

www.securecomputing.com

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers created trusted environments inside and outside their organizations.

Secure Computing IronIM
Secure Instant Messaging Gateway

Table of Contents

Abstract 2

Introduction 2

The Appeal of IM 2

 Real-Time Availability and Presence 2

Adoption of IM into the Enterprise 2

The Potential of IM in Business 3

IM Risks and Challenges 3

 Uncontrolled Use 3

 Heterogeneous IM Environments 4

 Security Vulnerabilities 4

 Backdoor for Viruses, Worms, and Spam 4

 Real-Time Volume 4

Best Practices for Managing IM Security 4

Secure Computing IronIM: Real Security for Instant Messaging 5

 Policy 5

 Monitoring and Enforcement 5

 Management 6

 Archiving 6

Conclusion 6

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

Berkshire, UK
Tel +44.0.870.460.4766

Asia/Pac Headquarters

Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel +81.3.5339.6310

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

© 2007 Secure Computing Corporation. All Rights Reserved. IronIM-WP-Apr07vF. Secure Computing, SafeWord, Sidewinder, SmartFilter, Type Enforcement, Cipher Trust, IronMail, IronIM, SoftToken, Enterprise Strong, MobilePass, PremierAccess, SecureSupport, SecureOS, Best, Cyberguard, SnapGear, Total Stream Protection, Webwasher, Strikeback, and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. Q2 Enterprise Manager, SmartReporter, SecurityReporter, Application Defenses, Central Management Control, RemoteAccess, SecureWire, TrustedSource, On-Box, Securing connections between people, applications and networks, and Access Begins with Identity are trademarks of Secure Computing Corporation.

Abstract

The real-time, interactive nature of Instant Messaging (IM) makes it a valuable tool for collaborative efforts with business partners, customers, and fellow employees. This paper discusses the opportunities created by the use of Instant Messaging, risks to businesses using instant messaging, and how Secure Computing IronIM® is designed to mitigate those risks.

Introduction

The use of Instant Messaging (IM) within businesses has seen exponential growth in the past several years. However, due to the consumer-oriented beginnings of the technology, IM has developed without the typical enterprise emphasis on manageability, reliability, and security. Conversely, early adoption by consumers has meant that the technology is easily deployed, installed, and utilized, benefits equally valuable for the business user. A major result of this ease of deployment is that IM has spread within the enterprise largely outside the control of corporate IT organizations.

The Appeal of IM

Instant messaging allows users to communicate in a manner similar to face-to-face interaction, in that it allows a real-time conversation to take place without the inherent delay of email.

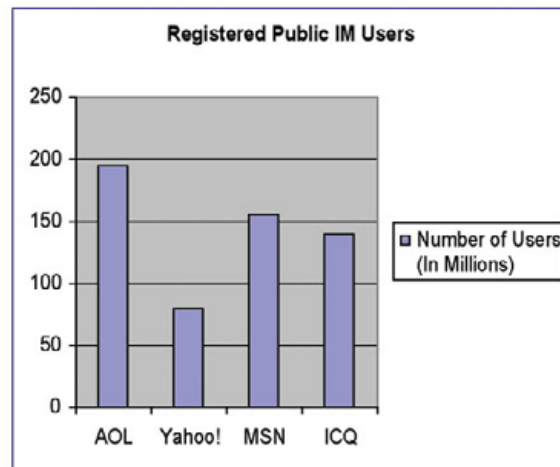


Figure 1: User bases for the four leading instant messaging providers (self-reported)

Real-Time Availability and Presence

Unlike the delayed, asynchronous nature of email, most IM clients display the current online status, or presence, of the intended recipient and allow instantaneous response. With email, the sender initiates an exchange without an expectation of an immediate response, and with the potential that the recipient will not respond with the complete information desired. Especially frustrating is when these exchanges are drawn out waiting for a clarifying tidbit of information, or delayed waiting for the user to return to their desk, read their email, and respond. An overall exchange that might only take 30 seconds of devoted effort might stretch over hours, or even days, because of this non-immediate feedback.

Presence awareness changes the dynamic of electronic communications with the expectation of an immediate response even before initiating the exchange. Because of this dynamic, the potential value of the exchange goes up for both the sender and receiver. Combined with the real-time, synchronous nature of IM, this value is realized by the facilitation of an interactive conversation.

Adoption of IM into the Enterprise

One of the interesting aspects of IM adoption is that it seems to be primarily a grassroots initiative driven by end users outside the purview of corporate IT departments. Some data points that highlight this are:

- Giga Information Group reports that 60% of mid-to-large enterprises have some level of IM being used for business purposes (installation percentage rises to roughly 85% if personal use is factored in) and yet 90% of these organizations (using IM) have no formal IT support and less than 10% of these organizations have implemented secure, enterprise instant messaging.
- The Osterman Research survey on IM identifies that only 29% of companies believe they are currently using IM for business, although numbers from IDC indicate that 70% of companies have workers using IM for business-related activities and 35% of users of public instant messaging services are business customers.

These statistics indicate that IM has already penetrated the enterprise, regardless of whether it is sanctioned or not, and more importantly, many organizations are unaware of this adoption.

The Potential of IM in Businesses

Currently, the four leading public IM providers claim a total of 569 million registered accounts¹, with roughly 229 million using IM for business purposes. A report published by INT Media Research states that of corporations using IM:

- 81% said their employees are more productive
- 19% said that file sharing had increased
- Email traffic was down by 30-40%
- Voice mail was down 10%

In the short term, instant messaging will continue to gain traction in the workplace as the technology becomes more and more ingrained in our daily communication. Long-term, the potential of IM lies in the underlying technology and presence awareness to be extended to devices such as PDAs, cell phones, and Blackberry-type devices, with capabilities moving well beyond text-only conversations into voice and video.

IM Risks and Challenges

Instant messaging presents enterprises with a completely new set of threats to network security, bandwidth availability, and program compatibility. Whether due to the always-on nature of IM, lack of monitoring tools, known vulnerabilities, or multiple protocols used by different vendors, businesses looking to incorporate IM into their communication strategies must address these issues logically and with an eye on maximizing security without sacrificing any of the technology's benefits.

Uncontrolled Use

Because of the ability of many IM products to tunnel through port 80 (the standard Internet port) on firewalls, blocking IM use in the enterprise can be very difficult. Similarly, the ease with which IM client products can be downloaded and installed makes preventing the spread of IM problematic as well.

Even if IM use is allowed by the company, without effective monitoring it is nearly impossible to determine the effect it has on network and computing resources, how much time is being spent on IM, and whether IM use is primarily used for business or personal discussions. In many ways, IM adds the challenge of Web browsing management to the established challenges of messaging management.

¹ http://en.wikipedia.org/wiki/Instant_messaging

“Since the data that is being transmitted over the instant messaging network is not encrypted, a network sniffer can be used to capture the instant messaging traffic. This is particularly dangerous in the corporate environment, in which proprietary or other confidential information may be transmitted along the instant messaging network.”

—Security Focus

Heterogeneous IM Environments

Unlike email with its established protocols of SMTP and POP, or HTTP for the Web, IM today is based on many different proprietary protocols. Although SIP and to some extent, SIMPLE, are emerging standards for IM, none of the public IM services has indicated a desire to migrate away from their proprietary protocols. To the contrary, these vendors view their own protocols as a key barrier to preventing their users to switching to competing services, and are currently engaged in an all-out effort to expand their user communities while maintaining/expanding their brand presence with their clients on the desktop.

Security Vulnerabilities

Many professionals have adopted IM as a primary tool for communicating with both clients and colleagues. However, widespread use of IM has created legitimate security concerns. Quite often, support staff and geographically distributed product development teams use public IM services to discuss their projects and communicate with clients, sending sensitive information over public networks. Messages on these services are transmitted through, and stored on, public servers; therefore, the opportunity exists for external parties to access this sensitive information. This issue of vulnerability of sensitive information is true for all companies using Public IM.

While there are secure IM clients on the market, trying to enforce security at the client level runs contrary to the existing trends of providing encryption at the edge of the enterprise. The perimeter approach to encryption allows archiving, server-based content checking and anti-viral products to be effective; otherwise these capabilities also need to be implemented at the desktop in order to check IM content both before it is encrypted and after it is decrypted. Traditional encryption techniques require end-user action in order to be effective; placing this reliance on the user is asking for trouble.

Backdoor for Viruses, Worms, and Spam

Unfortunately, the existing infrastructure for dealing with viruses, worms, and spam is primarily oriented towards protecting email, file transfer, and Web access. Due to the proprietary protocols used by many IM services, these services' ability to switch IP ports (or even tunnel through port 80), and heavily consumer orientation of these services, IM is an emerging and growing mechanism for the spread of viruses, worms, and spam within the enterprise.

Real-Time Volume

Due to the real-time nature of IM, it is difficult to apply the anti-spam, anti-viral, and content checking filters. With asynchronous email, it is possible to do processing on the email server, and any introduced latency is unlikely to be noticed by the users. For IM conversations to maintain their flow, any management and monitoring products must be able to work at near line speeds and introduce minimal latency. In addition to the latency issue, the nature of IM is such that there will be high volumes of many small messages that will surge as users engage in conversations.

Best Practices for Managing IM Security

1. All commonly utilized IM services should be supported by any tool chosen for IM security. These are public IM services such as AIM, Yahoo! Messenger, Google Talk and MSN Messenger, and Corporate IM services Microsoft LCS and IBM SameTime.
2. Corporate policies regarding the use of IM must be set, and appropriate consequences determined for violations.
3. All IM traffic entering and leaving the business should be monitored to ensure policy compliance.
4. Enforcement of policies against non-compliant messages must be automated with full accounting of enforcement actions available to authorized personnel.
5. The IM system should be kept secure from exploitation by viruses and hackers.

Secure Computing IronIM: Real Security for Instant Messaging

Secure Computing IronIM is a hardened appliance that can be located in the DMZ to protect businesses from the usage risks associated with instant messaging. For the first time businesses can be fully in control of their IM environments. The firewall is set up to allow IM traffic to enter and leave the business only through the Secure Computing IronIM appliance, and DNS entries for all IM services are redirected to the appliance. This gives businesses management capabilities over instant messaging that, until now, were not available.

Policy

Corporate messaging policies should be enforced on all instant messages to ensure compliance with any government privacy and accounting regulations, and to ensure the protection of confidential and sensitive corporate intellectual property. Secure Computing IronIM provides a simple-to-use GUI interface to set policies at a company-wide or LDAP group level. Access to public IM systems can easily be permitted or restricted on a user, group, or system-wide level, with administrators given the option of determining which protocols are to be allowed. Restrictions can mean blocking the entire public IM system to all users so when a user tries to send a message using a public IM service, their message will not be allowed through the corporate firewall—even if the recipient is within the same company. Secure Computing IronIM allows administrators to specify which users should or should not be granted access to public IM systems, and which IM protocols should be allowed or blocked.

Compliance enforcement is managed in two ways. First, regular expression patterns and keyword dictionaries can be defined for the content filtering engine to utilize, and secondly, file transfers through IM can be allowed or blocked. Thus, IM content is thoroughly scrutinized for compliance prior to being allowed out of the enterprise.

While content filtering is critical to IM security, encrypting the content in transit is equally important. When Secure Computing IronIM encryption is enabled, all messages sent between users residing behind Secure Computing IronIM appliances, regardless of whether they are in the same company or not, will be encrypted, rendering those messages safe from the prying eyes of network sniffers and other nefarious tools. End users need not be concerned with loading a new IM client, managing encryption keys, or any of the other difficulties typically associated with encryption. Secure Computing IronIM will do all the work, making the use of encryption transparent to the users. Additionally, there is no performance degradation or other impact on the use of instant messaging.

Monitoring and Enforcement

Secure Computing IronIM is designed to put administrators in control of the use of instant messaging. All IM conversations—inbound and outbound—are logged. Off-the-shelf instant messaging products require end-user action to save messages if the end user thinks the conversation was important enough to keep. Secure Computing IronIM simply saves all conversations in an “IMBox” that each end user can access at any time to retrieve and review their conversations offline. Users have the flexibility to search by name, date ranges, and keywords for prior conversations. Administrators and compliance or security personnel can be granted access to all “IMBoxes” as needed.

All IM conversations are monitored for violations based on policies. Multiple enforcement actions can be taken when violations are found:

- The message can be flagged and the violation logged for reporting purposes. The message will still be sent, but a specific record is kept of that message.
- The user can be sent a warning via his/her IM client in real-time. Again, the message will be sent.
- Secure Computing IronIM can drop a message and inform the sender of the violation.
- The session can be instantly terminated.

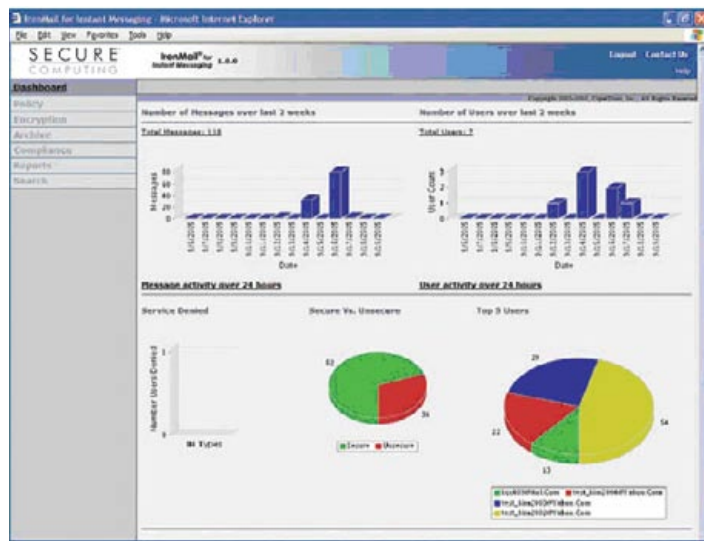


Figure 2: The IronIM dashboard presents a full view of instant messaging activity and usage at-a-glance.

Management

Secure Computing IronIM is easily managed through a simple at-a-glance dashboard. A full view of IM activity and usage is provided on the first screen, and message activity and user activity is tracked and presented in graphical format for easy reference. Complementing the graphical dashboard is a full set of reports that drills down into the numerous areas of instant messaging that security administrators and compliance or security officers are concerned about.

Ongoing management of policies and the dictionaries used is made easy through the intuitive point-and-click interface.

Archiving

IronIM monitors and logs all instant messaging traffic. While other IM security solutions simply record that a conversation has taken place, IronIM captures and stores the entire conversation and allows administrators to search historical conversations using keywords. IronIM also allows administrators to set granular archiving policies based on any number of enterprise-specific requirements.

Conclusion

Instant messaging is an increasingly accepted mechanism for providing real-time collaboration, and provides capabilities beyond that of email, which it complements. Its ability to provide presence awareness of connected users will eventually be expanded into other applications, which will further expand the utilization of IM technologies. The opportunities for leveraging IM for business include:

- Easily and quickly communicating in real-time with external and internal users.
- Improving productivity by enabling teams of remote users.
- Reducing phone, email, and other communication costs.

In many ways, the state of the IM use today is analogous to the state of email usage 10-12 years ago, and reflects the state of supporting email infrastructure which lacked mature management, monitoring, archiving, and policy tools. Organizations seeking to leverage IM for business can address uncontrolled use, security/privacy, and infrastructure protection issues by using Secure Computing IronIM while ensuring that there is no degradation of the unique real-time conversation and collaborative capabilities that have helped make it such a popular communication technology.