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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Craig Sweigart
Practical Research Paper
Security Essentials Certification Practical Assignment version 1.4b

Instant Messaging Security

Introduction

Instant Messaging (IM) has become the software communication medium of choice to chat with friends, family member and co-workers. It is far cheaper to contact people via IM than by the traditional telephone long distance calls. In some cases the reliability in IM has exceeded the telephone and other communcation mediums. IM is a real-time communication tool and has recently become dominant over e-mail. Especially in business when time sensitive transaction need to occur seamlessly. From IM beginning as a buddy-to-buddy chatting service, it has developed into a prominent mode of communication for tens or millions of Internet users and is increasing in popularity in both professional and personnel applications. Although IM has received high praise for its communcation capability to scale up, it has been designed with very little security in mind. The popular use of the IM tool has created security challenges for individuals, corporations, and government agencies.

Numerous vulnerabilities have been found in IM application and provides an easy mechanism to release various threats to gain access to corporate sensitive data, eavesdrop on a chat conversation, cause a denial of service and in extreme cases steal the identity of a user. Furthermore, IM is an easy platform to attach and propagate worms and viruses, which potentially could go undetected for long periods of time. At this time firewalls have extreme difficulty blocking and scanning IM ports or related viruses before they enter into the internal network. To defend against the threats exploited by the IM public enterprise system, administrators as well as end-users must be aware of the security risks they pose to themselves as individuals and their peers.

The following section breaks down the foundation of the IM infrastructure design and functionality. Secondly, the paper will identify the key vulnerability areas that that exist in the IM client-server infrastructure. Finally, the paper will address solutions to minimize the amount of vulnerabilities that can be exploited by the IM Systems.

Understanding that there are multiple vendors that supply IM services, this paper will take a vendor neutral approach and cover the common vulnerabilities. Occasionally throughout the document you will see that this paper single out certain vendors. This is due to the fact that viruses and worms generally are designed to compromise a targeted IM vendor, because each uses their own proprietary protocols.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Technical Overview

Most all IM Systems are designed and deployed with the client-server architecture. Generally, the user chooses the vendor (i.e. AOL IM, Yahoo IM, MSN IM, etc.) and downloads the client version to their machine, whether it is a workstation, laptop or Personal Data Assistant (PDA). Once the client has been installed on the users machine it is in direct communication with the IM Server. A username (unique identifier) and password is generated in order for the system to authenticate the user. Once the user is authenticated, all session are established through the Server messaging infrastructure to locate users whom they want to communicate via the IM messaging network.

When a user establishes a authenticate session with the Server, it seems as if they are in directly communicating over the Internet with their chosen recipients machine, however this is not the case. When a user wants to send a text-message to another person's machine, the IM client encapsulates the text message into a packet and sends it first to the IM Server. The IM Server looks into the packet identifies the recipient, re-encapsulates it with a new packet and forwards it on to it's destination.

The concept of having direct communication with our recipient's machine is not too far fetched. Although most IM System forces the Server to be mediator for all message traffic, some allow peer-to-peer communication once you have located your client recipient and send the first message. Once the first message is received then message traffic can flow without the IM Servers intervention. Peer-to-peer communication offer much better security then having to go through the server when two parties are communicating within their Local Area Network (LAN). Where the security risk is evident is when someone within the LAN establishes direct connection over the Internet to another external network. Point-to-point communication over the Internet leaves them vulnerable to potential eavesdropping, because the message traffic is not encrypted. Figure 1. Instant Messaging Communication Process illustrates the client-server and peer-to-peer communication modes.

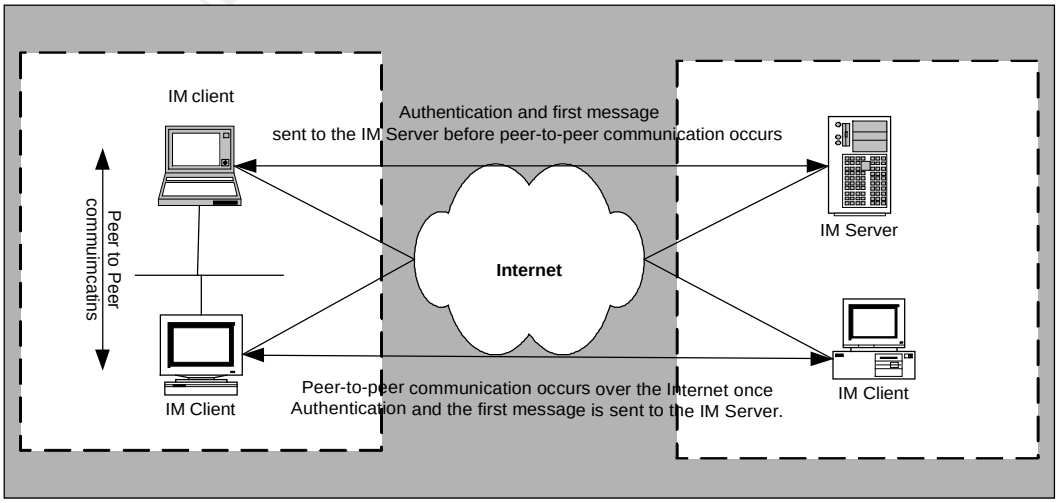

Figure 1. Instant Messaging Communication Process

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IM Privacy and Sensitive Information Issues
The concern of eavesdropper is due to IM sessions transmitting data in clear-text mode. Just about all of the popular IM Systems free to the public offer no encryption or secure mean to send a text message to the intended recipient. Therefore, corporation and government should beware that there is a potential to send sensitive information across the Internet where a hacker could potentially intercept the data. The Navy has actually stopped the use of IM on their ships, due to the fact that sailor may reveal their location or accidentally transmit classified information to their love ones. Any time information is transmitted via the ship it is possible that the enemy may intercept it. Many freeware network sniffers (i.e. NMAP, Ethereal etc.) are available to download and can easily strip off the text between two communicating parties.

Impersonation of users is another area of concern. If a hacker is able to circumvent an IM public account of an unaware user, friendships can be damaged, confidential information divulged or business clients lost. If a hacker were able to obtain an account of an IM user, theoretically everyone on his buddy list would trust him. Now the hacker has the advantage simply by the mere concept of trust. The hacker can now easily gain access to more information and computer systems by simply asking the user who trust the stolen account to execute malicious software, like password-stealing Trojans and backdoor worms. In other words compromised IM accounts can be detrimental the safety of innocent bystanders and corporate/government networks.

IM Malicious Software (MALWARE) Threat
Lately, there has been a growing threat of malicious software in the form of worms that have been spreading havoc to the IM client's machines. Internet based worms can propagate through the buddy list of the already compromised machine. Antivirus software has problems scanning viruses entering via the IM communication session and does not monitor at the network ingress point from the Internet. Antivirus has not been designed to detect IM related malicious software on the Server because of its inability to monitor traffic embedded with at HTTP packet. IM worms are on the rise and antivirus software cannot be trusted to eradicate the worm. Users and System Administrator must be aware and be able to quickly identify when an infection has occurred. More importantly administrator and users must gain and understanding of the social engineering techniques used to activate malicious software.

Worm Lookout

<u>W32.Choke Worm</u>
The W32.Choke Worm affects MSN Messenger and spreads itself through an executable file called ShootPresidnetBUSH.exe. When the worm is executed it become resident in memory and creates a files on the C:\ drive called

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Choke.exe, ShootPresidentBUSH.exe, About.txt and Dalist.txt. About.txt contain pre-made messages from the author of the worm. Dalist.txt contains the number of buddy list member that are infected. You can look into this file to determine how many people have been infected and be able to determine how many more are infected on you're network. It should be noted that you might have to remove the value that worm left in the registry. Worm information was taken from and more information can be obtained at
http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.choke.worm.html

W95.SoFunny.Worm@m

The W95.SoFunny.Worm@m is a password stealing Visual Basic script program Trojan horse that targets AOL IM users and replicates using the AOL IM software. This worm can release confidential information and steal login information. The good thing about this worm is it does not run under Window NT or Windows 2000. The worm copies itself to the \Windows\Msdos423.exe. In order for the trojan to run at startup it adds a value to the registry (msdos423 <Windows>\msdos423.exe to HKEY_Local_Machine\Software\Microsoft\Windowss\CurrentVersion\Run. What to look for is when the worm first is activated; it may display a message with a "Fatal Error #6834 – An unknown error has occurred." The Worm information was taken from and more information can be obtained at
http://securityresponse.symantec.com/avcenter/venc/data/pf/w95.sofunny.worm@m.html

W32.Goner.A@mm Worm

The W32.Goner.A@mm is a mass-mailing worm that is written in Visual Basic and spreads using the ICQ. The worm has been known to generate scripts, if IRC is installed, to enable the compromised computer to launch Denial of Service attacks (DOS). The worm adds the value C:\%SYSTEM%\gone.scr C:\%SYSTEM%\gone.scr to the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Once the registry key is added the worm will attempt to terminate processes common antivirus and firewall products. The Worm information was taken from and more detailed information can be obtained at
http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html

W32.Led Worm

The W32.Led is another mass-mailing worm that propagates itself through mIRC and Microsoft Messenger. Even though this worm targets e-mail messages the social engineering techniques revealed can prepare you not to fall into the trap. The worm is spread through using MSN Messenger and IRC through chat invitation that direct the user to a website that contains the worm. The Worm information was taken from and more information can be obtained at
http://securityresponse.symantec.com/avcenter/venc/data/w32.led@mm.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IM Trojan Horses
Hackers can do reconnaissance with the use of Trojan Horses that take advantage of the shortcoming of IM products. With the use of trojan horses, hackers can open up shares on the users computer, create backdoor access, reveal cached passwords and system information. Once the Hacker receive the information that he needs he can instruct the computer to make an unauthorized transaction or launch attack on other computer systems.

Trojan horses can use worms to do their dirty work for them. For instance a worm called W32/Rodok-A, which is similar to W32.Led mentioned above, used the MSN IM to entice a user to download an executable called BR2002.exe from a remote web site. Social Engineering is used to trick the user to execute the file. The worm launches a phony CD key-generating program. The program then connects back to the same web site, updates itself with a new version, and attempts to download a Trojan. The hacker can now launch remote distributed denial of service (DDOS) attacks. Hacker's generally infect the computer first with a virus or a worm and then inserts a trojan horse to allow access to the compromise computer. The trojan horse installed by the W32/Rodok-A worm is called BKDR_EVILBOT. As you can see it is important to keep up with the Internet worms based on what has just been described.

Trojan Horses can create backdoor and can be harder to detect through the use of IM clients than other traditional methods. Traditional trojan horses establishes a port on a computer, creating a session back to the remote host. This can be blocked by personnel firewall or even detected by using the NETSTAT command or loading Foundstone Fport Intrustion Detection software. However, the trojan horse operating within the IM client does not have to open a new port and utilizes the IM port session. Therefore, the trojan horse remains hidden from Intrusion Detection System or firewall, because the rules have been set to allow IM ports session through. One can predict that trojan horses will only become more popular in IM public systems, because they can hide themselves within the IM port communication session.

Denial of Service Attacks
There are several methods that hackers can use to launch IM client DOS attack. Whether or not a hacker would waste the time to launch a DOS attack to a computer running IM is questionable unless someone has personally made him/her angry. Anyone who takes hacking seriously would not go after the small helpless users instead would attack larger corporate systems for their personnel gratification and advantages. Never the less this does not hide the fact that IM System is vulnerable to DOS attacks. It is extremely easy to flood the IM Client's machine with large amounts of messages and the end result would be an unresponsive computer. Not only the IM client is vulnerable, but the IM Server is as well. A Hacker would get great satisfaction if he can successfully launch a successful DOS attack by flooding the IM Server with modified TCP/IP packets causing a buffer overflow and dropping thousand of IM Session. Furthermore, if

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the hacker were to compromise an IM Server with a combination of a worm and backdoor Trojan as mentioned above and obtain all IM accounts located on that server, one could only imagine the amount of destruction that could be released. Simultaneously, the hacker could run a script to flood all active accounts with massive amounts of messages and cause a distributed denial of service (DDOS) attack.

How do you begin to protect yourself?

Blocking the IM System

Well the first thing that comes to mind is to block all public instant messaging at your firewalls, that include all possible ports used by the IM application. Granted this would minimize a lot of IM public usage, however the savvy user would find other alternative to activate the IM client. Client's can use the common ports Hypertext transfer protocol (HTTP) port 80 and the File Transfer Protocol (FTP) port 21 to communicate via IM. What is even more disturbing is that the IM client has a secondary means to establish communication with the IM Server. The IM Client comes preconfigured with several IP addresses of the IM Servers, and if the IM client detects that it is being blocked it can it can map itself to the preconfigured IP address and communicate over the commonly allowed Internet ports that most firewalls allow, such as Simple Mail Transfer Protocol (SMTP), HTTP or Domain Name Server (DNS). System Administrator will have a hard time identifying IM sessions because it looks as if they are making legitimate connection over authorized ports.

Once way that a system administrator can prevent the IM client to sneak around the firewall is to include the IP address of the IM Servers in the Firewall configuration with a deny access. Finding all the IM Server IP addresses is not going to be easy and will require a fair amount of research, however it will be well worth the time and energy in order to secure the network. Once way to obtain the address is to utilize the NSLOOKUP and enter the DNS name to obtain the ip address.

Establish corporate instant messaging system

Consider deploying a secure corporate Instant Messaging System within your companies or agencies intranet. Not to single out a particular vendor, but IBM Lotus Software supports a product called Sametime. Sametime Messaging data is encrypted to protect meeting and chat content. By installing Lotus Sametime in your network's demilitarized zone (DMZ), users can access the Server from an external source without compromising internal network security. If IM is essential to your business, then deploying a IM Server on your network behind the firewall is one of the best security practices you can do for your organization.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Establish IM Security Policy

Corporation and government agencies should establish a policy so that all users understand that public Instant Messaging is not permitted on the internal network or on any own corporate computers. At the very least there should be a policy that mentions that any company proprietary information is not permitted to be transmitted with the use of any public IM systems. The policy should also indicate that close network monitoring of public IM traffic will be detected and possible termination of employment will occur if individual are not in compliance with the Corporate Security IM Policy.

Load Desktop Security Protection

Deployment of desktop antivirus software is a must, since corporate firewalls are unable to scan for malicious software transfer through an IM session. It is imperative that the desktop software be up-to-date with the latest virus pattern/engines to ensure that no malicious code has the chance to spread throughout the network. In conjunction with the antivirus software corporation can also deploy another layer of security with the use of desktop personal firewalls. Security Policy can be deployed on the personal firewall to deny communication of any unauthorized software of public IM system.

Pretty Good Privacy

If your organization cannot survive and is dependent on the scalability of the Public IM System, then you may consider looking into Pretty Good Privacy (PGP) cryptographic tool. A company called Command Code has a product that encrypts the content of the MSN Instant Messenger. The software product is called SpyShield and it uses PGP to encrypt your instant text messages to guarantee your privacy and the security of the information your organization is dependent upon. Command Code is also at this time focused on the MSN Messenger, but is open to adapt their product on other IM public platforms. The only problem with this solution is that the antivirus software is unable to scan encrypted executable files, which could be in the form of malicious code. However, you may want to accept the risk to secure your sensitive information.

How do you stay secure

In addition to protecting your organization of IM vulnerabilities it is essential to implement sound security practices. One of the important aspects of ensuring your corporate computer system are protected from vulnerabilities is by developing a patch management plan. Make sure that all your patches are up to date on you antivirus software and operating system. If public IM is allowed within your environment it is necessary to keep up with the new vulnerabilities that are discovered. New versions of the most popular IM client are released to fix the vulnerable software bugs. Often new versions of IM releases add on new security features to the product. Another recommendation is to change your password on a regular basis and make sure you use password complexity to include a combination of alphanumeric and special characters. In conjunction

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

with securing your password, make sure you enable the IM client program preference to hide your IP address so that hackers cannot launch a brute force attack to crack the password. Last but not least don't leave your computer unattended for a malicious person to send damaging information about you or your organization.

Conclusion

As we have already discussed Public IM is gaining popularity at an exponential pace and is making its presence in corporation and organization. Instant Messaging increases work productivity and facilitate training, meetings and other forms of collaboration. Lately there has been a strong movement to secure the public Instant Messaging infrastructure through the use of various security mechanisms because organizations have realized the value of the product.

The biggest threat the IM public client-server product is viruses. It is only a matter of time, where worms and Trojans and other form of viruses will improve to cause a widely distributed attack against computer systems running the public instant messaging application. However, the positive aspect is that the major IM applications use their own proprietary protocol system. This means that if successful attacks are targeted to a particular IM System, other IM systems will not be affected.

Privacy is another issue with the IM system. Can organization continue to take the risk of proprietary sensitive data get into the hands of unauthorized individuals? Organization must take corrective action and educate and bring awareness to their employees about the danger of the public instant messaging systems. Organization cannot rely on merely educating the end-users to solve the IM security issues. Additional security measure, policies and solution should be implemented in parallel to employee education to protect the interest of the business.

Reference:

Neal Hindocha; "Semantic Security Response; Threats to Instant Messaging" January 2003. URL http://securityresponse.symantec.com/avcenter/reference /threats.to.instant.messaging.pdf (March 6, 2003)

Symantec Enterprise Security, "Securing Instant Messaging" September 2002. URL http://securityresponse.symantec.com/avcenter/reference /secure.instant.messaging.pdf (March 6, 2003)

Neal Hindocha; "Instant Insecurity: Security Issues of Instant Messaging" January 2003. URL http://online.securityfocus.com/infocus/1657 (February 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Paul Roberts; “IDG News Service; MSN Messenger Worm Steals Game Keys W32/Rodok-A or Henpeck worm used via IM, then plant trojan to lift game access.” October 11, 2002. URL http://www.pcworld.com/news/article/0,aid,105897,00,asp (March 6, 2003)

Wendy McAuliffe; “ZDNet UK; Instant messaging boosts business” August 2001. URL http://news/zdnet.co.uk/story/0,,t269-s2092767,00.html (March 12, 2003)

Semantic; “W95.SoFunny.Worm@m” April 15, 2002. URL http://securityresponse.symantec.com/avcenter/venc/data/w95.sofunny.worm@m.html (March 12, 2003)

Semantic;”W32.LED@mm” April 15, 2002. URL http://securityresponse.symantec.com/avcenter/venc/data/W32.led@mm.html (March 12, 2003)

Semantic; “W32.Goner.A@mm” September 30, 2002. URL http://securityresponse.symantec.com/avcenter/venc/data/w32.Goner.A@mm.html (March 12, 2003)

Semantic; “W32.Choke.worm” June 6, 2001. URL http://securityresponse.symantec.com/avcenter/venc/data/w32.choke.html (March 12, 2003)

Internet Security Systems; “Risk Exposure Through Instant Messaging and Peer-to-Peer (P2P) Networks” April 2002. URL http://documents.iss.net/whitepapers/X-Force_P2P.pdf (March 15, 2003)

Command Code, “SpyShield”. URL http://www.commandcode.com/faq.html (March 20, 2003)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: January 23rd, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201701,	Jan 30, 2017 - Mar 08, 2017	vLive
Community SANS Albany SEC401	Albany, NY	Feb 06, 2017 - Feb 11, 2017	Community SANS
SANS Southern California - Anaheim 2017	Anaheim, CA	Feb 06, 2017 - Feb 11, 2017	Live Event
SANS Munich Winter 2017	Munich, Germany	Feb 13, 2017 - Feb 18, 2017	Live Event
Community SANS Columbia SEC401	Columbia, MD	Feb 13, 2017 - Feb 18, 2017	Community SANS
Community SANS Seattle SEC401	Seattle, WA	Feb 13, 2017 - Feb 18, 2017	Community SANS
SANS Scottsdale 2017 - SEC401: Security Essentials Bootcamp Style	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	vLive
SANS Scottsdale 2017	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	Live Event
Mentor Session - SEC401	New York, NY	Feb 21, 2017 - Mar 23, 2017	Mentor
Community SANS Minneapolis SEC401	Minneapolis, MN	Feb 27, 2017 - Mar 04, 2017	Community SANS
SANS Dallas 2017	Dallas, TX	Feb 27, 2017 - Mar 04, 2017	Live Event
SANS San Jose 2017	San Jose, CA	Mar 06, 2017 - Mar 11, 2017	Live Event
Community SANS Chicago SEC401	Chicago, IL	Mar 06, 2017 - Mar 11, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Mar 06, 2017 - Mar 11, 2017	Community SANS
SANS Secure Singapore 2017	Singapore, Singapore	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS London March 2017	London, United Kingdom	Mar 13, 2017 - Mar 18, 2017	Live Event
SANS Secure Canberra 2017	Canberra, Australia	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS Tysons Corner Spring 2017	McLean, VA	Mar 20, 2017 - Mar 25, 2017	Live Event
Mentor Session - SEC401	Orange County, CA	Mar 21, 2017 - Apr 20, 2017	Mentor
SANS Pen Test Austin 2017	Austin, TX	Mar 27, 2017 - Apr 01, 2017	Live Event
SANS Pen Test Austin 2017 - SEC401: Security Essentials Bootcamp Style	Austin, TX	Mar 27, 2017 - Apr 01, 2017	vLive
Mentor Session - SEC401	Milwaukee, WI	Mar 29, 2017 - May 31, 2017	Mentor
Community SANS San Francisco SEC401	San Francisco, CA	Apr 03, 2017 - Apr 08, 2017	Community SANS
SANS 2017	Orlando, FL	Apr 07, 2017 - Apr 14, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201704,	Apr 11, 2017 - May 18, 2017	vLive
Community SANS Norfolk SEC401	Norfolk, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Apr 26, 2017 - Jun 07, 2017	Mentor
Community SANS Salt Lake City SEC401	Salt Lake City, UT	May 01, 2017 - May 06, 2017	Community SANS
Community SANS Las Vegas SEC401	Las Vegas, NV	May 08, 2017 - May 13, 2017	Community SANS
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event