

# Securing Instant Messaging

Tom Olzak  
January 2006

Instant Messaging (IM) is becoming an attack vector of choice. Bypassing perimeter and email security, it provides a direct path to end-user devices. This path, and the vulnerabilities presented by its existence, is typically provided by the unsupervised public messaging activities of employees.

In this paper, we review the current challenges facing businesses in which employees use public IM services. We also define the possible damage to your business because of IM vulnerabilities as well as the objectives of an effective secure IM strategy. Finally, we look at various ways to meet the goals of that strategy.

## The Challenges

Efforts by security professionals have been very effective over the past few years. The walls that protect network perimeters are higher than ever. Email is filtered, scanned, and stripped of [malware](#) and attachments of known exploitable file types. These developments present the external attacker with greater challenges. Looking for an easier way to get through network defenses, he's beginning to exploit the inherent weaknesses of IM. In fact, recent attack trends indicate that IM is quickly moving to catch up with email as the favorite method of unauthorized access to business networks.

In the first quarter of 2005, there were 59 reported incidents of attacks that used IM. The number increased to 779 in the fourth quarter, with worms and [root kits](#) heading the IM malware list (Espiner, 2006). Continued increases of this magnitude will result in a shift away from hardened email systems and network perimeters to the softer target presented by IM. Figure 1 depicts a simple network with an IM user.

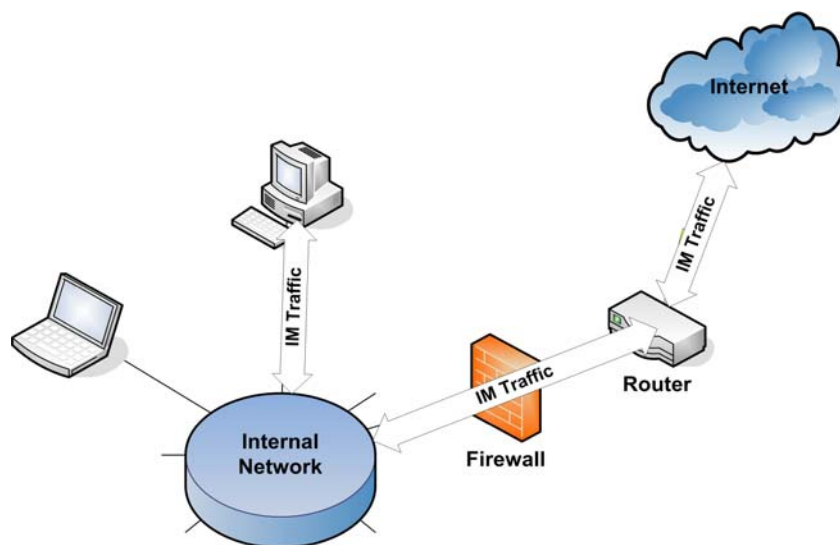


Figure 1: Unprotected IM Use

IM traffic passes unfiltered through the firewall. It can use any unused [port](#) to connect participants. This free flow of IM packets through an organization's firewall is analogous to punching a big hole in the network perimeter; a perimeter often built with significant effort and cost. There are two significant risks with allowing this hole to exist without constraints – malware infections and the compromise of sensitive information.

### *Malware Infections*

Most IM enabled malware attacks spread via user interaction. Some of the ways attackers partner with unsuspecting users include:

**Masquerading** – Posing as a friend of a friend, or as an innocent participant in an online chat, an attacker encourages one or more participants to visit a malicious site, download an infected file, or share sensitive personal or business information.

**File Transfers** – The file an IM user receives might contain a “special gift” that infects one or more enterprise systems.

**Unknowingly Visiting Malicious Sites** – Links made available during chat sessions or recommended by participating attackers can provide an open doorway from a malicious site to your internal network. Through this doorway can pass, unhindered, any type of malicious software that can be automatically delivered from a web site. You never know what you're going to get, but it isn't something you need or want.

**Running Applications during Chat Sessions** – Similar to file transfers and visiting malicious sites, running applications offered by participants in a chat session is a good way to spread [trojans](#), root kits, and other types of malware typically distributed through [executable](#) files.

**IM Client Software Vulnerabilities** – An IM client application, like any other software, contains undetected vulnerabilities. But organizations with no IM policies, standards, or guidelines typically fail to patch IM client security weaknesses. When an IM client exploit is released into the wild, aggressive protective action is absent; the enterprise remains vulnerable to attack.

**SPIM** – SPIM is a new acronym for SPAM for IM, and it's increasing. In a recent Gartner survey, 29% of the respondents said they receive SPIM (Cain, Smith, & Burton, 2005). Like SPAM, SPIM messages can contain malicious code.

Although each of these threats can create havoc in a business environment, they only represent a minority of the probable hits your critical information assets might take in any given year. It's more likely that your intellectual property and efforts at regulatory

compliance will be compromised through the lack of security awareness within your workforce. This is the topic of the next section.

### *Compromise of Sensitive Information*

In an organization without measurable employee security awareness efforts, the employee logged into the network or answering the phone is the weakest component in a company security program. The vulnerabilities introduced into such an organization through the use of public IM services are good examples of how business system users can elevate security risks.

In a Gartner research paper, Mathew Cain, David Smith, and Betsy Burton list the following public IM vulnerabilities associated with personal and organizational information (2005):

**Dissemination of personal or business confidential information** – If the information shared over IM connections is not filtered or audited, there are no limits on the type of unprotected information employees can send out over the Internet, to various entities, during chat sessions.

**Exposure of unencrypted information** – The Internet is a global network over which most businesses share information. Organizations have worked hard over the past several years to ensure the security of sensitive information as it passes over this public network. But employees can bypass existing safeguards in seconds by sending files through unencrypted IM chat sessions. This information might include banking and credit card information.

**Release of network resource access information** – Account IDs, passwords, and information about network infrastructure can be shared without malicious intent. But this information is useful to anyone interested in cracking network security safeguards.

Once this information is sent out over the chat medium, it's potentially stored for months on public or private servers. You've lost control over intellectual property, [protected health information](#) (PHI), financial data, or a variety of other types of sensitive information.

Unmanaged public IM sessions might also present other problems. They can use large amounts of bandwidth. Further, individuals and business entities might pursue claims of libel or harassment because of employee or business partner chat exchanges (Geer, 2004).

Overall, the use of unmanaged public IM elevates security risk in an organization. The following section identifies some ways to deal with this risk while allowing the use of IM where it makes sense.

## The Solution

The first step in dealing with any security issue is the inclusion of the target system, with its unique threat/vulnerability pairs, in the company security program. Building a security program is outside the scope of this paper. But Kurt Garbar describes the steps necessary to build one in “Implementing an Effective IT Security Program,” which can be found in the Reading Room at [www.SANS.org](http://www.SANS.org).

In general, IM can be integrated into a program by developing an acceptable use policy with supporting standards and guidelines. They should include:

1. Who is allowed to use IM
2. Guidelines covering approved and prohibited IM activities
3. Safeguards that must be in place for inspecting chat messages and transferred files

### Who is Allowed to use IM

It's a given that there are many uses for IM within an organization. Employees use it internally to communicate with a geographically distributed workforce. Business-to-business IM provides for quick updates on orders, shipments, or service delivery issues. In essence, anything you can do with email you can usually do faster with IM. But does this mean that everyone in your organization should be given the privilege of using this technology?

Yes, privilege. IM in the workplace is used over a company owned infrastructure while elevating risk to company-owned information assets. It's management's responsibility to manage resource use and to mitigate risk. This is accomplished by identifying the uses of IM that provide business value that exceeds the cost of necessary security safeguards. Once authorized use is identified, only those users who perform related tasks should be allowed access to IM services.

### Guidelines covering approved and prohibited activities

Writing a policy is useless unless [standards](#) and [guidelines](#) for compliance accompany it. Standards and guidelines help employees refrain from activities that might compromise security.

Microsoft provides a list of guidelines that any organization using unmanaged public IM should consider. The following recommendations are derived from that list (Microsoft.com, 2005).

1. Control IM use and provide access based on business need – turn off universal access.
2. Be careful downloading files in IM. Never accept, open, or save any file from any source that hasn't provided adequate identification.
3. Make sure to use an updated copy of IM software. Staying current provides the best defense against security vulnerabilities in various software releases.

4. Create a barrier against unwanted IM traffic by not listing individual contact information in any public Internet directories.
5. Never provide personal or business information over an open chat session. This includes employee information or PHI.
6. Never open pictures, download files, or click links in messages from unknown entities.

Developing these standards of conduct is just the first step. They're useless unless employees are aware of them as well as the impact non-compliance can have on the organization, customers, and them. This is where an active security awareness program adds value. Going beyond new hire orientation and annual refresher sessions for existing employees, an effective awareness program keeps security in the forefront of every daily activity. The use of posters and regular email messages are two ways to maintain awareness. The way in which an organization decides to communicate security to its employees depends in large part on the organization's culture.

Adding IM policies, standards, and guidelines to the company's security program is a good start. But using this approach alone relies on the vigilance of your workforce; the human factor introduces errors into any risk management effort.

## Safeguards

A security safeguard, or countermeasure, is a process or technology that helps protect information assets from compromises to their confidentiality, integrity, and availability. A combination of solutions combined into a layered approach provides the best protection. Figure 2 depicts a layered security model designed to mitigate the risks of public IM use.

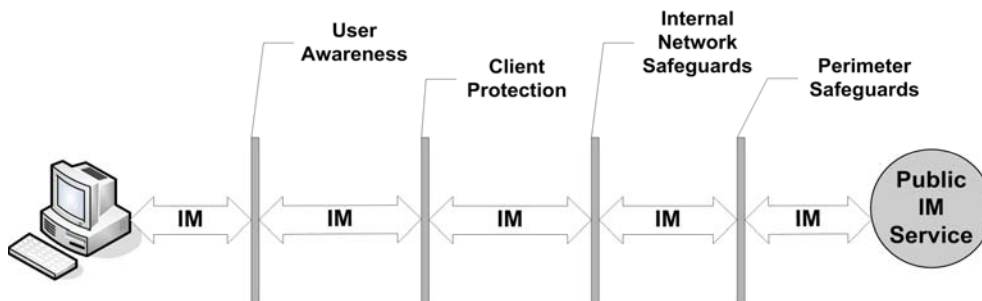


Figure 2: Layered IM Defense

We've already discussed user awareness. Let's take a look at the other layers.

### *Client protection*

Protecting end user devices from IM threats is not easy. In most cases, malware has to work relatively hard to gain a foothold on an employee device. But with IM, employees tend to provide assistance to attacking individuals and software. So how can an organization protect itself from the occasional lapse in judgment?

The most common method, and one that every organization connected to the Internet should have in place, is the deployment of anti-virus software. Up to date anti-

virus software is one of the best ways to prevent end user device infection. But it isn't enough.

In today's Internet environment, attackers have gone beyond using the venerable virus, worm, or trojan. Insidious malware in forms such as root kits and cookies can often be missed by traditional anti-virus applications. Anti-spyware software fills this gap. The combination of anti-virus and anti-spyware solutions can help protect end user devices from most if not all *known* threats and vulnerabilities. Unknown threats and vulnerabilities require a different kind of protection.

Host-based Intrusion Prevention Systems ([HIPS](#)) or Host-based Intrusion Detection Systems ([HIDS](#)) provide protection against attacks when the threat or the vulnerability is unknown to anti-virus application vendors. HIPS and HIDS detect anomalous behavior on end user devices. They can either block (HIPS) the activity or alert system administrators (HIPS and HIDS).

Another application organizations might consider is the [personal firewall](#). Many companies may have reservations about deploying HIDS and HIPS technology; both are still emerging relative to effectiveness and standards of use. Personal firewalls on the other hand represent a mature technology that operates in much the same way as HIDS and HIPS. Most anti-virus applications are available with a personal firewall option. Microsoft offers a free desktop firewall solution for users of current Windows operating systems.

Finally, organizations should develop an active patch management program. Applying security patches as vendors release them is the best way to prevent attacks against known desktop vulnerabilities.

### *Network safeguards*

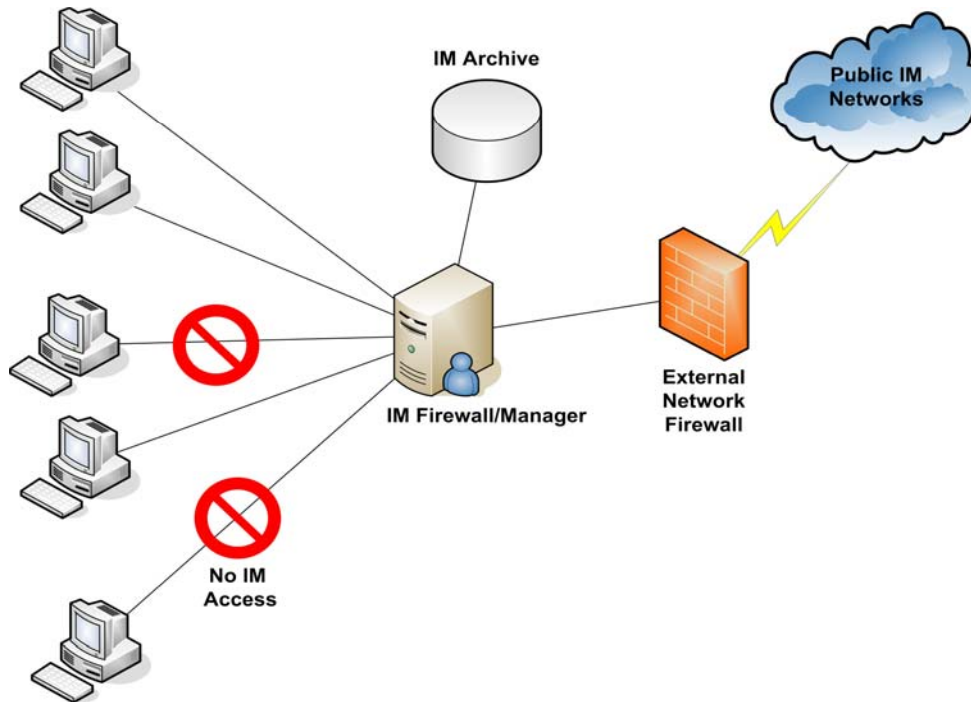
The next layer of defense is the internal network. Network-based Intrusion Prevention Systems (NIPS) and Intrusion Detection Systems (NIDS) serve a similar purpose on the network as HIPS and HIDS do on desktops. The primary difference is placement. Network-based solutions can protect large numbers of systems with a single device. This is accomplished by placing a NIDS or NIPS monitor or appliance at interfaces between the outside world and the internal network. Placement at gateways to critical [network segments](#) is also a good second layer network defense.

### *Perimeter safeguards*

There are several methods used to protect networks from external attacks. The most common device used for this purpose is the perimeter [firewall](#). Firewalls can block unwanted traffic before it has a chance to enter the company network. Organizations should review and harden current firewall rules. External penetration tests by a qualified security engineer are a good way to test the effectiveness of firewall configurations. But when used to protect against public IM threats, firewall effectiveness diminishes.

There are two approaches to combating IM threats – IM firewalls and internal IM services. IM firewalls sit behind the traditional perimeter firewall that separates your network from the outside world. Figure 3 shows an example. Both outbound and inbound IM [packets](#) are examined. Depending on the IM firewall's capabilities, you may configure the following:

1. Real-time threat protection, using both [anomaly](#) and [signature](#) analysis. This enables an organization to:
  - a. Identify and remove malware attempting to enter the internal network.



**Figure 3: IM Firewall Placement**

- b. Enforce policy compliance through traffic analysis and reporting, message keyword searches, and message archiving.
2. Deploy and manage a single client.
3. Implement reflection technology. This ensures that IM traffic between two internal entities never travels across the Internet, even if the sender and the recipient are using a public IM service.
4. Link blocking. Employees are blocked from visiting known problem sites when clicking on links provided during chat sessions.

Some IM firewall solutions provide for identity and authentication management. As shown in Figure 3, a network administrator can use this feature to block specific users or specific groups of users from accessing IM services. However, Enterprise Instant Messaging (EIM) is probably a better choice when granular identity and authentication services are required. For example, EIM can integrate access control into an operating system authentication mechanism like Active Directory.

An EIM solution is often combined with IM firewall technologies to provide the highest levels of control and protection. Figure 4 shows an example of this kind of configuration.

In addition to the features available in the IM firewall, EIM provides the following (Geer, 2004):

1. Tight integration with security services, such as Active Directory.

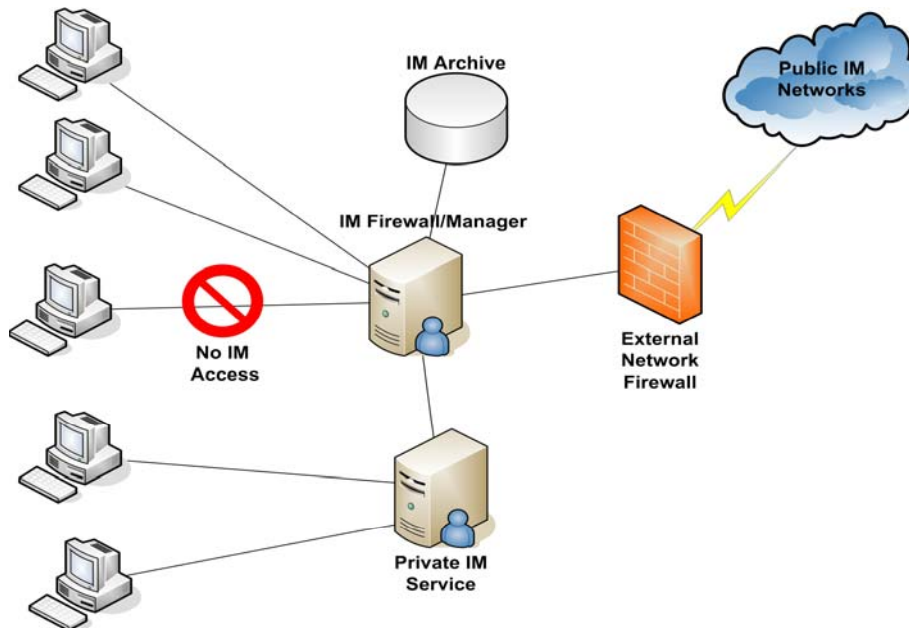


Figure 4: EIM

2. More granularity of control over IM use, including traffic types and content, authorized users, and user authentication.
3. The ability to designate a single port for IM traffic passing through your perimeter firewall. This is typically enabled through the use of either [SSL](#) or [TLS](#) connectivity.
4. Using third party [Certificate Authorities](#), certificate-based authentication is possible. This often eliminates the need for passing user IDs and passwords over the Internet.
5. Control over which employees from your organization, and from partner organizations, are allowed to communicate via IM. This is accomplished through account privilege and lifetime management.
6. For organizations that have not identified a business reason to allow IM communication with outside entities, internal IM is possible without any contact with public IM services.

Regardless of the configuration you choose, ensure your IM management device acts as a gateway between the public and private IM capabilities in your organization (Cain and Smith, 2005). Deployment methods to reach this goal include:

1. Segmenting IM so that internal IM stays internal and external IM is tightly controlled.
2. Forcing IM users to authenticate with an ID that also links them to network security. This facilitates access, accounting, and compliance management.
3. Integration of malware protection and content filtering.

## Conclusion

Instant messaging is quickly evolving into a communication medium of choice for many employees. Managers and business owners who choose to ignore this trend expose their day to day operations to various types of potentially crippling threats. Dissemination of sensitive business or personal information, exposure of unencrypted data, and the release of network resource access information can all be addressed by implementing administrative and technical controls.

In the administrative category, IM management and control must be added to an organization's security program. Documented policies, procedures, standards, and guidelines help employees do the right things to protect information assets. Technical controls support administrative controls by providing real time protection through the use of desktop, network, and malicious traffic blocking.

No matter what approach an organization takes to manage IM, the bottom line is, "do something." Segregate public IM traffic from the internal network, allowing only filtered, safe messages to pass. Don't allow IM to circumvent well designed network security.

## Works Cited

- Cain, M.W. & Smith, D.M. (2005, October). *Management update: create an instant messaging hygiene system*, Gartner research article G00132929. Retrieved January 5, 2006 from <http://www.Gartner.com>
- Cain, M.W., Smith, D. M., & Burton, B. (2005, October). *Management update: beware the inherent risks of public IM*, Gartner research article G00132928. Retrieved January 5, 2006 from <http://www.Gartner.com>
- Espiner, T. (2006, January 10). Study: instant messaging attacks rose in 2005. *News.com*. Retrieved January 12, 2006 from [http://news.com.com/Study+Instant-messaging+attacks+rose+in+2005/2100-7349\\_3-6025226.html](http://news.com.com/Study+Instant-messaging+attacks+rose+in+2005/2100-7349_3-6025226.html)
- Geer, D. (2004, November). Securing IM. *Technical Support*. Retrieved January 12, 2006 from <http://www.naspa.com/PDF/2004/1104/T0411008.pdf>
- Microsoft.com (2005, November). *10 tips for safer instant messaging*. Retrieved January 11, 2006 from <http://www.microsoft.com/athome/security/online/imsafety.mspx>