Instant Messaging

JOHN STONE AND SARAH MERRION, SYMANTEC

or Instant Headache?

IM has found a home within the enterprise, but it's far from secure.

It's a reality. You have IM (instant messaging) clients in your environment. You have already recognized that it is eating up more and more of your network bandwidth—and with Microsoft building IM capability into its XP operating system and applications, you know this will only get worse. Management is also voicing concerns over the lost user productivity caused by personal conversations over this medium. You have tried blocking these conduits for conversation, but it is a constant battle. Tools are now available to make this blocking job easier, such as those from Akonix,¹ FaceTime Communications,² and NetIQ,³ but IM is maturing, and your users are starting to depend on it as an essential business tool.

IM allows you to avoid long-distance phone charges you might otherwise incur, and it lets you know right away whether the person you're trying to reach is available. So now you realize the question is becoming, would you really want to block this traffic if you could? IM may be enhancing your bottom line. Despite management's concern, your users are more often than not using IM to be more productive in each workday. They are using IM to communicate with their coworkers more than their friends. They

Instant Messaging or Instant Headache?

are spending less time on the phone and reducing the time it takes to find someone with an answer. Quick, easy answers are what IM provides.

You can easily come to the conclusion that IM serves a useful purpose for your business and that the time has come to embrace it in your environment. Like many of the new Internet-based electronic tools, however, IM represents a significant risk to the security of your environment—so much so that Gartner identified IM as one of the top 11 security threats for 2003.⁴

Your job is to mitigate these risks without preventing the added productivity IM can offer to your organization. This article explains the risks to the environment that IM represents or could represent and possible controls you can use to mitigate these risks. Security is a management function of a business, not a technical function; although information security has its technical aspects, it is also primarily a management function. Technology is a method of implementing controls and mitigating the known and unknown risks. This article therefore may be less technical in nature than others.

THE CIA SECURITY MODEL

IM is here to stay, so what does this mean to the security of your network? What can happen? To understand the answers to these questions, you must first have a basic understanding of the purpose of information security and what it is trying to accomplish. This will allow you to look at the functionality of IM and see for yourself the possible ramifications of those actions to the security of your environment. The easiest way to describe the purpose of information security is to frame it in the discussion of a security model.

A widely accepted information security model is the CIA triad of *confidentiality*, *integrity*, and *availability* (see figure 1). These three key principles are oriented around the concept of securing data, whether the data is legal documents, the latest sales figures, the current pay of all employees, or the design codes running your production lathe. Part of your job is to guarantee these principles are met by putting in place administrative, physical, and technical controls to provide a secure environment. What

makes this difficult is that these principles somewhat contend with each other; you can lock down access to a file so tightly to keep the information safe from unauthorized viewing, loss, or corruption that it is virtually impossible for those who need access to that data to get that access. You must find a balance among the three goals of the CIA triad that best meets the needs of your environment.

Confidentiality. This is the concept of keeping your data private, allowing only those authorized to view or use the data to have access to that data. The importance of this concept is the easiest to understand of the CIA triad, but it is the confidentiality of data that is the most often attacked and that most often fails. Access control methods such as door locks, privacy screens, security guards, passwords and secure tokens, and encryption technology embedded in secure connections such as SSL (Secure Sockets Layer) and VPN (virtual private network) connectivity are all examples of attempts to ensure confidentiality of data stored on systems or transferred from one computer to another. Document-forwarding computer worms are examples of a security attack targeting confidentiality.

Integrity. This is the concept of making sure that data is accurate and stays that way throughout storage or

CIA Triad

FIG 1

transfer to another system. Read-only file access, document-change tracking, and file and e-mail signatures are examples of attempts to ensure the data does not change from its original form. One type of integrity security attack is the interception of important data, then making changes to it before sending it on to the intended receiver.

Availability. This is the concept of making sure the data is available to all authorized users when they need it. File backup, clustering servers, storage area networks, and business continuity planning are all examples of attempting to ensure the availability of data. A well-known security attack is a DoS (denial of service) that is used to deny the availability of a resource or to distract you from some other type of attack.

IM ARCHITECTURE

IM applications take one of two forms: They are either client/server-based or communication based via P2P (peer-to-peer). The majority of IM systems on the market today are P2P applications, meaning that no servers are involved—clients communicate directly with one another. Because this architecture eliminates the ability of an administrator to capture the communication, it's non-compliant with a number of new financial and health-care security requirements. IM applications can run without being detected by conventional security devices such as firewalls; thus, security takes a reactive role.

Client/server-based architectures are more conducive to the enterprise-grade IM solution. Control and management, auditing, and policy enforcement are allowed under this model.

The IM applications with the most users, and thus the ones your users are most likely to use, are all client/server-based and work off proprietary networking protocols. Although limited information on each protocol is available on the Internet, the word *proprietary* should scare anyone with a security mind-set. IM client software is frequently updated, but how often do we see changes to the protocols? History has shown that *proprietary* does not in

any way equate to *secure*. Table 1 details the best-known IMs and their specifications.

Earlier this year, AOL released AIM 5.2 build 3139, which offers P2P file transfers and direct IM functionality. Although this made communication much easier for users, it also bypassed perimeter defenses against file sharing.

WHAT ARE THE RISKS?

With the idea of confidentiality, integrity, and availability in mind, let's analyze the security risks presented by IM technology as it exists today.

Consumer versus Corporate. While businesses see the usefulness of IM, most have not implemented enterprise-grade solutions to address this growing business need. Most corporations still rely on consumer-grade "free" IM clients, which lack security, control and management, reporting, or auditing features. This is a bad idea, as consumer IM applications bypass corporate authentication systems, opening other points of entry for malicious code within the enterprise.

Externally Controlled Communication Medium. The most commonly used IM solutions are initiated by end users setting up Internet connections between client software running on their systems and management software running on externally controlled servers. Once that traffic arrives at the management server, it is passed on to a target system located anywhere with Internet connectivity. The questions you should be asking are:

- Who is in control of the IM management servers and should I trust them?
- What type of logging is done of the communication passing through the IM server?
- Are my users likely to communicate confidential information over these servers?
- Who are my users communicating with?
- Is this connection private?

The most obvious risk is that nothing is preventing the owners of the IM servers from logging and reading the transmitted traffic. If your users are transferring files

TABLE 1

IMs and their specifications

IM Client	Protocol	Default Communication Port	Password Encryption?	Message Encryption?
AIM	OSCAR and TOC	5190	Yes	Yes
Yahoo	YMSG	5050	Yes	No
MSN	MSNP	1863	Yes	No
ICQ	OSCAR and TOC	5190	Yes	No

Instant Messaging or Instant Headache?

to each other using IM, then these too can be intercepted. Let's say Bob is talking to Alice and asks her for the admin password to access the Web server. Could Frank, the IM server admin, be eavesdropping on this communication and gain this password information? No matter how much the IM providers assure you this can't happen, you almost have to assume that Frank can do so at any time—and if your users are communicating confidential information to each other over this channel, you are likely to lose data confidentiality at some point.

Not only do you have to worry about the interception of the IM traffic at the servers, but also, as with all Internet connectivity, it is theoretically possible to intercept the IM communication as it is being transmitted on the Internet—for example, by using the classic man-in-the-middle-attack, where the attacker sniffs packets from the network, modifies them, then puts them back on the network to accomplish a TCP hijacking. There are even tools available such as Juggernaut, T-Sight, and Hunt to assist the hacker in this effort.⁵

At this point we would be remiss not to point out that even with the proper tools, this type of attack is most effective with direct access to the network and thus is generally attempted only when the attacker has that level of access. Therefore, Frank could be anyone with sufficient access and knowledge, but Frank is most likely another user on your network. While you should consider this in planning your protection, don't make the mistake of assuming there is no risk, as a majority of successful attacks of any type are initiated from within your network. The interception of Internet traffic does not usually happen, but it is possible and should be taken into account when planning IM security.

Furthermore, it is possible to intercept the IM traffic and replace it with your own, thus affecting the integrity of the communication. Frank might use this technique to hijack an ongoing conversation between Bob and Alice so he can obtain the password from Alice without having to wait for Bob to ask for it. Frank is unlikely to do this, however, as Bob would probably notice this interruption. What is more likely to happen is that using information gained by earlier eavesdropping, Frank would start an IM

session using Bob's credentials to ask Alice for the information directly.

Another risk is that when your users set up and own IM accounts they then use for transacting business, nothing prevents them from continuing to represent your organization even after they have left or are asked to leave your business.

Individual Misrepresentation. With the common IM solutions, once you install the client application, you can add friends to your own network and communicate with them easily. All that is required is for the individuals you wish to add to your network to agree to setting up this connection. Malicious individuals can easily create fake identifications and attempt to set up such a network with your users in order to elicit confidential information by stating they are someone who they are not. You may ask, aren't there safeguards to protect against this? The answer is no. On the commonly used consumer-based IM applications, all it takes to create an IM account is an Internet connection and a little time. There is no requirement to prove you are who you say you are, so with a new IM account and some social engineering, Bob146 (a.k.a. Frank) could convince Alice that he is really Bob126 (a.k.a. Bob). Unless Alice checks with Bob using an offline connection, will she know the difference?

Malicious Code Entry Point. As mentioned before, your users are transferring files using IM. A file incoming to your user could be infected with a computer virus or the file itself could be misrepresented by a malicious individual and actually be a computer worm or Trojan horse. Sometimes this type of malicious code is hidden in files that users will want to share. The risks are obvious; when your user accesses the file, it could begin a malicious code infestation in your environment. There are known computer virus worms that use IM to spread. In some cases the malicious code simply uses the existing IM client software to send confidential data to a specific account or send messages back to the worm creator.

Although antivirus software can detect malicious code within e-mail messages, many do not yet support IM protocols. This gap could result in the loss of confidentiality if this malicious code successfully forwards data to an

externally controlled resource, data integrity if the malicious code were to alter data, data availability if the malicious code were to delete data, or it could result in loss of network availability if the malicious code is a computer worm and in attempting to spread it brings down your e-mail server or part of your network. In general, this ability to transfer files may represent the highest immediate risk to your environment.

IM Worms. Well over 60 vulnerabilities have already been mapped to instant messengers, and the list of worms targeting this propagation method is bound to grow in the coming months. Unlike other high-profile worms, IM worms use a much simpler propagation method: locating potential new targets via the “buddy list,” bypassing the Internet altogether. The progression of technical proficiency with each worm listed here is obvious—and although not listed, antivirus vendors have reported their customers’ experiencing crashing IM clients, DoS attacks, and installation/running of malicious code remotely. Here are a few example IM worms:

- W32.HLLP.VB.14336.C (May 15, 2002): If a Swedish version of Windows and MSN Messenger are installed, this worm attempts to spread itself (in a 28-KB file) along with two text strings each time an IM event takes place.
- W32.AimVen.Worm (March 4, 2003): Uses AIM to spread itself, by modifying the AIM program itself.
- W32.Upering.Worm (July 30, 2003): This mass-mailing worm is a blended threat that spreads by sending itself to e-mail addresses and IM contacts in the AOL address book.
- W32.Simic.Worm (July 30, 2003): This worm spreads itself using MSN Messenger and installs Visual Basic runtime components on the system.

Increased Use of External Internet Connections. You must mitigate the risk of the ever-increasing use of network bandwidth by IM solutions, as IM takes over more and more of the everyday communication of your users. If you don’t put in place the proper controls, this traffic could overwhelm your Internet connectivity, affecting the availability of these resources and the productivity of your users. It will also affect the availability of external resources to your customers and business partners.

Although there are limited figures to support exactly how much bandwidth IM applications take up on a corporate level, it’s a known contributor traveling on already busy ports. Many environments in North America are not affected adversely by the limited bandwidth used by the simple text messaging capability of IM, but in other global markets even this is problematic. Some organizations such as government agencies, retailers, and utilities

are particularly conscious of bandwidth usage and try to limit it as much as possible in all areas of their environment. As IM is used more and more for file sharing and branches out into providing other services (see the section on “Future Risks” later in this article), all administrators will need to consider IM’s use of bandwidth.

Universities have a particularly difficult time with limited bandwidth availability and students performing both academic and nonacademic activities online. Some institutions have found the solution to be in prioritizing traffic, sometimes called traffic shaping. Using prioritization, Web browsing, e-mail, Telnet, SSH (Secure Shell), academic, and network applications are given a high priority. Games and all other application and protocols are next on the priority list, with file-sharing applications given the lowest priority.

Lack of Communication Tracking on the Client. Many network administrators understand that these days if you are not already tracking your user communication, you must start doing so in the near future. This requirement is a result of new regulations such as the Sarbanes-Oxley Act of 2002.⁶ The questions you must ask are:

- What type of logging is done of the communication passing through the IM client?
- If I am not tracking this communication, does this represent a legal liability risk to my organization?
- While it is easy to implement solutions to track communication media that you control, how do you track communication of a resource outside of your control?

If you are not tracking this communication, you run the risk of not knowing when confidentiality has been breached. Akonix⁷ offers an IM compliance application that records conversations, allows for message auditing, and enforces corporate IM policies.

FUTURE RISKS

As with most communication media, we know that IM technology will not stay static. Its capabilities are already expanding and growing. In addition to the half-duplex text-based services we are all familiar with, IM providers are adding full-duplex communication options such as audio and video communication. As the capabilities increase, so do the inherent risks. So let’s look at the future directions IM technology could take and the risks they would represent to information security.

IM Forums. Chat rooms, also known as IM conferencing, provide the ability to join more than one person in a conversation. In the future, individuals will set up continuous chat rooms on a variety of topics, and IM technology will expand to make these “permanent” chat

Instant Messaging or Instant Headache?

environments easier to set up and join dynamically. Eventually, these IM forums will take on many of the features of current topic forums. Your users may find it useful to set up forums on internal topics such as current projects. Without the ability to limit access to these forums or properly validate those wishing to join, however, you risk loss of confidentiality through these channels and loss of information integrity if unauthorized individuals provide inaccurate data to internal processes. As internal processes become dependent on these IM forums, you risk loss of data availability if the forums are hosted on individual workstations.

Instant Audio. Instant audio as a replacement for phone conversations is unlikely to take hold in the business environment anytime soon. That said, the capability is already here and at some point your users may decide to take advantage of it. The risks of this type of technology do not differ much from the risks of phone technology itself—that is, the interception of the audio stream while users are talking about confidential information.

Instant Video. While technically feasible even now, instant video using Web cams has not yet been fully exploited. This is likely to change as more and more users become comfortable with Web-cam technology, as the quality of the imaging increases, and as this technology is integrated into the users' computer systems, whether their desktop or mobile systems. The questions here are:

- Where are your users as they take these instant video calls?
- What can be seen in these video images beyond your users themselves?
- If Bob sends a video message while standing in front of a whiteboard with confidential information, will Alice see this when she answers?

The risks represented by video Web cameras in your environment go beyond that of pure privacy to include the possible loss of confidentiality.

Folder Sharing. Eventually, IM services are bound to implement advanced P2P file sharing similar to the technology used in Kazaa⁸ and Gnutella⁹ today. As more and more people use IM for project collaboration, the advantages of folder sharing will be hard to pass up.

The risks involved in this type of communication are the same as for these other folder-sharing technologies, including the possible loss of data confidentiality and data integrity if the wrong people gain access. As with the IM forums, when projects become dependent on these shared resources hosted on individual workstations, the availability of these resources is at risk.

Meeting Collaboration Tools. Another possible future for IM technology is meeting collaboration tools such as online meeting whiteboards, program sharing, document sharing, and remote desktop sharing. All of these have inherent data confidentiality and integrity security risks.

WHAT CAN YOU DO?

We have covered most of the security risks involved with IM technology. I say *most* because certainly there could be more we are not aware of or that may develop as IM technology expands into areas not discussed. But now that we know at least some of the risks, let's discuss ways of mitigating these risks. Many of the solutions presented here are not specific to securing IM technology. They include administrative, physical, and technical controls, including internally controlled alternatives, encryption and file signatures, antivirus software, port and URL blocking, desktop firewalls, and proxy servers.

Administrative Controls/Policies. Don't underestimate the power of policies in protecting your environment. A good policy foundation goes beyond just making sure that security policies include software security requirements, software usage security processes, and user education. Users not being aware or not caring about the ramifications of using these external services often cause many of the risks. By setting specific policies on using IM technology and making your users aware of the IM security risks, their roles in IM security, and the policies surrounding the use of IM technology, you will have the greatest impact on protecting your network. One important policy requirement should be that your users' IM accounts on externally controlled systems should not indicate their real names (first or last), your company name, company stock symbol, or user location.

Physical Controls. To mitigate the risk of confidentiality

loss from Web cameras, when designing office spaces you should consider placement of whiteboards and bulletin boards so they are not within view of the probable placement of these cameras.

Internally Controlled Alternatives. You need to understand that IM meets a communication need for your users. To regain control of the security of your environment, you can put in place internally controlled alternatives that will meet these needs. Most of the major IM providers and many other software providers offer internal IM server technology so that you can put in place your own IM network. An internal IM network allows you to better regulate adherence to security policies and prevent the transfer of confidential information outside of your network. Although this might not prevent your users from taking advantage of externally controlled alternatives, it will provide them another option when they understand the need for a higher level of security for internal communications. As the capabilities of IM continue to expand, you will need to reevaluate your internal IM solution and provide alternatives that will fill the voids.

Encryption and File Signatures. There are applications on the market that will encrypt communication on the most common IM provider networks. JohnyTech¹⁰ provides such a solution that is as simple as installing its plug-in software on both IM clients and setting a random shared encryption key. The encryption and decryption of the communication is then automated, yet all communication on the wire and passing through the IM servers is encrypted. AOL is testing a built-in encryption capability, and all IM vendors are expected to offer this capability eventually. The encryption of IM communication will greatly mitigate the confidentiality risks posed by using externally controlled commercially available IM solutions.

With consistent usage of encryption by all your users, malicious individuals will find it difficult to hijack ongoing messaging conversations or initiate new conversations, then misrepresent themselves so they can obtain confidential information or introduce false information. Even if you are using an internally controlled IM environment, encryption of IM communication may still be important, especially if it involves high-level executives, the legal department, or human resources, as these groups often deal with highly confidential information that you don't want leaked even internally.

In the future, encryption must also be able to protect instant audio and instant video connections, along with the many other meeting collaboration tools.

In addition to encryption of the communication path, in the future IM clients must be able to sign files that are

transferred between clients to assure that the file received is the same as the file sent. This will guarantee file integrity during transfer. Look for this feature when evaluating internal IM solutions. In lieu of the availability of such a solution, you should instruct your users transferring files via IM to compress them in password-protected files and provide the password to the recipient using another communication method such as the phone.

Corporate versions of consumer IM applications such as Yahoo,¹¹ AIM,¹² or MSN¹²¹³ are being developed to address security concerns of this nature, primarily encryption. With a user base for each of these IM applications in the tens of millions, developers are banking on the enhanced products successfully satisfying corporate requirements such as control and management, compliance, liability, and reporting. This will further expand their user base and eventually generate cash flow. Lack of interoperability between the applications certainly guarantees that each of the consumer-grade IM players will, at a minimum, be addressed in terms of communicating securely with critical business partners.

The current version of AIM (5.2 build 3255)¹⁴ allows for true message privacy by introducing the ability for members to send and receive end-to-end encrypted messages via IM, chat, and file transfers.

Don't underestimate the
power of policies
in protecting your environment.

Antivirus Software. As with all other areas of computer technology these days, it is important to have in place antivirus technology to protect you from malicious code transferred into your environment through IM connections or attempting to spread through your environment using these IM connections. Installing and keeping up-to-date file-scanning antivirus solutions for all workstations and servers in the environment is a minimum requirement. Solutions are available from companies such as Akonix¹⁵ that will scan all your IM traffic during transfer to and from your environment for known malicious code.

Port and URL Blocking. A good short-term solution to the security concerns raised by externally controlled IM services is to block the ports used by these services at your firewalls. In the long run, however, this is not an effective solution, as the IM providers are constantly chang-

Instant Messaging or Instant Headache?

ing how their solutions function so that they cannot be blocked. Many now use standard HTML-type traffic over port 80, thus effectively making it impossible to use port blocking successfully. The next obvious step is to start blocking access to specific URLs using a content filtering solution. Of course, as was experienced with the e-mail services, this is also not an effective long-term solution, as the URLs will start changing. Already, IM clients allow users to select the ports and URLs they wish to use for communication.

Desktop Firewalls. As with port blocking, you can use local firewall software running on your users' systems to limit access to specific ports or URLs. This is a good short-term solution, but will not provide long-term relief.

Proxy Servers. Knowing that the battle to stop access to external IM providers is not winnable in the long run, it becomes more and more apparent that a specialized server is required that understands IM traffic and allows you to scan that traffic for malicious code and content. Such solutions are available from companies such as FaceTime¹⁶ Communications and Akonix.¹⁷ A proxy server that allows you to scan all IM communication for content that violates your organization's or customers' confidentiality and scans all transferred files for malicious code offers the best long-term solution for truly securing your environment from the possible effects of IM traffic. In addition, this type of solution allows for the logging of IM communication.

EMBRACE IM, BUT STAY SECURE

The time has come to embrace IM technology as a standard part of your network environment. As you allow this new type of service in your environment, however, be sure to put in place the proper security controls to ensure that your data stays confidential, keeps its integrity, and is always available when needed. Until fundamental changes are made to the IM protocols, that's the best that we can do. Q

REFERENCES

1. Akonix: see <http://www.akonix.com>.
2. FaceTime Communications: see <http://www.facetime.com>.

www.facetime.com.

3. NetIQ: see <http://www.netiq.com>.
4. Gartner: see http://www4.gartner.com/5_about/press_releases/pr25mar2003a.jsp.
5. For more information on this type of attack, refer to Bhansali, B. B. Man-in-the-middle attack, February 2001; <http://ouah.kernsh.org/mitmbrief.htm>.
6. Sarbanes-Oxley Act of 2002: see <http://www.sarbanes-oxley.com>.
7. See reference 1.
8. Kazaa: see <http://www.kazaa.com/us/>.
9. Gnutella: see <http://www.gnutella.com>.
10. JohnnyTech: see <http://www.johnnytech.com/home.asp>.
11. Yahoo: see <http://messenger.yahoo.com/business/products/msg/>.
12. AIM: see <http://enterprise.netscape.com/products/aimsvcs/>.
13. MSN Messenger: see <http://www.microsoft.com/office/livecomm/prodinfo/msnconnect.mspx>.
14. See reference 12.
15. See reference 1.
16. See reference 2.
17. See reference 1.

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

JOHN STONE is a consulting manager at Symantec, where he has performed targeted security assessments and developed security solution deployment plans for a wide variety of corporate and government organizations. He has cowritten and edited customer training manuals on Symantec technology and used his expertise to assist in editing books provided by the SANS (SysAdmin, Audit, Network, Security) Institute.

SARAH MERRION is a principal security consultant at Symantec with experience in the areas of identifying global security threats, developing security solution deployment plans, and vulnerability testing, as well as hands-on support for antivirus, file encryption, and firewall issues.

© 2004 ACM 1542-7730/04/0400 \$5.00