Global Information Assurance Certification Paper

Susan Willner
GSEC Practical v1.2e

Instant Messaging: How Secure Is It?

Instant Messaging has become an extremely popular method of communication, especially among home internet users. It is rapidly making headway in the business sector as well. Many business users are putting messaging clients on their individual machines without company approval, causing companies to rush to add their own systems and attempt to maintain some semblance of control. However, before jumping on the instant message bandwagon, there are some security issues that should be considered. First, some background on the technology.

What is Instant Messaging?

Instant Messaging can be considered a hybrid of email and chat. Email allows one user to communicate with another (or several others) whether the recipient is currently on-line or not. Mail is stored in the recipient's mail box on his mail server until he retrieves it. The mail can include attached files and links to URLs. Chat, on the other hand, is a real-time communication medium and is dependent on both parties being on-line at the same time. This communication does not include file transfer capabilities. Instant messaging offers the best of both worlds. It allows for real-time communication and file sharing. There are two different perspectives: file transfer oriented with messaging capabilities such as the troubled Napster, and message oriented with file transfer capabilities such as AOL's AIM (Seifried).

Standards

There has been an ongoing standards war for control of the customer base. At one time the main players were AIM and ICQ. AIM is an AOL proprietary system. ICQ was an independent system. ICQ (and many others) tried, unsuccessfully, to make their systems interoperable with AIM. Each time, the systems would work together for only a matter of weeks before AOL would block access. "Odigo make its software interoperable with AOL's AIM and ICQ messaging services last year only to have AOL block Odigo users after a couple of weeks" (Vance). AOL cites privacy and security concerns for it's unwillingness to embrace an interoperable standard. Many vendors doubt this claim, and feel that the real issue is access to AOL's large customer base. A common viewpoint is that AOL will lose it's market share as IM becomes more popular. This is already starting to happen. Currently the main players are AOL and MSN Messenger, Microsoft's entry into the proprietary messaging game. While ICQ does still exist, it has been bought by AOL. Where AIM and ICQ once held about 80% of users (Vance), AOL now controls 52% of consumers and 40% of business users. MSN is rapidly gaining ground, and

controls 36% of consumers and 40% of business users (Perera). In the mean time, several vendors have banded together to develop a standard for interoperability called IMUnified. As of yet, they have not been able to get AOL to cooperate with them.

How does Instant Messaging work?

Instant messaging requires the user to logon to the IM server when he goes on-line. This logon can be done automatically whenever the user establishes an internet connection. This logon sends user information to the IM server, including the user's IP address and port. After logon, his presence is announced to anyone who is interested. He is also alerted as people on his buddy list sign on or off. He can then initiate conversations with anyone on his list. Because the server knows the IP address and port of each user, the conversation is done directly between the user machines, without any server involvement.

What are the dangers of Instant Messaging?

There are several issues of concern when using Instant Messaging.

1. It announces information, including IP address, about the user and his machine whenever he logs on.

   Probably one of the more worrying aspects of IM is that it announces the user's actual IP address along with the port it is using. "It [ICQ] sort of hides the IP address of the remote user, but since you char directly with them you can get the IP address by simply running 'netstat' or a related utility" (Seifried). If the user is connected via an "always on" method such as DSL, the IP address is assigned to that user rather than coming from a large pool as in a dial-up connection. This opens up the machine to potential targeting.

2. Just like e-mail, it is a prime target for nuisance messages, or "spam".

   To be fair, IM providers have thought about this, and are taking steps to minimize this problem. Spam may be considered to be more of an annoyance than a danger. However, it can cause a loss of productivity, especially in a business setting, and there is really no way to completely block these types of messages.

3. Because of the file transfer capabilities, viruses can be easily transmitted from one machine to another.

   This issue is another carryover from e-mail. As people are copying files from machine to machine, any virus that they've picked up along the way can propagate. "Microsoft recently warned MSN Messenger users that a strain of the W32 virus was being distributed using the chat client's file transfer feature" (Spring).

4. Users may end up with shared directories and/or file server capabilities on their machines.

   This is something that is much more likely with the IM services that are file based,

such as the old Napster and the newer Morpheus, but it still occurs on the chat based services as well. This causes not only privacy issues, but bandwidth issues as well, especially when using a service like Morpheus. If the service discovers that your machine has a lot of disk space and a large amount of bandwidth, you could end up not only downloading a file you wanted, but also then becoming the server for others who want to download that file. This is not such a risk on a home machine, but if a user sets up an unauthorized IM service on his business network, it could impact the network services of his whole company, by using both space and throughput.

Even AOL Instant Messenger, which is chat based rather than file based, gives you the option to become a file server and contains a directory that is shared by default.

5. As business users add unauthorized clients on their machines, they can open up their networks to unsecured traffic.

   As already pointed out, this can be a big problem when office users set up accounts with services such as Morpheus which are used primarily for file sharing. All of the above problems are concerns with a business network. While the administrator thinks that he is safe (or at least relatively so) by setting up firewalls and intrusion detection, the user has initiated a connection that will get through the firewall, and allow not only conversation, but also file movement. Suddenly there is a large gap that potentially harmful traffic can flow through. "Workers sometimes tap IM for corporate business, thus using the Internet to chat with someone down the hall, maybe sending company secrets across public networks. 'It's uncontrolled and making a lot of managers very nervous,' says Louis Latham of Gartner Group, a market-research firm" (LaGesse).

6. It is a simple matter to log complete conversations, and the user will not necessarily be aware of it.

   Depending upon the version of IM being used, conversations may be logged by default. Even if a user knows to turn off logging, that doesn't make him safe. The other user may log the conversation without any notice being given. This doesn't consider the possibility that law enforcement or the IM services themselves may log information (although the leading IM services do deny that they track where users go or log messages). The very nature of chat messaging also lends itself to conversations that are even more casual in tone than e-mail. Therefore, if these logs were given to others, they could prove to be damaging.

   This brings in confusing legal issues about privacy. For example, it's not clear whether wiretap laws could apply, since they refer to phone conversations. "Even though IM conversations often are conducted on the Internet and transmitted through phone lines, it's unclear whether laws applying to the phone can be applied to Instant Messaging" (Hu and Konrad).

How can these dangers be countered?

One thing to realize up front is that *Instant Messaging is not secure*. "Messages

and connection information are maintained on servers controlled by the provider of the IM utility that you use. Most utilities do provide a certain level of encryption, but they are not so secure that you should send any confidential information through the system. There have been reported cases of IM user logs being captured and used by nefarious sorts" (Tyson, 3). Any communication requiring secure connections simply cannot be handled using this medium. Having said that, it is possible to reduce some of the more glaring risks by careful configuration.

1. While there isn't any mechanism for disallowing the machine IP address, care can still be taken.

   Users should not use the automatic connection option that is available with most IM services. Instead, try to minimize connection time by using the service only when necessary. Many users will log on to their computers, and then stay logged on for the day, just locking the terminal when away from their desk. During these idle times, the connection should be logged off.

2. There is no way to completely block "spam", but there are mechanisms in place to minimize it.

   "For example, AOL limits the amount of text you can send through your chat client within a given time period. … MSN Messenger requires you to first request a dialog in order to initiate a chat session, so that the person at the other end can decline the virtual confab" (Spring). The text limitation will at least make it more difficult for a sender to send messages to large numbers of people at once. AOL also allows you to control who you receive messages from. When you receive a message, you can add the sender to your "block" list. "Blocking the other user prevents both of you from seeing each other in your Buddy Lists, and it also prevents both of you from sending each other any more messages" (AOL-FAQ).

3. The biggest key to file transfers and virus control is the same as for e-mail.

   First, know who you're getting files from. You must make sure they're from a reliable source. This will reduce your risk, but even more importantly, you must run anti-virus software and *keep it current*. Viruses appear and mutate at an alarming rate, and regular updates of your anti-virus software is essential to keeping yourself protected. Finally, and most importantly, make regular backups. With all the care in the world, you could still be hit by a virus. If you can't restore your files, you turn what could have been an annoyance into a disaster.

4. The services that create file servers on user machines can be very hard to trace.

   "… firewalling them is very difficult, short of using non-routed IP addresses and using proxy servers and NAT at the gateways to the Internet you can't block it. Probably the simplest is to monitor network traffic going/coming from workstations and then zero in on the top 10, 20, 100, or whatever and talk to the users. … Scanning your network regularly with

tools like nmap and strobe will alert you to open ports" (Seifried).

5. Tracing and/or blocking unsecured traffic is somewhat simpler, but still is not absolute.

   In order to block, or at least slow down, usage of Instant Messaging services, there are certain ports that can be closed off. ICQ gets its user list from its server by using TCP port 4000. The actual chat addresses and ports will be different, so it's pretty much impossible to completely block, but closing off access to the server will slow things down (Seifried). "AIM uses port 5190 to talk to the server, and from there to other people making it hard to figure out who you are talking to, but very easy to block it (unlike ICQ)" (Seifried).

   Aside from trying to block IM services, companies need to make sure that their security policies address them. There need to be some rules in place governing what types of software users can put on their machines, and what kind of discipline they can expect to receive if those rules are broken.

6. On your own machine, you can disable message logging.

   This is probably one of the first things you should check before conversing with anyone. "ICQ automatically logs conversations once someone signs on for the first time. However, ICQ users can choose to disable the logging on an individual or an overall basis. As with Yahoo, people are not alerted when someone logs their conversation" (Hu and Konrad).

Is Instant Messaging worth the risk?

Instant Messaging, like e-mail before it, is poised to dramatically change the way that people communicate (and, indeed, this change has already begun). For business use, I'm not sure that its benefits outweigh its risks. The more users there are, the more chances for security holes. It is very difficult to control access and block ports, when they are constantly changing. "The potential for abuse, wasted time and bandwidth, as well as potential legal issues probably outweigh any benefit that might be received from them. They are not oriented to team work in the sense of groupware such as Lotus Notes or Novell Groupwise" (Seifried).

For home use, the risks are lessened. Home machines don't usually have the disk space or the bandwidth to make them the most attractive targets for being used as servers. Also, with a limited number of users, it's much easier to control the things that are being accessed. The only real issue here is that the home user must be savvy enough to be able to make the right configuration choices and maintain the machine through anti-virus updates, patches and backups, which is something that the average home user is not always consistent about doing.

All in all, Instant Messaging programs are very risky and should be avoided if possible. There are risks of exploitation through data, bandwidth, and disk space as well as questions about privacy, legal issues and liabilities.

References

AOL Instant Messenger Frequently Asked Questions - Warnings. URL: http://www.aol.com/aim/faq/warnings.html - warnme

Hu, Jim; Konrad, Rachel (June 20, 2001). *IM chats don't fade from PCs' memories.* URL: http://news.cnet.com/news/0-1005-200-6333967.html

LaGesse, David (March 5, 2001). *Instant Message phenom is, like, way beyond E-mail.* URL: http://www.usnews.com/usnews/issue/010305/nycu/im.htm

Perera, Rick (May 3, 2001). *Instant Messaging Wars Could be Short, Nasty.* URL: http://www.pcworld.com/resource/article/0,aid,49124,00.asp

Seifried, Kurt (April 19, 2000). *Instant Messenger, or Instant Security Risk?* URL:

Spring, Tom (May 24, 2001). *Who's Reading Your Instant Messages?* URL: http://www.pcworld.com/resource/article/0,aid,50984,00.asp

Tyson, Jeff (unknown). *How Instant Message Works.* URL: http://www.howstuffworks.com/instant-messaging.htm

Vance, Ashlee (February 7, 2001). *Instant Messaging Interoperability Nears*. URL: http://www.pcworld.com/resource/article/0,aid,40823,00.asp

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event