communication

Few instant messaging systems encrypt messages as they travel from the client to the server and back to the second client. This data is potentially visible to eavesdroppers anywhere along its Internet path or within the INSTANT MESSAGING provider's network. Since the data that is being transmitted over the instant messaging network is not encrypted, a network sniffer, which can sniff data on most types of networks, can be

used to capture the instant messaging traffic. By using a sniffer, a hacker could sniff the packets from an entire instant messaging session. The hacker could gain access to privileged information, which can have serious consequences in the corporate environment, if proprietary or other confidential information is transmitted along the instant messaging network.

File Transfers Revealing IP Addresses

In addition to sending messages between users, instant messaging systems allow users to exchange files. Engaging in a file transfer, image transfer, voice chat, or file sharing can reveal a user's true IP address. Once an IP address is known, it is possible for a malicious user to concentrate on the system for the purpose of cracking it. It is also possible that this information can be used to make the computer a target or agent of a Denial of Service attack.

Social Engineering

The CERT/CC has received reports of social engineering attacks on users of instant messaging services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. Reports have also been received by the CERT/CC indicating that intruders are also using automated tools to post messages to unsuspecting users of IM services, typically offering the opportunity to download software of some value to the use. Once the user downloads and executes the software, their system is co-opted by the attacker for use as an agent in a distributed denial-of-service (DDoS) network. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner [9].

Theft of Identity

Many instant messaging systems are vulnerable to account hijacking or spoofing, allowing an attacker to hijack another user's instant messaging account and impersonate that user in conversations with others. Hackers can impersonate other users in many different ways. The most frequently used attack is simply stealing the account information of an unsuspecting user. Password protection is very limited in most instant messaging systems. Some IM systems store user passwords in data files on the client's PC. In some cases, these passwords are encrypted; in other cases, they are plainly visible. To get the account information of a user, the hacker can use a password-stealing Trojan horse. If the password for the instant messaging client is saved on the computer, the attacker could send a Trojan to an unsuspecting user. When executed, the Trojan would find the password for the instant messaging account used by the victim and send it back to the hacker. The means for sending back the information to the hacker varies. They include using the instant messenger itself, IRC, and e-mail.

Though more difficult, one can also highjack the entire connection by using a man-in-the-middle attack. Since none of the four major instant messaging protocols encrypt their network traffic, attackers can highjack connections via man-in-the-middle attacks. By inserting messages into an ongoing chat-session, a hacker could impersonate one of the chatting parties [1]. For example, a disconnect message, which appears to come from the server, can be sent to the victim from the hacker. This will cause the client to disconnect. The hacker can also use a simple denial of service exploit, or other unrelated exploits, to keep the client disconnected. Since the server keeps the connection open and does not know that the client has been disconnected, the hacker can then impersonate the victim user.

Denial of Service

Instant messaging may make a user's computer vulnerable to denial of service (DoS) attacks. These attacks may have different end results: some DoS attacks make the instant messaging client crash; others will make the client hang, and in some cases consume a large amount of CPU power, causing the entire computer to become unstable. There are many ways in which a hacker can cause a denial of service on an instant messenger client. One common type of attack is flooding a particular user with a large number of messages. The popular instant messaging clients contain protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that allow the hacker to use many accounts simultaneously, or automatically create a large number of accounts to accomplish the flood-attack. Adding to this is the fact that once, the flood-attack has started and the victim realizes what has happened, the computer may become unresponsive. Therefore, adding the attacking user accounts to the ignore list of the instant messenger client may be very difficult. Even though denial of service attacks are more of an annoyance than they are dangerous, they can be used in combination with other attacks, such as the hijacking of a connection [6].

V. A Best Practices Approach to Mitigate Threats

Security analysts for some time have been warning that unchecked use of such software could cause dangerous holes in enterprise firewalls, leading to sensitive corporate data being exposed on public networks and files being transferred in an unprotected fashion. Addressing the security issues of instant-messaging services present significant challenges since the various IM systems don't talk to each other, users often have to load several of them on one computer. All of the major IM clients have experienced security flaws at one point or another that were quickly fixed and were not taken advantage of by malicious hackers. As well, there have not been any major virus outbreaks, but the potential for malevolence always exists. Administrators attempting to block IM traffic by closing firewall ports have learned that these applications are "port agile", often rolling over to Port 80 and other ports which must remain open for users to access the internet. E-mail users have been well educated in the ways of virus protection as a result of various high-profile viruses. The dangers in

Instant Messaging are no different and good security measures should be maintained when using IM programs.

Blocking Instant Messaging

The most effective way of preventing instant messaging to jeopardize the security of a network and the machines upon it is to deny it access to the network in the first place. Given the risks involved in using public instant messaging systems, corporations should consider prohibiting the use of public instant messaging systems entirely, or ask employees to refrain from using public instant messaging systems for business communications. A general security practice for system configuration is to disable all services that are not needed. The same concept can be applied to network configuration. Unless the services provided by chat clients are needed, then it is encouraged that consideration be given to disabling chat functionality on the network. Preventing the use of instant messaging is difficult. Simple port blocking firewalls will not be effective because clients can use common destination ports such as HTTP port 80 and FTP port 21. Most of the instant messaging clients will even auto-configure themselves to use other ports than the default one if they are unable to communicate over the default port.

Best Practices Approach to Securing Instant Messaging

Many organizations give their employees access to instant messaging, since it can be a valuable communications tool. Therefore, the organization system administrator needs to ensure that the IM service is employed as secure as possible, which is not an easy task. There are several documents are have been written and available on the web that provided a great amount of information and detail on vulnerabilities of IM.

Establish a corporate IM usage policy

A recent studied cited that “Eighty percent of all network security managers who were surveyed last month [May 2002] at the Gartner Information Security Conference in Chicago, claim their biggest security threat comes from their own employees. Just as surprising is that 58% of those surveyed said the careless use of personal communications by their employees -- especially e-mail and instant messaging - poses the most dangerous security risk to their networks” [11]. The responsibilities/acceptable us should be clearly stated in the corporation’s security policy. Corporate policies are the best way to prevent employees within companies from using instant messaging. In order to ensure that instant messaging does not jeopardize the security of the organization’s systems, it should be clearly stated in any and all security policies that instant messaging will be permitted only with the express knowledge and consent of the organization. Users should be prohibited from sending confidential information over public IM systems as part of the overall security policy/acceptable use policy.

Properly configure corporate firewalls to block unapproved IM traffic

System administrators should configure perimeter firewalls to block all non-approved instant messaging systems. Given that the firewall must block both messaging and file transfers, adding firewall rules for both cases is also a good practice. To block messaging, an administrator may add rules to their firewall to block access to all popular IM servers. If this is not feasible, administrators can configure firewalls to block commonly used IM port numbers from all clients on the network. Note, however, that this still permits properly configured IM clients to tunnel through the firewall. To block file transfers, system administrators can identify the port number(s) used for peer-to-peer file transfers by each IM product and configure the firewall to block all communications over those port(s).

Deploy antivirus software and personal firewalls on all desktops

Because current corporate firewalls are unable to scan IM file transfers for computer viruses, worms, and Trojan horses, it is imperative to have up-to-date antivirus protection on all desktops, currently the last line of defense against IM-delivered malicious code. Personal firewalls should be configured to prevent uncertified and unapproved programs, including unapproved IM products, from communicating over the Internet. Desktop firewalls can provide more protection than a perimeter firewall because the desktop firewall can be configured to permit or deny communications on a per-program basis

Install patches to instant messaging software as soon as possible

System administrators need to apply new fixes as soon as possible when security holes or bugs are found in instant messaging systems. CodeRed, Nimda, and even the Internet Worm of 1988 all used known vulnerabilities to spread to new systems. It is likely there will be future attacks on instant messaging systems employing similar techniques.

Enforce client-side IM settings

If a corporation chooses to use an external instant messaging system properly configuring the instant messaging software is important. The instant messaging client should be configured so that they will accept chat requests only from users specified in employees' buddy lists. This prevents attackers from connecting to computers on the network and sending malicious code. Only those users explicitly specified by employees should be able to contact them. The instant messaging system should be configured to either block file transfers or allow such transfers only from users specified on the buddy list. If this is not feasible, configure the instant messaging software to prompt the employee before all file transfers. The instant messaging system should also be configured to use antivirus software to scan all file transfers, if this feature is supported. To prevent unsolicited chat requests, all the IM accounts should not be listed on public servers. Finally, for the best security, do not use any external IM system that does not employ a certified encryption system.

Monitor to ensure IM client policy compliance

Corporations should consider using software tools, to ensure that users don't change instant messaging client settings in a manner that violates company policy. Such tools can provide system administrators with an overall view of instant messaging policy compliance and facilitate the process of updating machines that violate policy. These tools also help administrators determine whether instant messaging software is up-to-date, whether users are running versions with security holes or buffer-overflow vulnerabilities, and whether users are running company-required antivirus and personal firewall packages.

For example, SurfControl [12] has a product for helping corporations manage the growing use of instant messaging and peer-to-peer file sharing. Their product enables companies to intelligently control the risks of unauthorized use of public instant messaging and peer-to-peer to increase network security, optimize network resources and bandwidth consumption, reduce legal liability and increase user productivity. The product has the ability to block and manage leading instant messaging protocols and can block and manage file-sharing protocols. It has also has network reporting capabilities that enable network administrators to gather and analyze data, such as usage patterns, by the type of instant messaging and peer-to-peer communication. [Note that this is not to be taken as an endorsement of SurfControl's product.]

Blue Coat's [13] instant messaging security products control users and their utilization of public instant messaging applications. Blue Coat's security policy architecture provides features that can controls which users are allowed to utilize Instant Messaging, but which instant messaging protocols are allowed, what features are to be enabled, to whom they may instant messaging or chat with (inside the company and/or outside the company), what time of the day they can instant messaging, how logging should be handled. [Note that this is not to be taken as an endorsement of Blue Coat's product.]

Deploy private corporate IM servers to isolate corporate messaging systems

If at all possible, a corporation should deploy a secure instant messaging server on the company network and configure all instant messaging clients to connect to this server. A number of private companies offer instant messaging products for sale to corporations. Deploying one or more instant messaging servers within the corporate network to ensure that all internal instant messaging communications are kept behind the corporate firewall is a valuable practice.

Secure the information being transmitted by encryption

There are currently several companies that have introduced business versions of instant messaging enhanced with encryption, security and authentication features. An example is Top Secret Messenger (TSM), by Encryption Software (www.encrsoft.com), which provides a secure public-key encryption with fully and has integrated plugins for popular instant messengers and e-mail clients such as, ICQ. MSN Instant Messenger

(Microsoft), and is currently working on plug-ins for Yahoo Messenger and AIM [14]. TSM is based on the highly complex and well accepted by leading mathematicians and cryptography specialists, Elliptic Curve Cryptography algorithm. It is considered by many to be a much stronger (requires significantly smaller key sizes for similar security) and more efficient alternative to RSA public-key encryption algorithm.

VI. Summary

Instant messenger programs can be effective tools for communicating and sharing information. Unchecked use of such software could cause dangerous holes in enterprise firewalls, leading to sensitive corporate data being exposed on public networks and files being transferred in an unprotected fashion. While the most effective way of preventing instant messaging to jeopardize the security of a network and the machines upon it is to deny it access to the network in the first place, instant messaging programs are rapidly growing as the preferred method of communication. Therefore, addressing the security issues of instant-messaging services present significant challenges to the system administrator and requires the development and enforcement of good security policies along with implementing best practices regarding the use of instant messaging.

References

1. Thorsberg, Frank. "Can Instant Messaging Really Be Safe?" 17 April 17 2003. URL: http://www.pcworld.com/news/article/0,aid,110301,00.asp
2. McAuliffe, Wendy. "Instant Messaging Boosts Business." 8 August 2001: URL: http://news.zdnet.co.uk/story/0,,t269-s2092767,00.html
3. "Securing instant messaging." The Symantec Advantage. Spring 2002, Issue 14 URL: http://www.symantec.com/symadvantage/014/instant.html
4. "Risk Exposure Through Instant Messaging And Peer-To-Peer (P2P) Networks." Internet Security Systems. April 2002. URL: http://documents.iss.net/whitepapers/X-Force_P2P.pdf
5. Instant Messaging Software. "Security Risks of Instant Messaging." http://www.instant-messaging-software.com/security-risks.htm
6. Hindocha, Neal. "Instant Insecurity: Security Issues of Instant Messaging." January 13, 2003. URL: http://www.securityfocus.com/infocus/1657
7. Niemela, Jarno. "F-Secure Virus Descriptions." February 2, 2003. URL: http://www.f-secure.com/v-descs/blitzdun.shtml
8. Vamosi, Robert. "Instant Messaging: The Next Hacker Target." May 29, 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2868239,00.html
9. CERT® Incident Note IN-2002-03. URL: http://www.cert.org/incident_notes/IN-2002-03.html
10. Vijayn, Jaikumar. "Security problems persist with instant messaging." May 9, 2003. URL: http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,81104,00.html

11. Woods, Bob. IM Use a Big Security Threat – Study." June 7, 2002. URL: http://www.guardent.com/docs/news/Internet.com%20EAI%20Knowledge%20Base.htm
12. SurfControl. "SurfControl Launches Instant Message Filter for Enterprises at RSA." URL: http://www.surfcontrol.com/news/newsitem.aspx?id=563
13. Blue Coat Systems. "Instant Messaging Security with Blue Coat Systems." URL" http://www.bluecoat.com/solutions/im_security.html
14. Encryption Software. "Top Secret Messenger. URL: http://www.encrsoft.com/products/tsm.html
15. Heim, Kristi. "Microsoft to push instant messaging for business." Mercury News. March 6, 2003. URL: http://www.siliconvalley.com/mld/siliconvalley/news/local/5335953.htm
16. Hindocha, Neal. "Threats to Instant Messaging." Symantec Security Response White Paper. URL: http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf
17. Zeichick, Alan. "Instant messaging made secure." Inforworld, March 07, 2003 URL: http://www.infoworld.com/article/03/03/07/10akonix_1.html?s=tc
18. http://www.gslis.utexas.edu/~lis312le/restrict/im/im.html several pages on how IM works
19. Study: Instant Messaging Use Is A Big Security Threat, June 24, 2002 By Bob Woods http://www.smallbusinesscomputing.com/webmaster/article.php/1369981
20. Willner, Susan. "Instant Messaging: How Secure is It?" August 19, 2001, URL: http://www.sans.org/rr/threats/IM2.php
21. Levine, Stuart. "Instant Messaging: How Dangerous is It?" May 19 2001, URL: http://www.sans.org/rr/threats/IM.php
22. Frase, Dan. "The Instant Messaging Menace: Security Problems in the Enterprose and some Solutions." January 31, 2002. URL: http://www.sans.org/rr/threats/IM_menace.php