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

Finding the Right Instant Messaging Solution for Your Company

Jeff Richeson
February 3, 2003
GSEC Practical Assignment
Version 1.4b, option 1

Abstract

Instant messaging (IM) provides the ability to know when others are online and communicate with them in near real-time. Many security issues arise when using IM clients in the workplace. The solutions to the IM security issues range from blocking IM completely, to attempting to manage public IM, to purchasing an IM system that is meant for business use. The purpose of this paper is to assist the reader in making an informed decision about properly securing IM for use in the workplace.

Background

Instant messaging (IM) provides the ability to know when others are online and communicate with them in near real-time. IM is gaining popularity because it "… fills a niche between a phone call and e-mail--it's fast, and not too intrusive" (Vamosi). AOL, Microsoft, and Yahoo are currently the three major providers of public IM services.

Although each of the three providers implements IM differently, the basic concepts are the same. The user downloads and installs a desktop application or Java applet on the computer. An account must be created by the user if one does not already exist for the service. Once logged in, the user's list of contacts are presented. The user can communicate to any of the contacts that are also online. All text messages are first routed through the server and then to the other person. For certain high-bandwidth uses such as file transfer, audio, or video, peer-to-peer connections are brokered by the server. Currently, none of the major clients are able to send messages to users of a different service. The installation and account creation process must be repeated for each IM client.

AOL was granted a patent in September, 2002, for the invention of IM (Hu). However, IM in different forms has been around for longer. Many of the early Unix computers used in colleges and universities have "finger" and "talk" executables that allow users to find others logged in and establish a peer-to-peer interactive conversation. These Unix programs seem rudimentary when compared to the capabilities of today's IM clients. Today's clients have supplemented the text chatting with fonts, graphical icons, file transfer, voice, and video. Unfortunately, with the additional features come additional security concerns.

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

Purpose

The purpose of this paper is to assist the reader in making an informed decision about properly securing IM for use in the workplace.

IM Security Issues

IM clients were initially built for home-users, not businesses (Frase). Because of this, they emphasize functionality rather than security. However, the home users like to install the same insecure IM client at work. A recent non-scientific poll of internet users showed that 39% of those who responded used IM at both home and work (Woods). In many cases, the IM clients are installed on work computers without the approval of the IT department. Compounding the problem, the company may not have a policy that covers IM usage. In addition, companies that have IM policies often find the policies to be unenforceable. The unregulated installation of IM clients makes a company vulnerable to the following security issues:

- Unsecure traffic on a secure network – The company LAN is protected by a firewall that is supposed to block any malicious network activity initiated outside the network. The IM client punches a hole through the firewall which can allow in viruses, spam, and other unwanted files (Willner).
- Lack of authentication – Since each user chooses his own identity, one can never be sure if the message recipient is really who he claims to be (Frase). Because these user names are not generated by the IT department, tracking an IM message to the actual person may be difficult, if not impossible. Also, an employee can think he is communicating with a coworker while he is actually talking to a competitor.
- Social engineering – The informal nature of the communications sometimes makes it easier for intruders to trick users into downloading files or doing other activities to compromise the security of their own computer (Sullivan). Additionally, leading questions can be used to trick employees into accidentally revealing company secrets in IM conversations.
- Privacy concerns – Little or no encryption is used for login credentials sent to the server. Stolen credentials can easily be used to impersonate someone else. Also, no encryption is used for the messages. Because all messages must travel to the server before being forwarded to the recipient, the messages can easily be logged by the sender, recipient, server, or someone eavesdropping on the conversation ("Risk Exposure").
- Client vulnerabilities – Just like any other application, IM clients must be hardened against malformed data. Buffer overflows and other client vulnerabilities can lead to problems such as denial of service, client crash, or remote execution of code (Frase).

Each one of these vulnerabilities taken by itself may not be such a large issue. However, all of these issues taken together can lead to potential compromise of the entire company LAN. IT departments should start planning and preparing to defend the network against these security issues.

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

IT Decisions

IM is already in the workplace and it is predicted that business use will make up around 43% of the IM use in 2006 (Thorsberg). The IT department has several ways in reacting to the security issues. The IT department can ignore the issues, develop a policy, implement a complete lockdown, manage the use of public IM, or use enterprise IM. Each of the choices may not be exclusive of the others. Depending on the needs of the company, the IT department can take a phased approach to controlling IM.

Ignore Issues

"Unsecure IM lines are one of the hottest new targets for hackers looking for critical corporation information to steal" (Gaudin). Unfortunately, many IT departments allow unsecure IM installations to remain. One reason IT departments ignore IM is because they believe that IM is not being used within the company. Additionally, IT departments may believe that they do not have to worry about IM security because they already maintain a corporate firewall with antivirus protection and they restrict employees from installing software on their own computers. This course of action (or inaction) is cheap and easy: it requires no direct money, time, or effort. However, completely ignoring IM security issues is not a good idea.

One reason that IM should not be ignored is because IM is difficult to block at the firewall because the client is built to evade the firewall defenses (Vamosi). As long as a connection to the Internet exists, the IM client will attempt to connect to the server through a variety of ports until it succeeds. The IM vendors did not build the client this way to be harmful to the IT department, but rather to reduce their own support calls from the home user.

Another reason for not ignoring IM security issues is that even if users cannot install software on their own computers, they still can use an IM client because it can be run in a Java applet embedded within a web page. The java applets usually provide a reduced-functionality client. Nonetheless, these clients still have most of the security issues related to the full-functionality clients. Restricting Java applets impacts the usability of many other websites.

A final reason for companies not to ignore IM is that certain companies are required by law to monitor communications within the company. Companies that provide financial or healthcare services have been required to store and audit communications. Traditionally, this has meant phone and email, but it also includes IM (Saunders, "Enterprise").

Ignoring these issues is not a reasonable option. IM is probably already in use within the company, and something should be done to secure it.

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

Develop Policy

Developing an acceptable use policy for IM is a method of dealing with IM security issues. This policy would inform and educate employees of the appropriate uses of IM within the company. A company may choose to use only a policy approach because of limited funds. The cost of developing a policy is the cost of time; no additional purchase of hardware or software is needed. The company probably feels that they can sufficiently educate employees on the reasons to follow the policies.

The following steps will briefly describe what should be done to develop a useful policy concerning IM. Before drafting a policy, some amount of time should be spent studying the issues. A good first step would be to informally survey the employees to see how it is being used. The survey should include information such as:

- which client (AOL, Yahoo, Microsoft, other)
- what services (chat, voice, video, file sharing, collaboration)
- uses (business, personal)
- who employees chat with (coworkers, customers, clients, friends, family).

Next, perform a risk analysis and assess the tradeoffs between the benefits and the risks. The risk analysis takes into account each security vulnerability and the likelihood of a hacker exploiting the vulnerability. Finally, using all the information gathered, develop a policy that addresses the acceptable use of IM within the company.

The main disadvantage of a policy only approach is that without a means of enforcement, some percentage of the employees will ignore a written policy. Policy development is a good first step but, it is probably not sufficient on its own.

Complete Lockdown

A complete lockdown of IM usage is on the other extreme from ignoring the issues. The lockdown may be warranted after a risk analysis shows substantial risk and/or minimal benefit. When done properly, blocking IM services at the firewall will protect the company from the security issues of the known services that are blocked. As long as the company already owns a firewall, no additional purchases of hardware or software is required.

Normally, when a specific internet service is to be blocked, a port or port range is blocked at the firewall. However, it is not always that simple because IM clients do not use a standard protocol. In fact, each client has invented its own protocol to communicate to the server. Akonix System, a company that develops IM management tools, terms this as “Rogue Protocols” and defines them as “nonstandard application protocols that can expose confidential information, invite viruses in the network and provide conduits for malicious external attacks” (“Protecting”). Each IM client uses a different port number for communicating to the server. Many of the clients can be configured to use alternate ports, including port 80, which is the port used for web browsing. The clients are built

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

like this for the convenience of the consumer and to reduce support calls to the vendor. However, this build-in "convenience" causes problems for an IT department trying to manage communications through a firewall. A better way to block the clients is to block all communications to the IM authentication servers by name. This can easily be configured at the firewall for all the major IM services and will block all users except for the ones who can use an external proxy server to route the messages ("Risk Exposure"). "A simple search on the Internet will return hundreds of freely available proxy servers. Keeping up with blocking each one is an administrative nightmare" (Hindocha). Below is a table compiled from a whitepaper written by Akonix System that details the exact ports and domain names to block at the firewall in order to disable the specified services ("Protecting").

IM Client	Service	Block at firewall
AOL Instant Messenger (AIM)	File transfer and file sharing	Block TCP port 4443, inbound and outbound
	All IM services	Block access to login.oscar.aol.com on all ports
Microsoft Messenger	File transfers	Block TCP port 6891, inbound and outbound
	Audio and Video conferencing	Block UDP ports 13324 and 13325
	Application sharing	Block TCP port 1503
	All IM services	Block access to all hosts in msgr.hotmail.com subdomain
Yahoo! Messenger	All IM services	Block access to *.msg.*.yahoo.com
AOL ICQ	File transfers	Block TCP port 3574
	File sharing images	Block TCP port 7320
	All IM services	Block access to login.icq.com

Table 1: How to block IM at the firewall

Although blocking IM can be cheap because no additional purchases are required, it is not always easy or complete. Even when the above instructions are followed, only the major IM services are blocked and any other IM services still function. Another disadvantage to this approach is that the potential benefits from IM have disappeared. IM is becoming a more accepted means of communication in business. Instead of attempting to implement a complete lockdown, most companies would probably rather install proper controls to have IM be useful while minimizing the risk.

Manage Public IM

Managing the public IM services is a reasonable compromise between doing nothing and a complete lockdown. The management tools allow use of the public IM clients while adding regulation and control features needed by the IT department. IM management usually involves the procurement of software from

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

an outside vendor that specializes in this area. In general, this software is run from a central location and is not installed on the desktop. The IM management software does not change the client in any way. The software acts similar to a firewall for IM. As an additional bonus, certain management software can also help control peer-to-peer networks. Below is a composite set of enhancements to public IM made by the IM management software. Each IM management is different and may not provide all the functionality below.

- Authentication – On public IM, each user selects his own name. In general, the name selected by the user is not the same as the one given out by the company. This makes it difficult for the IT department to track who is using IM because, for instance, "theboogyman" on IM is really "jsmith" within the company. The management software maps IM user names to corporate login IDs which can be authenticated against a local directory service.
- Blocking – Without any controls, any user can log on to IM with any of the available clients. Because the management software is able to authenticate users to corporate directory, it can also use that information to authorize them. Unauthorized users and clients will not be allowed to connect to the server.
- Monitoring – One of a company's concerns with IM is that inappropriate communications may take place. This may be a disgruntled employee distributing company secrets, or a lazy employee taking dirty to a stranger. In either case, the company would prefer this communication not to be taking place at all. The management software provides alerts to administrators for certain events, messages, or keywords in an IM conversation.
- Logging and Auditing – Government regulation requires some industries (such as healthcare and financial) to record all conversations with clients which include IM conversations. Other industries record conversations as a matter of policy. In either case, this is not possible with public IM alone. Management software allows the capture of both sides of the conversations in a central location. The central repository of conversations can be audited to assure compliance with IM usage policies. Conversations should be deleted according to a retention policy.
- Routing – From the point of view of the user, messages are sent directly from his computer to the recipient's computer. In reality, the message was sent to IM server first before being delivered to the recipient. This means that employees who send sensitive information over IM to coworkers may have the false impression that the messages never leave the company. The management software ensures that communications for someone else inside the same company are not routed outside the company to the central server.

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

The disadvantages to IM management software are that it costs money and it takes time to configure and maintain. Also, the company's IM services are dependent upon the functionality of the public IM service.

Enterprise IM

Instead of relying on public IM which is meant for the consumer market, there are IM systems that are built specifically for business use. These Enterprise IM (EIM) systems provide companies their own clients and servers that are built with enterprise security features. In addition to the server features of authentication, blocking, monitoring, logging, auditing, and routing, as described in the previous section, EIM has additional features not found in public IM:

- Encryption – With public IM, all communications are unencrypted and can be read by anyone who intercepts the communications. EIM allows communications to be encrypted to prevent anyone except the intended recipient from understanding the contents. However, one detail that is not readily disclosed is that the encryption only works when both the sender and receiver are using the same type of client. This means that, for example, while an EIM Yahoo client can communicate with a standard Yahoo client, encryption is not possible between the two.
- Client tailoring – With EIM, the IT department has more control over the features that are available on the clients. Instead of just disabling features at the firewall, features can be disabled on the client interface so that the user does not even attempt to access them. This includes features such as games, voice and video chat, and file transfer.
- Namespace – Instead of each user tying to find IM user names that are not already in use on public IM, a company using EIM can use its own email addresses or other naming scheme to identify the users as employees of that company. Since each company has its own namespace, there will be no conflicts with user names in other companies. This naming makes it easier for the IT department to track and audit the IM users.

If IM is only needed for communication within the company, a closed EIM system can be used. This system does not operate with any of the public systems and cannot be used to communicate outside the company. A closed system is ideal for collaboration among employees in a company. Using a closed system avoids many of the security issues discussed earlier, but it also cannot take advantage of the wide audience that public IM has. Also, unless the closed IM system has the ability to block the public IM clients, some employees will continue to utilize the public IM.

Around October of 2002, the major IM providers began deploying their own EIM services. Each IM vendor has partnered with one or more IM management software vendors to integrate the management services in the EIM products. The new EIM service from each vender interoperates with the standard IM service offered by the same vendor but not the other vendors. Because of the

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

integration of the management software into the EIM service, the same management features discussed above are part of the EIM service. The major disadvantage of purchasing an EIM system is that the system does not interoperate with other vendors' systems. A company locks itself into communicating only with other users on the same vendor's IM system. Another disadvantage is that the encryption only works when both the sender and receiver are using an EIM client. This means that encryption is not available when it may be needed most: communicating to users over the internet who are using the public IM clients.

Attempts at Interoperability

Although interoperability issues do not directly affect the security of IM, they are a major consideration when choosing an IM system. Interoperability among the major IM clients has been a goal for several years now. At least, it has been a goal of regulators and consumers, but probably not a goal of all the vendors. The vendors do not want clients that work with another vendor's client. Interoperability would mean that consumers could use just one client to communicate with anyone on a public IM system. To work together, vendors must agree on a common protocol and a basic set of functionality. In 2000, a consortium of IM vendors was formed to discuss building a unified messaging service. AOL, the largest IM provider, was not invited to participate (Wearden). A separate attempt at creating a common protocol has achieved some limited success. SIMPLE stands for Session Initiation Protocol (SIP) for Instant Messaging and Presence Leveraging Extensions. This protocol is close to becoming an official standard and has been incorporated in some vendors' products. However, due to a lack of robust features, some vendors have reduced or dropped the protocol completely (Saunders, "SIMPLE"). It seems that true interoperability among clients may still be a few years away.

A few small IM vendors take a different approach to the interoperability issue. They offer a single client that has a few enterprise features, such as encryption, and it works with all of the major services. The single client can be used to send messages to any user on a major IM system. Instead of using a common protocol, these clients must use all the proprietary protocols of each IM system with which they communicate. The major disadvantage of these clients is that they are piggybacking on the major providers' servers and can be blocked by the vendor at any time because they have no official agreement to use the servers (Thorsberg).

Choosing the Right IM System

Which of these options is best? There is not one answer that fits every situation. These are the major variables in the equation:

1. The company's need for IM services
2. Available funds for purchases
3. Risk versus benefit assessment
4. Regulatory compliance

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

If there is no business need for IM, no money for purchase, high risk and low benefits, or stringent regulatory compliance issues, then IM should probably be completely blocked at the firewall. However, this decision will be unpopular with any employee currently using IM. If the block is only temporary so that more appropriate security measures can be put in place, convey the timeframe for the block to the employees. Ensure that the reasons for blocking IM are clearly communicated to the employees.

If the only business need for IM is to communicate with employees within the company and there are funds available for purchases, then a closed IM system can be bought and deployed within the company. The closed system will avoid most of the security and regulatory issues associated with the public IM systems. Additionally, blocking the public IM clients at the firewall will need to be done to enforce using only the closed IM system.

If there is a business need to communicate to users outside the company, money for purchases, and benefits that outweigh the risks, then purchasing IM management software would be the correct choice. The management software allows the company to leverage the power of the free public IM systems while maintaining control of how it is used within the company. If regulatory compliance is an issue, choose IM management software that has the needed abilities of recording, auditing, and reporting of IM conversations.

At this time, purchasing an EIM system from a major vendor does not seem to make business sense. The EIM client will only be able to communicate with other clients from the same vendor, leaving out the segment of the population that does not use a client from that vendor. The IM management software that is integrated with the EIM service can be purchased separately (and when purchased separately will manage IM from all major vendors). The encryption only functions when communicating with another EIM client. The EIM services need more time to mature and the vendors should work on interoperability before EIM will become useful in business.

Conclusion

IM is already in use in business and is gaining popularity. Public IM poses a security risk for a company because the clients can quickly be installed and can easily evade current firewall defenses. A policy should be developed that addresses the acceptable uses of IM. The policy should be enforced by a technical means of either blocking the services at the firewall or using management software to help regulate and control IM usage. The lack of interoperability between different clients causes the EIM offering from the vendors to be less useful.

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

References

Frase, Dan. "The Instant Messaging Menace: Security Problems in the Enterprise and Some Solutions." 31 January 2002. URL: http://rr.sans.org/threats/IM_menace.php (15 Nov. 2002)

Gaudin, Sharon. "IM Security Risks Spark Workplace Monitoring Debate." eSecurityPlanet.com. 6 Sept. 2002. URL: http://www.esecurityplanet.com/trends/article/0,,10751_1458241,00.html (25 Nov. 2002)

Hindocha, Neal. "Instant Insecurity: Security Issues of Instant Messaging." Security Focus Online. 13 Jan. 2003. URL: http://online.securityfocus.com/infocus/1657 (22 Jan. 2003)

Hu, Jim. "Patent creates IM wrinkle." News.com. 17 Dec. 2002. URL: http://msn-cnet.com.com/2100-1023-978234.html (22 Dec. 2002)

"Protecting the Enterprise from Rogue Protocols." Akonix. 2002. URL: http://www.akonix.com/download/support/AkonixWhitepaper-ProtectingFromRogueProtocols.pdf (3 Dec. 2002)

"Risk Exposure Through Instant Messaging and Peer-To-Peer (P2P) Networks." Internet Security Systems. April 2002. URL: http://documents.iss.net/whitepapers/X-Force_P2P.pdf (2 Dec. 2002)

Saunders, Christopher. "A Lack of SIMPLE Pleasures." InstantMessagingPlanet.com. 12 Nov. 2002. URL: http://www.instantmessagingplanet.com/enterprise/article.php/11208_1498911_3 (20 Jan 2003)

Saunders, Christopher. "Enterprise IM Spurs Privacy Concerns." eSecurityPlanet.com. 18 Nov. 2002. URL: http://www.instantmessagingplanet.com/enterprise/article.php/10816_1502941 (25 Nov. 2002)

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

Thorsberg, Frank. "Is IM a Sieve for Corporate Secrets?" PCWorld.com. 19 July 2002. URL: http://www.pcworld.com/news/article/0,aid,102867,00.asp (20 Nov. 2002)

Vamosi, Robert. "Instant messaging: The next hacker target." ZDNet Tech Update. 29 May 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2868239,00.html (26 Nov. 2002)

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

Wearden, Graeme and Richard Barry. "AOL not invited to IMUnified alliance." ZDNet UK News. 26 July 2000. URL: http://news.zdnet.co.uk/story/0,,t269-s2080416,00.html (20 Jan 2003)

Willner, Susan. "Instant Messaging: How Secure Is It?" 19 August 2001. URL: http://rr.sans.org/threats/IM2.php (15 Nov. 2002)

Woods, Bob. "IM Poll Results." Instant Messaging Planet. 7 Jan. 2002. URL: http://www.instantmessagingplanet.com/enterprise/article.php/10816_946951 (21 Dec. 2002)

© SANS Institute 2003, Author retains full rights

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