

Ipswitch Instant Messaging



Instant Messaging as a Business Tool

Abstract

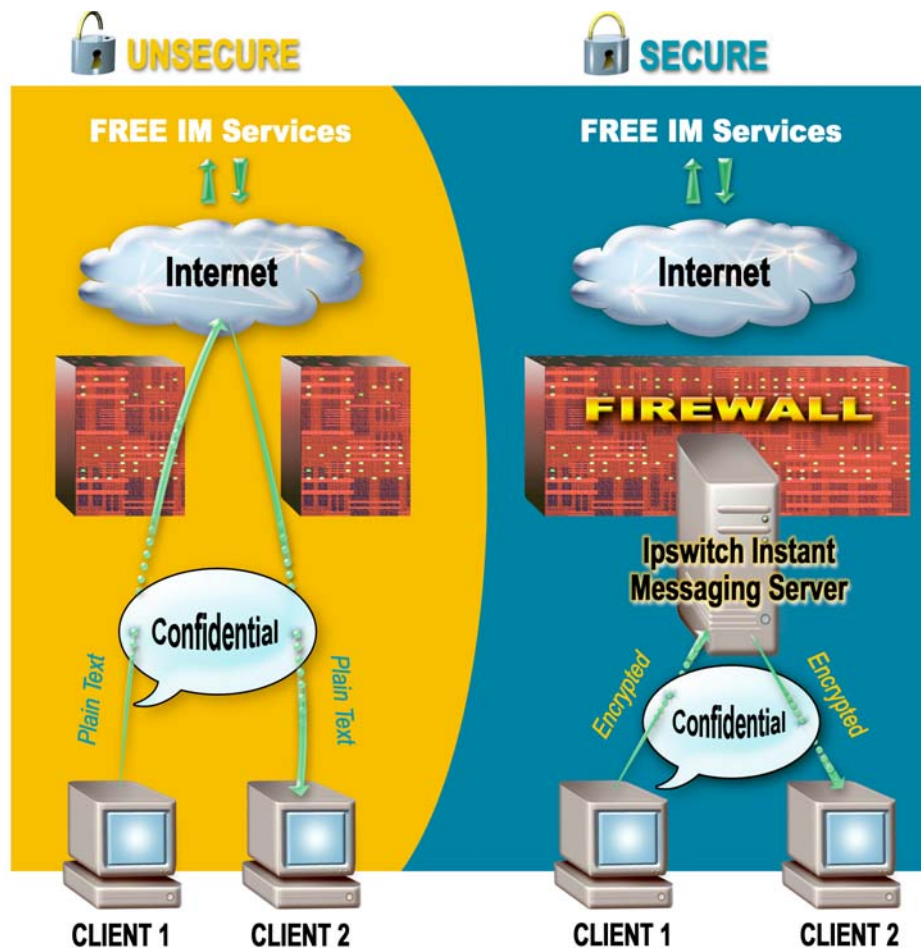
Instant Messaging in the enterprise improves communication and collaboration, but at what risk? While many companies and business users have recognized the benefits of Instant Messaging (IM), not all are aware of its potential shortcomings. For business use, consumer IM services provide too much information where they should not – because the communication through these systems is not secure. At the same time, they provide not enough information where they should – because communications are not logged, and users can never be sure of who they are communicating with. Enterprise Instant Messaging, or EIM, eliminates these drawbacks, and makes Instant Messaging a viable, and valuable, business tool. Many organizations are already using EIM very effectively for a wide range of common business uses, including customer service, technical support, and product development. Others are finding that EIM provides them with a competitive advantage as they use EIM to address the specialized requirements of industries such as healthcare, financial services, government, education, and legal services.

IPSWITCH™

Instant Messaging - The Good And The Bad

Consumer Instant Messaging (IM), started in 1996 as a new way for Internet users to communicate with each other in real-time, has found its way into the workplace. The advantages of using Instant Messaging are apparent. IM combines the convenience of email and the immediate response of phone conversations. Features such as the ability to share files instantly and presence/absence indicators led many business users to introduce IM tools into the workplace themselves, without waiting for management to mandate it – a further testament to IM's utility in the business environment.

Despite its benefits, business decision-makers have been reluctant to encourage employees to use Instant Messaging. From a business standpoint, there is good reason to consider the use of IM carefully, and businesses are right to be reticent about using consumer IM solutions, such as AOL® Instant Messenger™, Microsoft's MSN® Messenger, and Yahoo!® Messenger.



One major drawback of Instant Messaging is that it is insecure. Even communications between two employees in the same building travels out of the company through the IM provider via the Internet before returning to the company's network. And, because they are unencrypted, any and all communications are susceptible to being intercepted and read by third parties. Some consumer IM applications allow direct peer-to-peer contact, which may be acceptable for intra-company use, but opens an unmonitored channel and potential security hole when

used to communicate with users outside the business. In addition, anyone can create an account for free from consumer IM service providers and there is no identity verification. Since there is no guarantee that business users are communicating with who they think they are, the business is at risk of sending confidential information to malicious users posing as legitimate contacts. Even the simple presence indicator, which seems innocuous, can have security ramifications. For example, a hacker planning to attack a business network could be aided by the knowledge that staff in the IT department has just left for lunch.

Aside from the security concerns, many businesses are legally required to log and archive all electronic communications. In the U.S., the Securities and Exchange Commission (SEC) requires all electronic communication to be logged and archived. In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) requires that all access to patient information be secured and logged – making consumer IM unacceptable on both counts. In many cases, corporate policy demands that all business communications must be monitored to ensure sensitive data is not leaving the company, and to ensure that Instant Messaging is not being overused for personal purposes, wasting company time and resources.

In addition, there is no way for a business to ensure the reliability and uptime of a consumer IM service. Businesses do not manage the IM service, nor are they customers of the service and are not entitled to any service level agreement. As a result, business users exert no control over a consumer IM service's reliability or availability. If an IM service begins to experience outages or other problems, organizations that have come to rely on IM heavily have no recourse.

To regain some measure of control over IM in the workplace, some organizations have installed gateway products that log IM communication as it passes through the company firewall. While this approach addresses one drawback of consumer IM solutions, gateway products still rely on the infrastructure of the consumer IM service. As such they do not verify a user's identity, nor do they provide corporate service level agreements on reliability and uptime. More importantly, all communication outside the firewall remains unencrypted and unsecured.

Enterprise Instant Messaging Makes IM Workable

To capitalize on improved efficiency and other benefits of IM in the workplace, while avoiding the negative aspects of free consumer IM services, many organizations are using Enterprise Instant Messaging (EIM). EIM restores control to the organization, because the IM clients *and the server* are managed entirely by the business. This architecture enables EIM to address all of the weaknesses that render consumer IM unsuitable as a business tool.

The entire IM system can be run behind the firewall, and intra-office communications never leave the office. In addition, all communication is encrypted -- including login, presence indications, messages, and file attachments. This encryption allows users to communicate securely within the organization and with field offices and remote users. Overseas offices can communicate at a tiny fraction of the cost of telephone calls; and their conversations are kept private, even if the offices do not share a VPN (virtual private network).

Security is further enhanced because the creation of user accounts and server trust relationships with outside offices are managed by the organization itself. Users can be confident of who they are communicating with at all times, because each user must login in using an account established by the business. And, because the organization decides what outside servers to trust, communications are limited to only people approved by the business.

EIM addresses the security issues inherent in consumer instant messaging systems, specifically:

- **Stalking -- using presence information to infer the location of a user, especially for malicious or illegal purposes**
- **Spoofing -- a user impersonating another user**
- **Spam – unwanted instant messages.***

*** These “three S’s” are defined in RFC 2778, A Model for Presence and Instant Messaging. (<http://www.ietf.org/rfc/rfc2778.txt>)**

Further, with EIM, all messages pass through the company-managed server where they can be logged, archived, and if desired, monitored. The ability to encrypt, authenticate, monitor and archive communications effectively transforms Instant Messaging into a viable and efficient business tool.

How Enterprise Instant Messaging Is Used Today

Businesses of all sizes and in many disparate industries have found a wide range of applications for EIM across their organizations.

General Business Use

Many communications that were previously unadvisable with consumer IM services – such as those shown in figure 1 – are perfectly safe with the added security that EIM provides. For example:

- Human Resources – information about salaries, benefits, and health information can be securely exchanged.
- Customer Service – private customer data, including credit card information, remains private.
- Technical Support – support representatives can instantly contact other representatives to get answers to questions, without having to place the customer on hold.
- Call Center – managers can instantly disseminate vital information, such as system status, to the entire call center staff. In addition, presence indicators provide managers with a high level view of who is on duty at any time.
- Product Development – proprietary development information, such as specifications, models, designs, code and blueprints, can be shared quickly and safely.
- Remote Users – delivery personnel and work-from-home employees have a continuous and convenient communications channel with the home office that automatically registers their presence at their computer.
- Meetings – groups of users in geographically distributed locations use EIM to collaborate and share relevant files in real-time, without travel, conference calls, or reserving conference rooms. In addition, during conference calls between organizations, EIM can be used within an organization to communicate “in the background”, allowing call participants to message privately without placing the other party on hold, or muting the call. The written-word nature of EIM meetings also helps improve communication between groups using multiple dialects and languages.

HR1: you know we are not doing across-the-board salary increases but we need to give Bill a raise.
HR2: ok, how much?
HR1: increase by \$5,000 ☺

PM: do you have the release info for "Sierra"?
PMM: we release in 60 days, two weeks before our competition
PM: have we spoken to any customers
PMM: only under NDA

Gov1: the pres is coming in at 2 pm. Are you ready in Boston?
Gov2: yes, we have people stationed at the airport. Along the route to the Ritz we have 10 agents and another 20 at the hotel.
Gov1: 10-4

Dr. No: do you have John Doe's test results?
Nurse: they came in a minute ago.
Dr. No: Anything odd?
Nurse: he tested negative for diabetes. Here's his file (paper clip emoticon)
JohnDoeHistory

JSmith: Have bids been recd for project 3762813?

Figure 1: Without EIM security, exchanges such as these pose serious risks

Healthcare

In the healthcare industry, HIPAA requires all patient information to be secure, and access to patient information must be controlled and logged. An effective EIM solution will comply with HIPAA regulations and allow healthcare professionals to transmit patient information in an encrypted form. Also, because EIM users are authenticated and conversations are logged, organizations can enforce accountability and monitor communications relating to patient data.

Finance

Like healthcare providers, business in the financial services industry must comply with regulations from governing bodies. Both the Securities and Exchange Commission (SEC) and National Association of Securities Dealers, Inc. (NASD®) require that all electronic communications be archived. Member organizations must ensure that the software they use for electronic communication enables them to make and keep records, as required by SEC Rules 17a-3, 17a-4, and NASD Rules 3010 and 3110. In addition, EIM security features help finance companies keep consumer information private and maintain control over corporate financial data.

Law

Law offices are particularly aware of the risks of unsecured communication channels. EIM ensures that conversations concerning clients are confidential, while guaranteeing that everyone involved in the conversation is authenticated. EIM also helps law offices quickly locate available resources such as secretaries, paralegals and lawyers.

Education

EIM provides educators with a number of advantages over consumer IM. First, EIM insulates children from outside contact by creating a controlled environment in which only trusted individuals are allowed to

communicate. EIM also facilitates distance learning, allowing teachers to conduct classes, share files, and answer questions in real-time across long distances.

Government

Security has become a top priority at all levels of government. As a result, consumer IM services are no longer feasible for most government applications. However, with communications encrypted and authenticated, government agencies are safely using Enterprise Instant Messaging for a wide range of situations. Disaster management teams use EIM to complement phone calls, which can be disrupted in emergencies. Police departments and other government entities also use EIM to communicate securely with officers and other employees in the field.

Ipswitch Instant Messaging

For many organizations, the disadvantages of consumer IM services all but offset the potential benefits of using IM in the work environment. EIM eliminates the drawbacks, but maintains all of the business benefits that IM provides. In almost any business context, cost is a factor, particularly when moving from a free service. Companies switching from consumer IM to EIM must consider near term and long term costs. Ipswitch Instant Messaging is an affordable solution that provides all of the benefits of EIM, including HIPAA-compliant security and SEC-compliant logging. In addition, because it is designed to be easy to install, configure, and maintain, Ipswitch Instant Messaging minimizes maintenance costs. For more information on Ipswitch Instant Messaging, visit : <http://visit.ipswitch.com/info-im>.

About Ipswitch:

Founded in 1991, Ipswitch, Inc. develops easy-to-use, affordable, software products that extend mission-critical IT resources for businesses and improve efficiency for consumers.

Its product family includes WS_FTP Pro, the world's most popular FTP client; WS_FTP Server with 128-bit SSL encryption, the first industrial-strength, full-featured FTP server for Windows NT/2000/XP; WhatsUp Gold, a leading network mapping, monitoring, notification and reporting tool; IMail Server, a leading Internet messaging server with 53 million users; IMail Anti-Virus, an add-on product powered by Symantec's CarrierScan™ and fully integrated with IMail Server; and Ipswitch Instant Messaging, a secure Instant Messaging solution specifically designed for businesses.