GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Version 1.4b

The Evolution of Instant Messaging
Susan K. Scheele

Summary

The world of Instant Messaging (IM) has evolved from its early origins as a vehicle for real-time interpersonal communication, in particular instantaneous 'chat', to today where it is on the verge of being the source of instant communication in enterprises and across almost every electronic device conceivable. Along with the promise of the technology, comes the reality of security vulnerabilities, social engineering concerns, the challenge of interoperability and growth pains in going from peer-to-peer to enterprise applications. This review details the major Instant Message players and some of their history as well as their architecture and vulnerabilities. Recommendations for safe usage in public and enterprise arenas are suggested. The exciting direction of Instant Messaging into the future is beginning to come into focus.

IM Overview

Today, the ability to 'chat' using the Internet is nearly taken for granted. Interestingly, my personal experiences began in 1997 when I became a subscriber to America Online (AOL) and was quickly fascinated with the native AOL Instant Messenger, and the newfound ability to connect with friends and family. Little did I know that the history of this technology was already almost ten years old. Jarkko Oikarinen from Finland, created Internet Relay Chat (IRC) in 1988. Bill Gates' famous vision, also reiterated and expanded by President Bill Clinton, to have a computer in every home and have them be connected to the Internet, is approaching reality. The shear numbers, combined with the ease of graphic user interface (GUI) operating systems, have enabled many novice computer users to get connected.

IRC, unlike other IM clients, utilizes public channels. During the Gulf War in 1991, users around the world interconnected on the same IRC channel to learn and discuss the happenings of the war, real time. Another example of international usage was during the coup against Boris Yeltsin in Russia, in 1993. IRC users again gathered on a common channel to learn of the unstable situation surrounding the coup.

In addition to IRC, more private IM communications are popular today. Four major players sometimes referred to as the "big four", are considered to dominate the IM world, including AOL Instant Messenger (AIM), ICQ, .NET Messenger (formally MSN Messenger) and Yahoo! Messenger. AOL, a leader in IM from the start, has three IM entities -- its own native Instant Messaging, AIM and also AOL's wholly owned ICQ software.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ICQ originated in 1996 when four Israeli men saw the potential of Internet communication and launched a company called Mirabilis. Mirabilis named its technology ICQ (to suggest 'I seek you') and target people seeking people connections. Popularity of ICQ grew rapidly, and by June of 1997, Mirabilis Internet Communications Network was handling 100,000 concurrent users. In 1998, AOL acquired ICQ and its user base. Usage statistics continue to explode. A recent count suggests that there are 100 million IM users worldwide today, with the big four making up the majority of the market share. Projected estimates predict usage will increase to 180 million users by 2004. To date, the majority of IM has been in the public domain and has primarily been utilized by individuals using computers at home. However, the potential growth explosion will most certainly include the business sector and IM is quickly becoming possible from cellular phones, pagers, Personal Digital Assistant (PDA) and other wireless devices.

Public IM

With all good things comes a little bad. IM is no different. Since the events of September 11, 2001, the desire to stay connected with family and friends has probably never been higher. Internet access is easy, capabilities have expanded to include not only 'chat' but file transfer (graphics, sound, voice, video, online gaming, workgroup collaboration and files), access speeds are faster than ever and public IM is booming. Although systems are better understood and more completely documented, the down side is that the potential for intrusion is of considerable concern.

Millions of unsuspecting IM users are vulnerable to malicious hackers, known as crackers that target IM to:

- Spread viruses, worms and Trojan horses
- Break into and compromise computers
- Disrupt, destroy or ease drop and record confidential conversations
- Wait for malicious software (malware) to activate on a new host to gain authentication information and subsequently take over the compromised computer

These are considered to be social engineering attacks. Allen D. Householder, an Internet security analyst at CERT, describes a social engineering attack as one where 'the user's decision to download and run the software is the deciding factor in whether or not the attack is successful.' The CERT Coordination Center has published an incident detailing this type of attack (IN-2002-03 "Social Engineering Attacks via IRC and Instant Messaging"). The incident note details that crackers are using automated tools to post messages to IRC or IM service users. The messages trick the user into thinking they are legitimate sources for beneficial software for things such as anti-virus protection, improved music

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

downloads, get-rich-quick schemes and pornography. Once the software has been downloaded and executed, the user's computer can be utilized by the cracker as an agent in a distributed denial-of-service (DDoS) network attack, which results in a buffer overflow to the targeted computer. In addition, crackers are using similar techniques to propagate viruses, Trojan horses and backdoor programs.

Understanding the nature of IM networks helps to see the vulnerability to malicious attack. One model of a network is the peer-to-peer (P2P) model. In this case, two computers running similar IM clients connect directly through their network addresses. The danger in P2P connections arises from the identification details that are directly exchanged by the participating computers.

More common network models are the peer-to-server type (sometimes called client-server), which utilize synchronized channels on servers using common protocol. Messages are received and distributed simultaneously by all of the synchronized participating servers. This model represents the popular AOL (AIM), Microsoft (.NET Messenger), and Yahoo!'s IM networks. The peer-to-server IM networks allow peer-to-peer connections for private chats and file exchanges.

Vulnerabilities of each of the four major IM networks vary slightly. For example, given the P2P nature of AIM and .NET Messenger, intruders are most likely to attempt to disrupt private chat channels or send malicious files. Attacks of ICQ are similar, although less frequent.

IRC, on the other hand utilizes public channels and is divided into subnets, each with multiple synchronized servers and multiple chat channels. As messages pass from clients across numerous servers to recipients, most are wide-open to eavesdropping (unencrypted). The nature of the complex server network alone opens IRC to more frequent attacks and allows it to be used as a dangerous vehicle for spreading malicious messages or files. The danger of file transfer stems from the fact that files transferred via IM are currently not scanned at the firewall to protect against virus invasion since IM protocols are proprietary. However, good news is on the horizon. Symantec Corp. has announced that Norton Antivirus 2003 will scan files transferred over IM for malicious viruses, Trojans and worms. The anti-virus software is designed to work with AOL, .NET Messenger and Yahoo!. This type of anti-virus software will be pushed into the enterprise arena within the coming year.

Another critical vulnerability of IM comes with the capability of scripting. While potentially allowing creative and constructive coding resources, the potential for malicious activity is also a reality.

Perhaps the most damaging exploitation in IM is the ability for an attacker to gain access to any client through an exposed vulnerability. Once in, an attacker can

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

wreak havoc by impersonating the unknowing user, or by accessing confidential files or password files. The impersonation may take the form of false conversations, or worse, accessing information using the no longer secured passwords.

Although new vulnerabilities seem to be constantly exposed with all of the IM networks, there are actions that can be taken to protect users and minimize the risk of attack. For example:

- Utilize a personal firewall
- Encrypt file transfers whenever possible
- Update client software to the most current revision
- Load any client recommended software patches
- Load and run anti-virus software
- Update anti-virus software regularly
- Run content filtering software
- Be skeptical of messages or files from strangers
- USE COMMON SENSE

IM communication occurs through defined port numbers. However, for the public sector, improving the security of IM through port blockage is difficult, if not impossible. Such security measures for enterprises are critical.

Enterprise Instant Messaging

The decision to utilize the potential benefits of IM in enterprise arenas is the subject of great debate. Some organizations believe the positives outweigh the negatives. One such advocate is a first of its kind consortium of government agencies in the Washington, DC area who have joined with IBM to create a wireless emergency network that will allow 40 police, fire and safety agencies to communicate in real time via IM and access one another's databases. Congress has authorized a $20 million budget for the project.

Already, corporate IM users number some 65 million and are expected to grow to 255 million by 2005. Much of the responsibility for enterprise security falls on network administrators and corporate executives. However, even the United States Government recognizes the importance. President Bush directed the development of a National Strategy to Secure Cyberspace. Included in the document is the following statement on IM:

> Instant Messaging (IM) programs present another point of vulnerability to large enterprise systems. For example, IM programs can by-pass firewalls and antiviral scanners allowing malicious code, unauthorized intruders, and valuable data to covertly move in and out of enterprise

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

systems. Enterprises should adjust their computer security policies to appropriately account for the risk presented by IM programs.[1]

Of course, the specifics of protection is much more complex than the concept. One of the first decisions is whether IM clients will be supported at all in an enterprise. If so, then the decision to allow passage through enterprise firewalls is another fork in the road. Some enterprises decide to keep all IM internal. Even this does not prevent the ability to quickly spread worms or viruses once they enter a network. Others will endorse only one IM client in the enterprise. Even within the enterprise, a troubling statistic is that approximately 70% of all cyber attacks on enterprise systems are believed to be perpetrated by 'trusted' insiders. Insiders are trusted people with legitimate access rights to enterprise information systems and networks.

The potential benefit of enterprise IM is great, from customer service to instant purchasing and marketing. Unfortunately, the potential damage is tremendous as well. Nonetheless, enterprises are wading through the possible mine field. An INT Media Research survey says that of the 47% of enterprises allowing or supplying IM access in the workplace, 13% take no security precautions at all. Forty-one percent said their IM applications are installed behind a commercial firewall, while 41% said a network firewall prevents access to unauthorized free IM services. Just 5% say they outsource IM security functions to a third-party firm.

Besides security, another deterrent to fully open enterprise IM communication is the lack of interoperability between IM clients. Businesses who support IM are encouraging IM providers to figure out how to work together. In September 2002, six top financial institutions met secretly with AOL Time Warner, Microsoft, IBM and other leading corporate instant messaging providers and urged them to build communication networks that interoperate. The meeting was one of the first convened by the Instant Messaging Standards Board (IMSB). The goal of the board is to encourage, not write, standardization amongst IM clients. The Federal Communications Commission (FCC) attempted to apply pressure to AOL by ordering it to open its IM systems to rivals. AOL has since responded by shifting its strategy toward allowing certain rivals to access its own proprietary system. While at a clear crossroads between public and enterprise IM systems, the IM suppliers are seeing the opportunity to cash in financially. AOL has announced plans to introduce a fee-for service for corporations. Surely the others are thinking the same.

Another organization, IETF (Internet Engineering Task Force), is sponsoring development of a protocol that would be a key to interoperability. AOL Time Warner and IBM's Lotus Software criticized the protocol, calling in insecure. The Lotus-AOL test used a protocol called SIP (Simple Implementation Protocol) for Instant Messaging and Presence Leveraging Extensions (SIMPLE). Although it

[1] A National Strategy to Secure Cyberspace, p. 21.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

appears to be a step in the right direction, there is clearly a lot of work ahead. The bottom line seems to be that there is more interest from outside entities to achieve interoperability than amongst the key players.

One solution is Trillian, a cross-platform IM service that allows interoperability as long as the software is being used on both ends of the IM communication. Another perk is that when both Trillium users are on the AIM network, their one-on-one electronic chat is encrypted.

So, the focus for now is back at the enterprise. Once an enterprise makes a decision to control, rather than prohibit IM, then two initiatives need to be taken. One is establishing rules, constraints and standards for enterprise workers to operate within. The second is maximizing security through software such as firewalls, anti-virus and port blocking. In other words, the IT management must initiate IM in an enterprise by establishing a well thought out use policy and educating employees on the policy and proper usage. Well-respected TechRepublic has published an IM Policy Template. Highlighted in the template are the responsibilities of the IT management, which includes installation of IM software and user training. It is recommended that only one IM application be supported within a given enterprise and that additional features such as downloadable ringers, tones, playing MP3 music files and other nonessential extras are prohibited. Department managers have responsibilities as well, including educating employees on appropriate usage and monitoring IM activity. Individual users are directed to follow the IM etiquette guidelines. The etiquette guidelines make it clear that IM communications should never include sensitive content unless encryption is used, files should not be transferred using IM (only through email where anti-virus software can scan the attachments), and authorized usage is for business activities only. Following advisement and training, enterprise employees are required to sign a form acknowledging their awareness of the policy. Security is essential for enterprises and the IM security policy should be part of a comprehensive and ongoing security-awareness training program. With the interconnection of networks, the strength of IM security in enterprises is only as strong as the weakest employee link.

Minimally, IM security practices should include the same elements as those listed in the public IM section above. In addition, considerations should be made to properly configure corporate firewalls to block unapproved IM traffic, use private corporate IM servers to isolate IM activity from outside of the enterprise, enforce IM settings such as refusing file transfers by default, and use of Vulnerability Management solutions.

However, vulnerability of enterprise security and the ability of IM solutions to bypass firewalls, intrusion detection systems (IDS) and anti-virus scanners should still be considered carefully. Directing transactions through an external proxy server on any non-restricted port can elude firewalls. The vulnerability comes from the fact that most IM software allows the user to select the ports to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

use and monitoring unauthorized ports is difficult, if not impossible. To protect against this, a network-based IDS can be set up to monitor and reset unauthorized IM traffic. Other alternative countermeasures include monitoring traffic with a 'field expedient' Linux system with tcpdump, dsniff or ethereal, or a comprehensive network recording system such as Niksun's NetDetector, SilentRunner or Sandstorm's NetIntercept. Of course, limiting IM to internal usage is a reasonable approach, given the current vulnerabilities in IM and the available solutions.

The next security hold facing enterprises with IM usage is the bypass of anti-virus scanners and the possible damage by malicious file transfer. This is possible since the current status of anti-virus scanning software is not capable of scanning IM attachments which go directly to the desktop. A large market opportunity for anti-virus software company beckons, and soon solutions will be available. Of course, the effectiveness of anti-virus software is dependent on maintaining current versions and updated definitions.

Perhaps the scariest of vulnerabilities through IM security holes is the thought of hackers gaining access to networks by using an invaded workstation as a jumping off point, as has been documented in recent AIM buffer overflow flaws. With the network of interconnected computers within enterprises, and the importance of confidential information, the potential damage could be catastrophic.

Finally, the effectiveness of encryption in IM software is a concern. Most IM vendors have some level of authentication/password encryption but many have little session protection. It is best for enterprise users to edge toward safety and skepticism rather than a false sense of security when it comes to working with IM.

The architecture of IM solutions and their inherent security risks are similar amongst the major players as well as most of the minor and developing players. Critical to security are the proprietary protocols and encryption algorithms that are employed during transmission of authentication information including screen names and passwords. Another important architectural feature is the interaction between clients and servers. IM providers utilize proxy servers to secure traffic between connected users. In addition enterprises can make use of proxy servers, which allow traffic to be funneled through servers and implies a check-point where controls, including encryption, monitoring and port blocking, can be imposed.

Amongst the four major players, AOL IM uses TCP port 5190 for instant messaging, voice/video chat, file transfers and file sharing. However, the user can pick any authorized port so blocking only port 5190 is not completely effective. Sending and receiving images in AOL IM can be inhibited by blocking

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

inbound and outbound TCP port 4443. All IM services can be blocked in AOL by blocking access to login.oscar.aol.com on all ports.

Similarly, Microsoft .NET Messenger, file transfers and file sharing can be blocked at TCP port 6891. IM, voice and video chats are blocked at UDP ports 13324 and 13325. Application sharing is blocked at TCP port 1503 and all IM services can be blocked by inhibiting access to hosts msgr.hotmail.com sub domain on TCP port 1863.

IM voice and video chat can be blocked in Yahoo! Messenger by blocking in and outbound file transfers on TCP port 5010 and all IM services are blocked by inhibiting access to hosts within the *.msg*.yahoo.com sub domain.

Inbound and outbound IM on AOL ICQ can be blocked at ports TCP 5190 and UDP port 4000 and TCP port 4001 (for earlier versions) while file transfers are blocked on TCP port 3574 and file sharing is blocked on TCP port 7320. All IM services are blocked in AOL ICQ by blocking TCP ports 5190, UDP port 4000 and TCP port 4001 (earlier versions) to .login.icq.com.

The Future of IM

The future of IM will, no doubt, be exciting. However, this discussion of the current status of IM in both the public and the emerging enterprise sectors, already gives a glimpse of what is to come. In roads are being made toward ubiquitous IM applications. It simply isn't too difficult to imagine having IM capability from any of a number of mobile devices (cellular phones, PDA's, Pocket PCs), home computers, and certainly from the workplace, no matter what your occupation.

Applications will most likely become more directed, like the models being initiated by financial groups or public service groups today. IM capability will evolve in embedded applications and process specific services within business systems. Some of the small general-purpose IM vendors will develop more toward specialty applications like supply chain automation or archiving and security. Sectors will organize, like the cooperation of the top three cellular phone manufacturers, to enable greater IM interoperability.

Perhaps it is not where we are going, but what will it look like when we get there that is the more interesting of the questions. The introduction to IM that the world has, and is experiencing reveals concerns about security and interoperability. In the future more sophisticated products for malicious file detection, encryption and monitoring will become available. Most likely, hackers and crackers will keep up too, and will find innovative new ways to disrupt systems.

More broad-based usage of IM in enterprises raises the question of purging versus archiving. In some instances, archiving may be necessary for knowledge

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

management, whereas in other cases purging may be critical to avoid court ordered discovery processes. IM product capability, if not actual products, will be developed to manage IM activity records.

One of the biggest challenges for the future of IM remains interoperability. Software companies have traditionally held tight when it comes to sharing their proprietary architectures and protocols. Greater cooperation will be needed to break down the silos created by product specific IM.

As enterprises continue to embrace IM, today's popular public products will no longer be used in workplace environments, mostly because of their security risks. Rather those same players will develop products intended specifically for use in enterprises. Yahoo Inc. has recently introduced Yahoo Messenger Enterprise Edition to address the security, integration and administrative control needs of enterprises.

Finally, enterprises will become more comfortable with the idea of IM. Products, capabilities, applications and security will be more sophisticated. Even given the barriers to ubiquitous IM usage, consumer pull will most likely necessitate rapid progress. The cat is out of the bag. Before you know it, the vision of IM everywhere will be a reality.

References

Woods, Bob. "Yahoo Extends IM to the Enterprise". Internet News. October 7, 2002.
URL: http://www.internetnews.com/ent-news/article.php/1477661

"Securing Instant Messaging". Symantec, Spring 2002 Issue 14.
URL: http://www.symantec.com/symadvantage/014/instant.html

Dalton, Curtis E. and Kannengeisser, William. "Instant Headache". Information Security. August 2002.
URL: http://www.infosecuritymag.com/2002/aug/cover.shtml

"Personal E-Mail, Instant Messaging Biggest Security Threats". Business Journal Online. June 10, 2002.
URL: http://www.business-journal.com/LateJune02/netthreat.html

Kanellos, Michael. "IBM building emergency IM network". ZDNet News. August 22, 2002.
URL: http://zdnet.com.com/2100-1105-954809.html

Grimes, Roger A. "Protect Your Instant Messaging". Security Administrator. August 2002.
URL: http://secadministrator.com/Articles/print.cfm?ArticleID=25669

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Gaudin, Sharon. "Norton Antivirus Tackles Instant Messaging". Instant Messaging Planet. August 14, 2002.
URL: http://www.instantmessagingplanet.com/security/article/0,,10818_1446911,00.html

Woods, Bob. "Study: Instant Messaging Use Is A Big Security Threat". Small Business Computing. June 24, 2002.
URL: http://smallbusinesscomputing.com/webmaster/print.php/1369981

Sullivan, Brian. "Intruders Target Instant Messaging". Computerworld. March 20, 2002.
URL: http://pcworld.com/news/article/0,aid,90164,00.asp

Callaghan, Dennis. "IM Interoperability Hits Entanglements". EWeek. February 4, 2002.
URL: http://www.eweek.com/print_article/0,3668,a=22356,00.asp

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

Olsen, Stafanie. "Business takes lead for IM harmony". ZDNet News. September 13, 2002.
URL: http://zdnet.com.com/2102-1105-957787.html

Hu, Jim. "Is IM ready to do business?". ZDNet News. June 28, 2002.
URL: http://zdnet.com.com/2100-1106-940271.html

Thorsberg, Frank. "Worms Crawl Toward Instant Messaging". PCWorld.com May 28, 2002.
URL: http://www.pcworld.com/resource/printable/article/0,aid,101084,00.asp

Grimes, Roger A. "IM Security Primer". Security Administrator. May 2002.
URL: http://secadministrator.com/Articles/print.cfm?ArticleID=24665

"Instant Messaging Policy". TechRepublic. May 23, 2002
URL: http://www.techrepublic.com/download_item.jhtml?id=r00520020524gcn01.htm

Leyden, John. "Instant message, cracker tricks". The Register. March 20, 2002.
URL: http://www.theregus.com/content/archive/24388.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cain, Matt. "META Report: The Future of Instant Messaging". Instant Messenging Planet. April 29, 2002.
URL:
http://www.instantmessagingplanet.com/enterprise/print/0,,10816_1023321,00.html

"What is IRC?". mIRC. August, 2002.
URL: http://www.mirc.com/irc.html

President's Critical Infrastructure Protection Board. "A National Strategy to Secure Cyberspace", Draft, page 21. September 18, 2002.
URL: http://www.whitehouse.gov/pcipb

Clinchard, Cal. "Say Hello to Instant Messaging". Smart Computing. Vol. 13, Issue 9 (September 2002): Pages 50-53.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.