

Instant Messaging. How dangerous is it?

Written by Stuart A. Levine

I have been guilty long ago, of every security sin in the world of instant messaging. I've transferred files to strangers, accepted files from friends and strangers, exchanged password information, and likely a dozen other things I now know to be quite dangerous. Like many, I would communicate with my colleagues and friends via the 'instant messenger'.

At the time, I thought it was efficient and cool. I think many of us would lean towards the efficiency statement while using a messenger in the corporate environment, however, how many of us chat with friends while at work? The intent of this paper is designed to raise the level of awareness to the dangers of using the more popular free instant messengers in and out of the corporate environment.

Instant messengers often bypass corporate security measures, like firewalls, providing another opening for hackers to the Windows client. These are open doors, and while large corporations are beginning to spend billions of dollars on security, the possibility of this open door makes it a weak link in the security chain. As hackers become more sophisticated, hackers will increasingly enter networks through the client side -- the open front door to the system.

We should start by examining social engineering, and how it relates to the chat world. If I am on your buddy list, it is likely that you trust me, and we chat about business, personal information, just about anything. You trust 'me', don't you? Hey, we're chat buddies! Here's some food for thought... "What if that user is spoofed?" What if someone is sitting at the desk of my friend, but it's not them. Have you ever clicked on 'save password during login', or 'remember my password' in the sign on dialog box? These attacks may entice users into taking insecure actions, such as communicating sensitive information with outsiders or executing untrusted software.

This is dangerous behavior in my paranoid world, I trust no one these days. Maybe that makes me a better security engineer. Do I trust that instant message from 'the IT department' that says "I need your password information due to some restructuring/re-installation of software in our department"? In an environment that has no policy against the usage of instant messaging, it is easy to believe the message from a 'technical' department, when in truth; it may be coming from the outside world. How many of us use the same password for our chat programs as our email or login? Has anyone ever wondered if these conversations are saved?

Privacy Issues:

Beyond all the possible ways to exploit these messengers, there is a more basic issue. Privacy. Conversations are easily recorded. There is potential for enormous damage to a company if their internal conversations become public knowledge. For sensitive communications, it may be difficult to strongly authenticate the identity of remote parties using only the information provided in most chat clients.

For example, a company named [eFront](#) had their CEO's conversations made public, which contained information and comments made about business partners, employees and web affiliates. Needless to say, the news for eFront was not good afterwards. Partners have publicly distanced themselves, and legal action may be taken against eFront.

Instant messages introduce many of the same problems that e-mail does. Not only can instant messages harbor viruses, but also they are efficient conduits of information that can cause legal headaches for a corporation, including the divulgence of trade secrets or the exchange of libelous

or harassing statements.

Exploits

AOL Instant Messenger.

I have seen this program on machines everywhere. My friends have it on their personal computers. At my previous position as an Internet development manager, the entire company used it. Imagine one of the top 5 software houses in the world with thousands of computers and laptops all with AIM installed.

We start with a simple program called [Chat Recovery](#). A visual basic program that detects users that have the 'save password' feature selected. It reveals the password up to 16 characters. Imagine, working at that firm and acquiring a high level executive's (who is unaware of security) AIM userid and password. This program does not work remotely but how hard is it to walk around your office, being the great tech guy, and install a program on someone else's machine. Yes, a combination of things must happen to be successful here, but it's not that hard. My last two positions used 'push' software and at most any given time, you could install software remotely on other machines. The point is...this program does exist. Once I've acquired someone's username and password, I *become* that person. Social engineering takes over. Let your imagination run wild on this point.

I was shocked to find an entire manual called '[The hackers guide to AOL Instant Messenger](#)'. It comes with multiple exploits such as crashing another users machine, find the user's IP address via the transfer file facility as well as explicit information on password cracking.

Example: In the newest version of AIM (AOL Instant Messenger) there is a way to transfer files. When you are transferring the file, you can open a DOS prompt and type: netstat -a -n . The output gives you the users IP address.

Another nice attack using AIM would be to completely take over a remote machine. Not possible you say? One such overflow can be demonstrated by typing the following: (provided by [@Stake](#)):

```
aim:goim?=<insert 300+ string of AAAA here>+-restart
```

Another vulnerability can be demonstrated by typing the following: (provided by [@Stake](#)):

```
aim:buddyicon?screenname=abob&groupname=asdf&Src=http://localhost/AAA (x 3000 characters)
```

Another more basic, yet very dangerous, problem is file transfer. This one is quite simple, and is applicable to most transfer protocols. AOL Instant Messenger has the ability to embed images into an instant message. The user sends the graphic to the person they wish to show, and the graphic shows up on their screen. If the graphic is not a valid image then an icon will be displayed showing the file type. Due to improper HTML parsing it is possible to cause the AIM program to embed malicious JavaScript/VBScript inside a locally saved HTML that when later viewed would be executed with higher than normal privileges

The images are saved in a the following format:

```
<BINARY><STYLE><DATA ID="1" SIZE="66">Data that would be inside a GIF</DATA></BINARY>
```

If you were to send an HTML file which included malicious JavaScript/VBScript code with a image extension that started with </DATA></STLE></BINARY>, then the code would be executed if

logs of the conversation were saved and viewed with the default browser. One could also embed a web bug, Java applet, etc.

ICQ (I seek you)

In my current position at a security firm which specializes in vulnerability assessments, I talked to a potential client who wanted his ICQ servers tested among his other dmz machines. These ICQ servers were reachable from the internet. Without giving away too much, this was a financial institute. I later found out that they use ICQ for chatting globally. I was hungry to test for backdoors on this clients machine such as [Netsphere](#), which performs standard backdoor functions such as keystroke logging, capturing screenshots, and several functions that operate with ICQ.

There is a fantastic (and shocking) [ICQ Security Tutorial](#) floating on the net that describes myriad problems with ICQ. From cracks, flooding, spoofing, ICQ homepage flaws, file transfer problems, stealing passwords etc. The list goes on and on.

Example:

When you receive a file transfer request from someone, you see the filename in a small text box inside the request dialog box. But, what happens if the filename is too long to be displayed?

Take an executable file called "file.exe" (without the quotes), and change its name into "file.jpg .exe". Now, send this file to someone on ICQ. Since the filename is too long to display, the little text box will only show as much as it can, thus hiding the ".exe" part from the victim's eyes. This is a great way to send Trojans and backdoors to unsuspecting individuals. Very much the same as the AIM problem described above.

In addition to the above, these programs send plain text authentication. Not only that but they send it once per session.

ICQ also uses easily guessable sequence numbers. Starting from 0 for each user session, they use UDP and to make life even easier their query service will tell you exactly what IP address to spoof as source when faking them. So you can find someone is on, find their IP and spoof sequences 0-100 with a fair bet that somewhere before the 100th fake message you'll get several hits and spoof messages.

Yahoo! Instant Messenger

Among my searching, The Yahoo! Messenger revealed few current day exploits. I suspect as market share changes this too will change. It is however, not without problems.

The Yahoo! Messenger client transmits your personal information in clear text across the network. The transfer of any information in clear text presents major privacy problems. Information, including passwords, may be passed across untrusted networks (both domestic and international) in clear text, making them subject to interception.

I was able to find a denial of service attack existing in build 733 of Yahoo! Messenger. The vulnerability exists when Messenger leaves port 5010 open. When a connection is made on port 5010, Messenger crashes. The connection stays open until the user closes the program. Malicious users cannot only crash Yahoo! Messenger users, but it also gives them the capability of scanning and detecting Messenger users across wide networks by simply scanning port 5010.

MSN Messenger

Although it was hard to find exploits or anything of substance on this messenger, it is not exempt from hackers. A recent virus has surfaced that spreads via the MSN messenger. W32/Hello, an Internet worm that affects Windows machines, arrives via MSN Messenger as a file called

Hello.exe. The user clicks on the file, which is actually a visual basic 5 application (surprise!) and creates a worm shortcut in the windows start-up folder. It then attempts to send a copy of itself along with the message "I have a file for u. its real funny", to people on the contact list of an infected user's machine. This is a low risk virus. The importance here is the warning that users should be careful of instant messaging applications. As these services become more prolific, virus authors and hackers will target it.

There was a problem in version 1.0 of the MSN messenger relating to weak encryption: the email username and password were stored in the registry key
KEY_CURRENT_USER\Identities\9C53B920-A2E8-11D1-A59D-008048B12C6E\Software\Microsoft\MessengerService\ , which could be decrypted by using the MessengerServiceEmailPasswordDumper 1.0.

Solutions and final thoughts

Unencrypted instant messages can be intercepted and read en route to their destinations, a point the major providers concede but downplay as a matter best left to individuals' discretion. If you must have a chat client on your machine or corporate server, could you protect yourself better?

Several companies now offer corporate messaging solutions. One such solution can be found at [Encrsoft](#) or [Jabber](#). Additional IM companies targeting the enterprise include: [Mercury Prime](#), [QuickSilver](#), [2Way](#), [Ikimbo](#), [Ezenia](#), [NetLert](#), [ACD Systems](#) and [Bantu](#). Competition is already fierce for the corporate IM market, which analysts expect to explode in the next three years. Corporate IM users are expected to rocket to 181 million in 2004 from a meager 6 million last year, according to an August 2000 report by [IDC](#).

Is there a place for instant messaging in the work place? Has the pain just begun? Many exploits and vulnerabilities are easily found on the Internet making this difficult to answer. Multiple versions of these messengers make it even harder to manage. The above are simple examples of what a security engineer or IT department is up against. You can't trust the users on your buddy lists, as many of the exploits spoof those users. Viruses, trojans and backdoors are easily disguised within file transfer. Software flaws, such as buffer overflows or insecure configurations, may be present in client software and may provide a means for remote users to initiate attacks that execute code on internal systems. 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.

Sources:

Excite News

<http://news.excite.com/news/zd/010405/10/ebay-yahoos-security>

Black Sun Research Facility

<http://blacksun.box.sk/>

Windows IT Security

<http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16349>

PacketStorm

<http://packetstorm.securify.com/9909-exploits/indexdl.shtml>

Dark Eclipse Software

<http://www.dark-e.com/des/software/aim/index.shtml>

CNET News

<http://news.cnet.com/news/0-1005-200-5148422.html>

<http://news.cnet.com/news/0-1005-200-5149126.html?tag=st.tv.toc.top.0-1005-200-5149126>

McAfee Virus Center

http://vil.nai.com/vil/virusSummary.asp?virus_k=99077

Bugtraq

<http://www.securityfocus.com/templates/advisory.html?id=1644>

Bugtraq

<http://www.securityfocus.com/templates/advisory.html?id=1925>