Global Information Assurance Certification Paper

Instant Messenger, Instant Security Headache
Erika Trigg Gifford
GSEC Version 1.4 Option 1

ABSTRACT

Instant Messenger (IM) is a free and easily installed method to communicate real-time with others. This paper will cover vulnerabilities such as IM transmitting messages in the clear making them easy targets by eavesdropping. By promising everything from free software to free porn, hackers have become very adept at social engineering IM users to click on whatever links or software sent to them. Once the link is clicked, Trojans and viruses are downloaded and your network has now become easy game for the hacker. Some versions of IM utilize common ports so they are hard to shut down through the firewall. Conversations on IM are not recorded, therefore making investigation of security breaches impossible.

This paper will also cover immediate risk mitigation as well as software solutions. Various companies have come out with corporate versions of IM that are more secure than the freeware version. Add-on packages are available to help secure the free IMs that may already be installed in corporate networks. These add-on packages add encryption and logging features and are targeted to companies that need to meet legal standards such as The Securities and Exchange Commission (SEC) or the Health Insurance Portability and Accountability Act (HIPAA). Firewall vendors are also getting into the act by creating plugins for existing firewalls to allow the IM protocol: session-initiated protocol (SIP) or creating new firewalls that incorporate SIP controls.

WHATS THE RAGE ABOUT?

It is 8PM and you decide to go online for a little bit of surfing. You bring up IM and within seconds you get notification that five of your friends are online including your sister who lives across the country. You bring up a chat interface to talk to her and within minutes you are talking to her live: a few seconds later you receive a file from her containing the latest family pictures. Another five minutes and your parents are online, so now you are talking and sharing pictures with them and your sister simultaneously. All this is done in real-time and best of all it is free.

IM is the fastest growing communications medium of all time. Giga Information Group reports that there are at least 20 million corporate users of IM and that number is growing at 200% a year. There is a good chance that if you are reading this, someone in your company is using IM.[1]

[1] IM Logic, "Instant Messaging Management", 2002 URL: http://www.imlogic.com/Brochure.pdf, August 13, 2002

IM is free and "The Big Three" AOL, Microsoft, YAHOO host the most commonly used packages. The software is readily available, easy to download and install. The IM sends and receives in real-time and has been described as somewhere between email and a phone call.

Most corporate use seems to be real-time critical exchange of information. IM allows the transfer of files and is much quicker than using a file transfer protocol (FTP) server. Users can keep the window opened on their workstation and continue to work while having a conversation with others on IM.

IM is often commonly used to share files such as MP3, movies, and other software that may be copyrighted. Transmitting this software across company networks can render the company liable for piracy. The Business Software Alliance (BSA) is a group of companies and individuals that are trying to prevent the illegal distribution of copyrighted material.

The BSA states their purpose as:

> The BSA is the voice of the world's software and Internet industry before governments and with consumers in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates computer users on software copyrights and cyber security; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy.[2]

The BSA has a tool to download called GASP that helps companies find licensed and unlicensed software and files on the company's network. This can be an important tool in discovering IM use on the network. Illegal software can also contain viruses, so this tool is good for overall security risk mitigation targeting software.

Along with the ease of use, real-time conversations, and expedition of the exchange of information for work requirements, IM has a down side. The down side is that it is impossible to trace a user through this service. If highly sensitive information has been publicly released or slander has been rendered against a company, there is no way the company can pinpoint the employee, since screen names can be anything. There is no recording of IM communications through the servers; therefore there is no way to get copies for investigations.

INSTANT MESSENGER ARCHITECTURE

IM is a client-server based architecture. The client is loaded onto a PC, laptop, workstation, etc and is what the user uses to communicate with. The controlling server is maintained by the provider: Yahoo, AOL, etc. The server is responsible

[2] Business Software Alliance, http://www.bsa.org, August 13, 2002

for authenticating users, verifying their online status, and delivering messages to the intended destination.

RECENT HACKS

Hackers have been very persistent in their pursuit of "owning" IM. The following is a list of hacks targeted to IM users:

- W32.Aplore worm targets AIM. The worm sends an email with an attachment named Psecure20X-cgi-install.version6.01.bin.hx.com to all addresses in the victim's Microsoft Outlook address book. When the infected system is connected to IRC or AIM, the worm sends a website link to the victim's "buddy list" which references the .html file on the infected computer. When activated, this file displays a Web page and the user is tricked into running a copy of the worm on their own system and the cycle continues.[3]
- W32.Goner worm targets ICQ. The worm also spreads by Microsoft Outlook email after the victim clicks on the executable. When the machine is connected to ICQ goner sends itself out on this service. This worm targets firewall and antivirus software on the resident machine and disables them. Goner attaches itself to the victim's Registry so that it activates each time the system reboots.[4]
- CoolNow worm (also known as JS.CoolNow.A, JS.Menger.A, JS.Exploit-Messenger.A) targets .NET. This worm propagated from a Web page that has since been shut down, but is still worth of note since it was spread through social engineering. The worm not only sent itself out through .NET, but also targeted a hole in Internet Explorer.[5]
- W32.Choke targets .NET users. Users are tricked into downloading this worm through social engineering, the worm further tries to propagate itself through .NET users. Although this worm is not harmful, it can take up bandwidth and be insulting to users.[6]
- AIM has also been the target of two separate buffer overflow attacks, one in January 2002 and the other in April 2002. The victim's system is penetrated anonymously and there is no opportunity by the user to refuse

[3] Symantec Security, "w32.aplore@mm", June 27, 2002 URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.aplore@mm.html, August 13, 2002

[4] Vamosi, Robert, "Goner is a Script Kiddie-inspired Worm that Disables Firewalls, Antivirus", ZDNet Reviews, December 3, 2001 URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2825281,00.html, August 1, 2002

[5] Vamosi, Robert, "CoolNow MSN Messenger Worm exploits Internet Explorer Flaw", ZDNet Reviews, February 14, 2002, URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2847885,00.html, August 5 2002

[6] Vamosi, Robert, "Choke Worm Tries to Shoot the President Via MSN Messenger", ZDNet Reviews, June 7, 2001, URL: http://www.zdnet.com/products/stories/reviews/0,4161,2769395,00.html, August 5, 2002

the request. Buffer overflows render the attacked system useless as it takes up all of the CPU.[7]

COMMON SECURITY RISKS

All versions of IM have common security risks. Of course individual versions have their own inherent risks. Take for instance AIM to activate a user account the user signs in using a userID and password. The password is sent encrypted to the AOL server. Once the user is verified, they are able to communicate. AIM passwords are easy to decrypt with software such as dsniff. Identity theft is easy once the password is cracked. This can also lead to social engineering of people on the victim's "Buddy List". People can be tricked into giving out their own sensitive personal information including credit cards. It is easy to see how one vulnerability can lead to a major security breach.[8]

There are common vulnerabilities with all free IM packages and they are:

- Malicious files can be sent from one user to users on their "Buddy List"
- Users can be social engineered into activating Trojan horses or viruses through malicious users offering links or free software. Once the target user clicks on a link or software, a Trojan horse or virus is downloaded to their system.
- The file-sharing feature is configurable and if not configured correctly, it can enable others to view corporate shared directories containing highly sensitive information
- Utilizing features such as file transfer and voice chat can reveal the user's true IP address, possibly making that machine a hacker target
- All text is transmitted in the clear
- No encryption to encrypt text

RISK MITIGATION STEPS

AIM is configurable on different ports and can work around firewalls and proxies. Here are a few steps to help mitigate the AIM risks:

- Disable TCP incoming and outgoing on port 5190, this will prevent file sharing and file transfers
- Disable TCP incoming and outgoing on port 4443, this will disable AIM images and is not configurable through the AIM client
- In order for the user to utilize AIM, the AIM client verifies itself to the Open System for Communications in Real-time (OSCAR) server. To shut down AIM totally, block access to login.oscar.aol.com.

---

[7] W00W00, "AOL Instant Message Overflow", April 2002 URL: http://www.w00w00.org/advisories/aim2.html, August 5, 2002

[8] X-Force, "Risk Exposure Through Instant Messenger and Peer to Peer (P2P) Networks", April 2002, URL: http://documents.iss.net/whitepapers/X-Force_P2P.pdf, August 2, 2002

Microsoft ships the .NET client in WindowsXP and Microsoft Office as well as its free email service hotmail. This makes .NET the fastest growing IM software. Here are a few steps to help mitigate the .NET risks:

- Disable TCP incoming and outgoing on port 6891, this will prevent file transfers
- Disable UDP ports 13324 and 13325 to prevent audio/video teleconferencing
- Disable TCP port 1503 to prevent application sharing
- Disable TCP port 1863 and block access to msgr.hotmail.com to totally disable .NET

YAHOO! Messenger has the weakest security of all the IM software. Unlike other versions of IM, the userID and password is sent in the clear via http, which enables them to be recorded on http logs. Here are a few steps to help mitigate the YAHOO! Messenger risks:

- Disable TCP port 5050 to block instant messaging
- Deny access to the *.msg.*.yahoo.com sub domain to totally disable YAHOO! Messenger

Although AOL Time Warner owns ICQ now, it still maintains a separate database for this application. In January 24, 2002 there was a warning for buffer overflow, a number of denial of service attacks have targeted ICQ clients. Here are a few steps to help mitigate the ICQ risks:

- Disable TCP port 3574 to block standalone file transfers
- Disable TCP port 7320 to block file sharing images
- Deny access to login.icq.com to totally disable ICQ

Caution: Even with all these steps in place a user can still utilize an external proxy server to route their IM messages. An Intrusion Detection System (IDS) can be used to see if this is happening.[9]

DANCING AROUND DEFENSE-IN-DEPTH

Defense-in-depth is the practice of creating layers of security to prevent a breach of security; this is a combination of a strong security policy(s) as well as security hardware and software. Utilizing IM can divert defense-in-depth measures:

- Security Policy - A strong Security Policy needs to be outlined letting users know that downloading, installing, and using IM is forbidden on corporate networks and on corporate machines
- Firewall - Some versions of IM utilize common ports to make connections to the servers hard to stop
- Antivirus - Antivirus software is bypassed utilizing the file transfer option in IM

[9] Ibid

- Physical Security – Since files can be transferred to another IM user quickly and without record or having to physically carry the information out, company proprietary information can easily get into the wrong hands without leaving a trail.

Note: Even though major vendors say they do not record IM transactions, there is the capability for individuals to record and keep their conversations, thus there may be a slight chance that some information can be gained during an investigation.

A NEW TYPE OF INSTANT MESSAGING?

A new type of instant messaging has been taking hold: a Java application embedded in a web page. Users are required to have a Java virtual machine on their systems in order to use this program. For systems without this service, it is easily downloaded and installed.

The web IM works the same way in that it allows users to chat live. IM on websites allow users to talk about the contents of the website in real-time with other users. This application is tied to the web page. For companies thinking of utilizing this service, keep in mind that it holds the same security concerns as other IM applications and can greatly increase the administration workload.[10]

CORPORATE SOFTWARE PACKAGES

In March 2002, Osterman Research did a study and found that 84% of 164 businesses surveyed use IM. With these types of numbers is there any wonder that software companies have decided to create and market a corporate IM strategy.[11]

Software vendors have added the following features to their corporate IM solutions:[12]

- Archive traffic to comply with industry regulatory requirements such as SEC and HIPAA
- Generate audit reports and statistics to prove compliance
- Users are required to register their IM screen names and access can now be based off the screen names
- Block file transfers to mitigate virus transfer risk
- Disable access to public IM networks to ensure internal security

---

[10] Schlesinger, Lee, "Make IM Work for Your Company" June 6, 2002, URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2869212,00.html, August 6, 2002

[11] Derby, Meredith B., "Instant Messaging Insecurity Gains Momentum", May 01, 2002, URL: http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci820928,00.html, August 6, 2002

[12] IM Logic, "Instant Messaging Management", 2002, URL: http://www.imlogic.com/Brochure.pdf, August 6, 2002

- Generate usage report by employee or office
- Enable encryption for transmission of sensitive information
- Restrict user access to files they do not have the need to know to access
- Log file transfers for authorized persons
- Administrators can easily gather information needed in the research of an incident
- Restrict IM use to authorized employees

The following shows the market share IM.[13]

- AOL 48%
- .NET 35%
- YAHOO! 14%
- Other 10%

With only 10% of IM software belonging to corporate sales, software companies have also started creating plugins that can be used with free IM used in corporate settings. VeriSign has announced that it will issue security credentials to enable employees to send and receive encrypted messages over AIM. Makers of the free IM packages are also creating and marketing secure plugins for their software including encryption capabilities and virus scanners.[14]

Some companies such as IM-Age Software have gone a step further and created a whole suite of services for free IM. Among these services are:

- Authentication to eliminate spoofing
- Encryption (blowfish 448 big)
- Auditing and logging use of public IM networks
- Special alert feature for keyword tracking and reporting
- Alerts through pager, phone, e-mail or SMS
- Disclaimer forced on all IM transmissions
- Ability to run in "steal mode" so users will not know they are being monitored

IM-Age also offers free software called IM-Age Sniffer designed to let companies measure the amount of IM traffic on their networks and perform keyword searches on those transmissions.

IM-Age is aware that some companies want choices in where the server is hosted, whether it is at another site (IM-Age hosts its own IM server) or in-house. For a hosting fee corporations can use the IM-Age server, or in a different

[13] Ibid
[14] Gaudin, Sharon, "IM Users Being Duped into Security Laxes", August 09, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1444011,00.html, August 2, 2002

package, and price, corporations can choose to host their own IM servers utilizing IM-Age's software.[15]

Other companies with IM solutions are FaceTime Communications, Akonix Systems Inc, Communicator Hub, Cordant, Jabber Software Foundation, and Divine to name a few. Utilizing any search engine on the Internet will bring up a listing of companies offering IM solutions.

Even with this new view of securing IM, users should utilize a personal firewall and antivirus on their machines. All attachments should be scanned with the antivirus software before opening.

A NEW AGE OF FIREWALLS?

Session Initiation Protocol (SIP) is the signaling protocol that allows real-time communications used for voice over IP (VoIP), conferencing, and IM. At the beginning of each session ports are assigned at random and SIP negotiates the highest common denominator of both machines then establishes the connection. Most firewalls can block this protocol, but makers of firewall software understand that something more needs to be done.[16]

Firewall vendors are now creating firewall plugins that enable corporations to control SIP though their firewalls. One corporation, Ingate, has created a SIP capable firewall and a product called a SIParator, which plugs into an existing firewall to enable SIP.

Ingate's firewalls include a SIP proxy and registrar; support NAT and PAT as well as TLS for automatic encryption of IM messages, which help to alleviate identity spoofing and eavesdropping.[17]

Other major firewall vendors are now developing plugins for their currently fielded firewalls and creating SIP friendly versions for the future.

CONCLUSION

Instant messaging has the ability to destroy a company's security posture, but it can also be an incredibly powerful tool for getting business done. Corporations can now buy a full IM package with all the security bells and whistles along with the ability to host the IM server in-house, or purchase the security add on packages from "The Big Three" makers of the IM software.

---

[15] Woods, Bob, "IM-Age Rolls Out Security Platform", August 5, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1439431,00.html, August 6, 2002

[16] Rendon, Jim, "SIP-capable Firewalls Hits the Street", July 30, 2002, URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci841647,00.html, August 5, 2002

[17] Woods, Bob, "Ingate to Distribute IM-capable Firewalls Through ICS", July 23, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1430991,00.html, August 5, 2002

For Defense-In-Depth, corporations need to write an official Security Policy on the corporation's view of IM use in its networks. Firewalls can be tuned to prevent SIP, IM ports and the sub domains from traversing its boarder. Antivirus software, which should already be put on individual workstations, should be used to scan ANY attachments received by users. BSA software and IDSes can be used to track the presence of IM software and its use.
No matter what decision is made concerning IM, one thing is for certain it is here to stay.

FINAL THOUGHT

A Security Policy and end user security awareness training cannot be stressed enough. No matter what procedures are in place, the employee is still the biggest security vulnerability a company can have:

> "We did a security awareness study last year and found that a company's greatest vulnerability is the employee," says Logan. "If your employees aren't educated about security policies, there's a gap in the human firewall. You're instantly vulnerable."[18]

[18] Gaudin, Sharon, "IM Users Being Duped into Security Laxes", August 09, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1444011,00.html, August 12, 2002

REFERENCES

1. IM Logic, "Instant Messaging Management", 2002, URL: http://www.imlogic.com/Brochure.pdf, August 6, 2002
2. Business Software Alliance, http://www.bsa.org, August 13, 2002
3. Symantec Security, "w32.aplore@mm", June 27, 2002 URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.aplore@mm.html, August 13, 2002
4. Vamosi, Robert, "Goner is a Script Kiddie-inspired Worm that Disables Firewalls, Antivirus", ZDNet Reviews, December 3, 2001 URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2825281,00.html, August 1, 2002
5. Vamosi, Robert, "CoolNow MSN Messenger Worm exploits Internet Explorer Flaw", ZDNet Reviews, February 14, 2002, URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2847885,00.html, August 5 2002
6. Vamosi, Robert, "Choke Worm Tries to Shoot the President Via MSN Messenger", ZDNet Reviews, June 7, 2001, URL: http://www.zdnet.com/products/stories/reviews/0,4161,2769395,00.html, August 5, 2002
7. W00W00, "AOL Instant Message Overflow", April 2002 URL: http://www.w00w00.org/advisories/aim2.html, August 5, 2002
8. X-Force, “Risk Exposure Through Instant Messenger and Peer to Peer (P2P) Networks”, April 2002, URL: http://documents.iss.net/whitepapers/X-Force_P2P.pdf, August 2, 2002
9. Schlesinger, Lee, "Make IM Work for Your Company" June 6, 2002, URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2869212,00.html, August 6, 2002
10. Derby, Meredith B., "Instant Messaging Insecurity Gains Momentum", May 01, 2002, URL: http://searchwindowsmanageability.techtarget.com/originalContent/0,289142,sid33_gci820928,00.html, August 6, 2002
11. Gaudin, Sharon, "IM Users Being Duped into Security Laxes", August 09, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1444011,00.html, August 2, 2002
12. Woods, Bob, "IM-Age Rolls Out Security Platform", August 5, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1439431,00.html, August 6, 2002
13. Rendon, Jim, “SIP-capable Firewalls Hits the Street”, July 30, 2002, URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci841647,00.html, August 5, 2002
14. Woods, Bob, “Ingate to Distribute IM-capable Firewalls Through ICS”, July 23, 2002, URL: http://instantmessagingplanet.com/security/article/0,,10818_1430991,00.html, August 5, 2002

Last Updated: July 24th, 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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	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 Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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 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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor