Security and Risk Management Concerns to Corporations Through the Use of Instant Messaging

SANS GIAC Certification – Version 1.4b August 2002

Submitted By: Martin Porea

Table of Contents

Abstract

Instant messaging is quickly becoming an important communication tool used by many corporations today. The tool is used for a variety of functions, including sending short communications with staff or colleagues, asking quick questions, scheduling meetings, enhancing a customer service function, as well as many others. Instant Messaging is being used in many corporations today to increase productivity and reduce the costs.

However, as with any new technology, Instant Messaging comes with a number of risk management issues that must be acknowledged and addressed. This paper will identify a number of the issues that may impact an instant messaging deployment in a corporate environment. This paper will also offer potential mitigation techniques for the issues identified.

Instant messaging can offer corporations many benefits. Many of the risks associated with instant messaging can be mitigated with technology and the development of sound policies. Corporations should consider implementing instant messaging solutions, but do so using a planned approach versus a ‘grass roots’ approach.

Introduction to Instant Messaging

Instant messaging, once considered a product used by teenagers to chat with one another, has now entered the corporate workplace. IM is quickly becoming an alternative communications tool, which allows employees and co-workers to effectively complete their daily tasks in a productive fashion. Corporations are also discovering that instant messaging solutions can offer a return on investment through cost reductions in long distance telephone calls or cellular telephone calls. Instant messaging is also providing productivity gains by making it easier to reach coworkers, spending less time on telephone calls, and getting immediate response to questions. All of these benefits translate into financial benefits for the corporation.

Instant messaging solutions can also offer opportunities to enhance the customer relationships. For example, an instant messaging solution could be added to a customer portal. Customers using instant messaging may find it easier to interact with the customer support group. Corporations have proven that the cost of providing instant messaging service is far less expensive than a telephone call.

Since instant messaging systems were originally designed to be available to the public, corporations must take care to understand the risks associated with instant messaging systems. Corporate users must understand the difference between the public access systems and the systems designed for internal corporate use.

This document will discuss the various issues that need to be considered by the corporations looking to implement instant messaging. The document will highlight issues associated with the use of IM and will recommend actions that can be taken to mitigate risks. This document will primarily focus on the most popular instant messaging products available and will present the information in general terms. It is recommended that a thorough evaluation be conducted against any product chosen.

Technical Overview and Features of Instant Messaging

The following section provides a brief technical overview of Instant Messaging. This overview is intended to be a high level review versus an in-depth technical discussion.

Architecture

Most instant messaging applications use a client – server based architecture. That is to say, the IM client communicates with an IM relay server in order to perform its tasks rather than communicating directly with another IM client as happens with Peer-to-Peer systems. (An exception to the use of the client-server architecture occurs when the IM clients are conducting file transfers. Some IM systems allow a client-to-client session to be established during a file transfer to allow a more efficient transfer process to occur.) The IM server is responsible for authenticating the IM users, monitoring the 'state' of the IM user, and forwarding or relaying the IM messages being sent. The instant messaging service relies completely on the availability and accessibility to the relay server.

Some instant messaging clients have the ability to modify the port assignments that are used, so a standard port number is not always assigned. This feature was developed primarily to allow corporate users of public instant messaging services (e.g. AOL and Yahoo) to access the public relay servers through firewalls. If a firewall port was blocked or never opened, the instant messaging client would attempt to reconfigure itself to identify an open port on which it could reach the public relay server. This feature makes it nearly impossible to block instant messaging traffic with port blocking. Individual products should be evaluated prior to implementation to understand the specifics for a given application.

Protocols

Protocols used between IM systems today are, for the most part, proprietary. Due to the proprietary nature of the protocols used, most IM systems are closed to exchanging IM messages with dissimilar systems. This is analogous to only allowing the same make and brand of telephones to work with each other. As long as everyone is on the same brand of application, there's no problem. However, given that IM will be used to communicate with business partners, clients, and others, the probability of everyone using the same IM application is small.

Efforts are underway in the IM industry to standardize the IM protocols being used. The two most notable efforts are Session Initiated Protocol for Instant Messaging and Presence Leveraging Extensions, know as SIMPLE, (Additional information on SIMPLE can be found at www.ietf.org/html.charters/simple-charter.html) which is being lead by the Internet Engineering Task Force and JABBER, an open source instant messaging protocol based on XML. (Additional information on JABBER can be found at www.jabber.org) While it may be too early to declare a winner, SIMPLE has support from IBM as it has incorporated SIMPLE into version 3 of Sametime, the IBM Instant Messaging product reportedly used by more than 8 million corporate users. Additionally, Microsoft has incorporated SIMPLE in the current beta release of Greenwich, codename for the newly redesigned collaboration server that incorporates enterprise instant messaging. Given the weight of these two industry leaders, SIMPLE will most likely develop an early lead and a major market share in the enterprise instant messaging space.

Features

Most Instant Messaging products incorporate similar features in their design. At a high level, most products contain the following functionality:

- Awareness – the ability to see who is on-line
- Conversation – exchange messages with a single user or a group of users.
- File Transfer – the ability to exchange files
- Shared Objects – view, edit, and share live documents using whiteboard features
- Multimedia – the ability to incorporate voice and video in a session
- Meeting Rooms – on-line collaboration via scheduled meetings

Some of the IM applications designed for corporate use, products such as Lotus Sametime, include functionality to meet the requirements of the corporate user. This functionality includes:

- Encryption capability for the IM sessions
- The ability for the IM application to leverage a corporate directory
- Translation capabilities of IM sessions between different languages
- The ability to log transactions and/or monitor chats
- The ability to customize the User Interface
- Java based client software (does not require the installation of proprietary client software to the desktop)
- The ability to select the ports used for IM sessions

Security and Risk Management Concerns

As discussed in the Introduction, Instant Messaging is not a product that was initially designed with corporate use in mind. As such, many of the popular Instant Messaging products today are still ill suited for corporate use. Some of the more notable risk management and security issues associated with using Instant Messaging in a corporate environment include:

Exposure to Infected or Malicious Files:

Although basic instant messaging, the sending of text messages between clients does not create an exposure where malicious or infected files could be introduced, the use of such features as file transfers and file sharing could.

When an instant messaging client either accepts a file transfer or shares an application with another user, the IM client is opening up a direction communication path between the two IM clients, rather than allowing the session to pass through the IM relay server. This action introduces the potential for one IM client to intentionally or unintentionally pass and infected or malicious file to the other system.

Some of the more notable attacks that have occurred include a number of successful worms such as Aplore[1], which spread via AOL Instant Messenger (AIM); CoolNow[2], Choke[3], and NewPic[4], which were spread via the MSN Messenger application. Patches for these worms are now available.

Unencrypted Communication Channels:

Many of the Instant Messaging products available today do not include functionality to encrypt or otherwise safeguard the exchange of data between the IM client and the relay server or between IM clients. As such, IM sessions are

[1] A more detailed description of Aplore can be found at http://www.ravantivirus.com/virus/showvirus.php?v=145

[2] A more detailed description of CoolNow can be found at http://www.f-secure.com/v-descs/coolnow.shtml

[3] A more detailed description of Choke can be found at http://www.europe.f-secure.com/v-descs/choke.shtml

[4] A more detailed description of NewPic can be found at http://www.europe.f-secure.com/v-descs/newpic.shtml

susceptible to interception or eavesdropping. Further, user names and passwords sent during authentication could be intercepted.

IP Address Compromises:

The original design of Instant Messaging, the client-server model, allowed users to communicate using IM without risking the exposure of their IP address. However, in an attempt to make the architecture more efficient, sessions that require larger data exchanges, such as file transfers or file sharing, were designed to facilitate the exchange through a point-to-point connection rather than through the relay server. This approach requires that each of the IM clients know the IP address of the other so they can establish and maintain the session. Doing so allows a compromise situation to exist where IP addresses are exposed.

Message Logging and Audit Trails:

Message logging and logging of system audit related material is nearly non-existent with services such as AOL or Yahoo. Services such as Lotus Sametime or Microsoft MSN Messenger offer Instant Messaging solutions that will allow private relay servers to be installed within the corporate network, behind the firewall. System logging and message logging is an important feature that corporations need to consider.

Message logging is particularly important for companies that work in the industries where the Health Insurance Portability and Accountability Act (HIPPA) regulations pertain or Financial Services industries where compliance to SEC regulations may apply. HIPAA (The final version of the HIPAA regulations can be found at http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf) and the SEC regulation 17a-4 (For more information regarding SEC regulations regarding electronic records, please refer to http://www.sec.gov/rules/proposed/ic-24890.htm) require that firms record, log, index, and be able to search, audit and retrieve electronic communications for a period of two years in real-time and six years in a non-real-time fashion. Although neither HIPAA nor the SEC 17a-4 specifically address instant messaging, many attorneys familiar with the regulations feel that the broad nature of the language used for both HIPAA and SEC 17a-4 guidelines regarding electronic communications could be interpreted to include instant messaging. As such, many corporations are taking a conservative approach and adding the additional logging and retention features to meet the regulatory requirements.

Identity Theft and User Account Compromises:

Since a significant number of instant messaging solutions do not encrypt the communication between the instant messaging client and the relay server, the risk of the user account name and password being compromised is high. A user that has an account compromised is now as risk of having their IM identity stolen. The stolen or compromised identity could then start a session with a second party. The second party would not be aware that the first party's account has been compromised and that they are being duped into a conversation with an impersonator. Such a situation might cause the second party to share sensitive or private information unknowingly.

To further complicate the issue, most instant messaging systems rely on directories that use aliases or nick names, not fully qualified names. These services offer little in the way of validating the data provided when a new account is opened. As such, there is little or no assurance of the true identify of the account holder.

Social Engineering:

Social engineering is a term describes the process of 'tricking' an individual to divulge information that is private or sensitive in nature. Since instant messaging relies on a system of trust, where a user's identity cannot be confirmed, social engineering is possible. For example, assume an instant messaging user with a name of SYSTEM ADMIN contacted another instant messaging user. It may be possible for the SYSTEM ADMIN user to convince the other user that they are the SYSTEM ADMIN for the service and convince them to provide their user account name and password for maintenance purposes. This would represent a social engineering compromise.

Copyright or Trade Secret Infringement:

There is a two-fold risk related to Copyright or Trade Secret infringement. Both conditions are issues that corporations should consider. First, a condition exists where sensitive internal material could be transferred via the instant messaging system to unauthorized individuals. This situation could be either intentional or unintentional, perhaps through a social engineering attack or an identity theft situation.

The second type of risk related to Copy Right or Trade Secret infringement comes in terms of receiving the material. Corporations are now at risk for data stored on employees' computers. This data could contain bootleg MP3 files, illegally copied copyrighted material, or some of form of trademark infringement. Employers could be held liable for such material being stored on corporate computers.

Harassment or Inappropriate Language:

As with any form of electronic communication, the possibility of abuse exists. Corporations must be concerned with the inappropriate use of the instant messaging system to cause harassment, send inappropriate material, or communicate using inappropriate language. Similar to email, employers can be held legally liable for misuse of corporate resources or for failing to take actions to prevent misuse.

Options to Mitigate the Risks Associated with Instant Messaging

In this section of the document, options will be discussed to manage the risks categories that were identified. As with any risk management plan, it's unlikely that a single policy, technology, or approach would be used to manage risk. What is required is a risk management plan that incorporates the use of multiple approaches, including policies, technologies, and user awareness. A combined approach to addressing risk management allows the best overall plan to mitigate the risk to an acceptable level.

Exposure to Infected or Malicious Files:

Limiting exposure to infected or malicious files could be accomplished through a number of techniques. Any or all of the techniques described would help reduce the risk.

1) Install anti virus software and/or personal firewalls on the desktop computers. This is the most effective way to detect and eliminate compromised files. Firewalls and Intrusion detection systems today are still not capable of accurately detecting and identifying malicious code being passed in instant messaging traffic.

2) If practical, consider disabling the features associated with file transfers or file sharing if the package allows. Blocking ports that the application may use for file transfers or application sharing is another option, but will depend on the specific application. Some applications use defined ports for this functionality, while others allow the user to reconfigure the ports.

Packages such as AOL AIM, Yahoo, and Sametime are difficult to block at a port level due to the application allowing the selection of different ports in the event the default port is blocked. (AIM however does use a default port for image exchange that can be blocked. The AIM image exchange port used is TCP 4443. Sametime does not offer public relay servers, so it is less of a concern.)

MSN's recently released .NET (Greenwich) collaboration server uses specific ports for file transfer, audio and video, and application sharing. The ports are TCP 6891, UDP 13324 and 13325, and TCP 1503 respectively. However, given the fact that the MSN collaboration server is designed to be an enterprise solution, it is more than likely to be used as a private instant messaging service and not have the same risks associated with it's use as would a public service.

Another alternative that could be considered is to block all traffic to the public relay servers. This option would however block instant messaging traffic as well as file transfers and application sharing features. To block traffic to the public relay servers, the domain name or IP address must be blocked. Doing so we prevent an instant messaging client from reaching the public relay server, regardless of the port the client tries to use. It should be noted that since most public relay servers use a 'round robin' approach to load balancing across multiple relay servers, the most effective approach is to block the sub-domain associated with the relay server and not the IP address, as there may be any number of IP addresses used.

The most popular instant messaging relay server sub-domain names are listed below along with port blocking recommendations.

- MSN – msgr.hotmail.com and block TCP port 1863
- AIM – login.oscar.aol.com and block ALL ports.
- Yahoo – *.msg.*.yahoo.com and block all ports (Where * represents a 'wildcard'.)

It should also be noted that blocking access to the sub-domains of the instant messaging public relay servers at the enterprise firewall will restrict authentication to the public IM services, a user could bypass this added security assuming they were to gain access to an externally configured proxy server. In this case, and intrusion detection system or IM sniffer product may be the only way to identify instant messaging traffic on the network.

3) Create a communications awareness plan to make users aware of the risks associated instant messaging and, specifically, with file transfers or application sharing. Education can go a long way to reducing risk.

Unencrypted Communication Channels:

Unencrypted communications can be addressed in two ways. First, simply select an instant messaging solution that incorporates encryption technologies that meet your requirements. This is by far the simplest and easiest way to address the situation.

For products that do not support native encryption, there are a number of 3rd party products available that may provide 'after market' encryption. A couple of examples of products to consider include:

- Trillian (http://www.ceruleanstudios.com/trillian/index.html)
- IM-Age (http://www.im-age.com/)

Adding a 3rd party encryption package will provide encryption to those users who have the added application installed. However, for communications with users who may not have the 3rd. party application installed, like business partners or customers, the encryption would not be extended to those sessions.

Developing a communication plan to educate the user community of the dangers of communicating over an unencrypted session is also important factor to mitigate risk.

IP Address Compromises:

IP address compromise is a more difficult situation to address. By design, Instant Messaging must reveal an IP address when creating a peer-to-peer session. The best method to address this situation is to make the user base aware of the situation and educate them on the dangers associated with using peer-to-peer features. Clear policies should be established that governs the use of file transfers and application sharing.

If the file transfers or application sharing will be done with users that may reside outside of the corporate firewall, Network Address Translation (NAT) may help. Although the user outside of the firewall would still see an IP address, that address would be of the corporate firewall itself and not the individual user. This may help reduce the direct threat to an individual user.

If the risk of having an IP address compromised is to great for any particular circumstance, the only effective way to eliminate the risk is to block access to any functionality that would require a peer-to-peer session. This may vary depending on the individual application being used, but a good rule of thumb would be to consider any functionality involving file transfer, voice or video, application sharing, or image exchange.

Message Logging and Audit Trails:

In additional to general best practices associated with the monitoring and review of system audit files as a risk management practice, industry and government regulations related to HIPAA and SEC 17b-4 has specific requirements. In general, those regulations require companies to record, log, index and be able to search, audit, and retrieve electronic communications. The regulations do not specifically identify instant messaging as a covered technology, however, based on the broad interpretation associated with electronic communication, a number of legal sources feel the regulation could be interpreted to include instant messaging communications. As such, consideration should be given to determine the requirements for your network.

Although most of the commercial products intended for private IM installations offer very basic logging and auditing functionality, a number of 3rd party products are available to supplement the features offered in the IM applications. A number of 3rd. party applications are available to provide logging and archiving. Such packages include:

- Imlogic (http://www.imlogic.com/)
- Communicator Hub (http://www.communicatorinc.com/)
- Ikimbo (http://www.ikimbo.com/).

These 3rd. party solutions work with most all of the popular IM applications discussed in this document.

In addition to logging and archiving, compliance software may be required. Compliance software provides content filtering to search and annotate IM sessions. Products that provide features with the ability to filter content from IM sessions and provide annotation features include:

- FaceTime (http://www.facetime.com/main.shtm)
- Imlogic (http://www.imlogic.com/)

Further, both of these applications provide a feature that allows a company-specific disclaimer to be included in IM sessions. Although the disclaimer may do little to safeguard data inadvertently or intentionally sent to the wrong person, there may be value associated with the use of a disclaimer if litigation were to result from an incident. This would be similar to disclaimers used on facsimile transmissions or network login banners stating the data is confidential and intended for only authorized addressees or users.

Auditing and logging, as well as compliance requirements, are more difficult when using public instant messaging solutions. If auditing, logging, and compliance are requirements, it may be best to consider a private enterprise solution. The use of disclaimers however, is a good policy to establish regardless of whether or not a private or public instant messaging solution is used.

Identity Theft and User Account Compromises:

A couple of approaches can be used to minimize the risk associated with Identity Theft and User Account compromises.

1) The use of an instant messaging solution that incorporates encryption will help minimize the ability for someone to intercept a user name or password being sent in clear text.

2) Instant Messaging systems that utilize a company's internal directory service should be used. A number of instant messaging systems designed for corporate use can now leverage LDAP directories. As such, the instant messaging system can be configured to utilize the fully qualified user name contained within the LDAP directory. This fully qualified name will be more difficult to impersonate and will provide some level of assurance to users that they can identify the person that they are communicating with. (This again will only address communication between instant messaging clients on the same system. This does not apply to use outside of the corporate network.) Further, the use of an internal directory provides more management control over users being added or removed from the instant messaging service.

Social Engineering:

The only effective way to address social engineering is education. User must be educated in the techniques used by social engineers. User must be taught to never divulge private information to anyone that cannot be definitively identified.

As with many of the recommendations, a user awareness program should be developed and implemented.

Copyright or Trade Secret Infringement:

Instant messaging system is not the root cause of this risk; it is just a vehicle to facilitate the transfer of the material. The users themselves can only effectively mitigate this risk. As such, a program to educate users to the risks should be undertaken. Included in the communications should be related risks that could contribute to the inadvertent release of confidential information. Those related risks would include social engineering and identity theft.

In addition to the program of education, a policy describing the process and exchange of sensitive or private information should be communicated. The policy should address the acceptable, as well as unacceptable process for exchanging or copying sensitive data.

Harassment or Inappropriate Language:

As with the copyright infringement, this issue must be addressed through education and policy. A policy that addresses the position on harassment and inappropriate language must be published. The policy must also address the disciplinary actions that will be taken for violations. The policy must also be reinforced with an education program that promotes awareness.

Depending on the degree of enforcement that a corporation determines it needs, compliance software such as that mentioned in the Message Logging and Audit Trails section offers a search feature that could be used to search for key words. Those key word searches could be used to identify violations of corporate policy related to inappropriate language.

Further Considerations:

In addition to the items addressed above, a few other items should be given consideration. These items don't fit neatly into any of the above categories but are important nonetheless.

Corporations should identify a standard product for use within the corporate network. This selection of a standard product will allow the IT or Security specialists to focus on securing a single product versus multiple solutions. This will also have additional benefits to the corporation in that it will help control costs and allow for standardized support processes.

Further, IT departments should enforce the use of standard products. This enforcement could come in a number of ways. The IT department, if practical, could lock down the desktop configuration to prevent users from adding non-standard software. This would prevent outside software from being added.

IT departments could also monitor the network for rouge instant messaging traffic. Network traffic analyzers or sniffers are effective in identifying unauthorized instant messaging traffic on the network. Once identified, steps can be taken to block access to specific ports, both inbound and outbound, at the firewall. Networks should be analyzed periodically to determine if unauthorized traffic is traversing the network.

If the corporate IT department doesn't own a sniffer, or if the sniffer does not support instant messaging protocols, a number of free sniffers are available. These include:

- Network Probe (http://www.objectplanet.com/Probe/)
- IM-Age (http://www.im-age.com/_downloads/snifflic.asp)
- Ethereal (http://www.ethereal.com)

Conclusion

Instant messaging systems are quickly becoming a key component of the corporate communication network. Instant messaging can offer important productivity and costs savings if implemented properly. However, there are number of risks that must be identified and managed before a deployment can be undertaken.

Corporations serious about instant messaging systems should consider a system that is installed within the corporate firewall, not a publicly accessible system. When selecting a system for corporate use, features such as encryption, the ability to use a corporate directory for authentication, logging and access to the application code for customizations should be considered.

In addition to the technical considerations given to instant messaging systems, security policies and user awareness programs are also required. The policies are required to state conditions for acceptable usage of the technology, guidelines for governing language and inappropriate material, as well as state a standard for the type of instant messaging system that is acceptable.

References

Flynn, Nancy
The ePolicy Handbook
American Management Association 2001

Kontzer, Tony
Battening Down The Instant-Messaging Security Hatches
Information Week June 10, 2002
http://www.informationweek.com/story/IWK20020607S0017
(March 16, 2003)

Langa, Fred
Langa Letter: More Instant-Messaging Security Holes
Information Week October 1, 2001
http://www.informationweek.com/story/IWK20010927S0021
(March 16, 2003)

Vamosi, Robert
The next hacker target: instant messaging
ZDNet Reviews May 30, 2002
http://zdnet.com.com/2100-1107-928415.html
(March 16, 2003)

Symantec Enterprise Security (no individual author identified)
Securing Instant Messaging
Whitepaper
http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf
(March 16, 2003)

Hindocha, Neal – Symantic Security Response
Threats to Instant Messaging
Whitepaper October 2002
http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf
(March 16, 2003)

Internet Security Systems (no individual author identified)
Risk Exposure Through Instant Messaging And Peer-To-Peer (P2P) Networks
White Paper April 2002
http://www.iss.net/support/documentation/whitepapers/xforce.php
(March 16, 2003)

Greenfield, David
Taming the IM Animal
Network Magazine February 2003
http://www.networkmagazine.com/article/NMG20030204S0004
(March 16, 2003)

Greenfield, David
Lesson 175: IM and the IETF
Network Magazine February 2003
http://www.networkmagazine.com/article/NMG20030204S0003
(March 16, 2003)

Greenfield, David
IM's Buddy Brawl
Network Magazine December 2002
http://www.networkmagazine.com/article/NMG20021203S0010
(March 16, 2003)

Sigaba (no individual author identified)
Sigaba Instant Messaging and Presence
Technical White Paper October 15, 2002
http://www.sigaba.com/products/whitepapers/SG_wpaper_SSIM.pdf
(March 16, 2003)

Olavsrud, Thor and Saunders, Christopher
Microsoft Unleashes Greewich IM Beta
Datamation March 6, 2003
http://www.instantmessagingplanet.com/enterprise/article.php/2105971
(March 16, 2003)

IBM Lotus Web Site
Sametime Home Page
http://www.lotus.com/products/lotussametime.nsf/wdocs/homepage
(March 16, 2003)