Security in Instant Messaging

Securing the Desktop with StormWatch™ Intrusion Prevention

ABSTRACT

Instant Messaging (IM) technology, as advanced by several vendors such as Microsoft and AOL Time Warner, permits the use of real-time communication between participating users. The Instant Messaging environment can be used for text-based messaging, and also permits other communications mechanisms such as immediate file transfers, voice, and email. Corporations that enforce security within their networks are faced with a potential evasion of their corporate security policies through IM protocols and attacks against insecure IM clients. Companies do not currently have the ability to control – with a level of granularity they require – which aspects of the IM environment they wish to permit through their firewalls and other security mechanisms except on a gross "allow all/deny all" level.

OKENA StormWatch™ gives companies the ability to control, with a high level of specificity, which aspects of the IM application are used within their organizations. Utilizing StormWatch, corporations can allow text messaging, for example, but explicitly forbid the transfer of files through the IM system, while continuing to allow file transfers via other mechanisms such as browser or ftp. StormWatch also protects vulnerable IM clients from remote attack by malicious outsiders or computer viruses. IM policies contained within StormWatch restrict the IM system from changing key system files or registry values, and let the user decide if they wish to permit file transfers through the IM system, permit email, and/or voice. Using StormWatch, companies can easily tailor the IM policy to match their specific security policy requirements.

Instant Messaging in a Business Context

Increasing numbers of organizations are deploying Instant Messenging applications like AOL Instant Messenger, Yahoo! Messenger, and Mirabilis ICQ. The ability for support technicians to get an answer to a question in real time, or for executives to communicate silently while on conference calls, or for customer user “communities” to exchange tips is leading to a rapid spread in corporate deployments.

According to Richard Stiennon of Gartner Group, Instant Messaging will surpass e-mail as the most frequently used means of online interpersonal communication by 2006.[1] Indeed, corporate users are demanding that the real-time, on-demand service be available as an important business facilitator.

Corporate IT departments, who are charged with supporting new business applications to meet evolving business requirements, also have the responsibility of evaluating new applications in the larger context of corporate operations, including security. Part of a new application’s security assessment involves determining whether the company’s security

[1] What May Lurk in Your IM Session, Gartner Note Number COM-14-2666, 16 August 2001, by Richard Stiennon

71 Second Avenue, Waltham, MA 02451
Tel: 781-209-3200 Fax: 781-209-3199
E-mail:info@okena.com

www.okena.com

6905 Rockledge Drive, Suite 600
Bethesda, MD 20817
301-896-9388

posture must be modified to accommodate the new application, whether the new application has the potential to circumvent the corporate security policy, and whether users require additional security training on safe application use.

This paper discusses three risk areas of this technology. These risks include:

- Vulnerable IM client software that can be exploited by external users, or by a new generation of network viruses or worms, to take control of the IM user's computer.
- Increasingly sophisticated attempts by viruses or attackers to trick IM users into running dangerous commands or opening infected files, compromising the IM user's computer.
- Insecure IM infrastructure, including insecure storage outside the organization and lack of encryption of the IM session expose sensitive corporate information to discovery by unauthorized parties.

Some of these risks involve exploitation of traditional security vulnerabilities; others involve possible activity that is best addressed by appropriate definition and enforcement of corporate policy. Methods that organizations can use to mitigate these risks are discussed at the end of the paper.

1. Exploits against vulnerable Instant Messenger agents can compromise computers.

A number of Instant Messenger programs have been discovered to have vulnerabilities that can be exploited by remote users. This type of attack involves one program communicating directly with an IM client, and sending it commands that will confuse it. A properly chosen set of commands will result not in the IM client crashing, but rather in it executing the code that the attacker sent. A number of different types of attacks against IM client software have been demonstrated.

- Attack code hidden in files transferred from one IM client to another can be executed, possibly installing virus or Trojan Horse programs on the target. Because the IM client did not properly validate the type of file that was transferred, it was tricked into running executable code[2].
- A buffer overflow in a feature of AOL Instant Messenger results in the silent download and execution of an attacker's code. The buffer overflow attack was performed when one user invited another user to participate in an on-line game. The Instant Messenger user was not prompted before the download, and did not have the opportunity to stop this attack[3]. As many as 100 million users are vulnerable to this attack.
- Sometimes, the IM vendor has used buffer overflow attacks to identify whether the user is running their own IM client, or a competitor's. AOL once exploited a buffer overflow in AIM to battle Microsoft. By exploiting the overflow, AOL attempted

[2] "Modifed images can lead to JavaScript/VBScript execution in AIM", 24 January 2001, http://online.securityfocus.com/archive/1/158334

[3] "ICQ contains a buffer overflow while processing Voice Video & Games feature requests", 17 January 2002, http://www.kb.cert.org/vuls/id/570167

to identify and exclude users of Microsoft's MSN Messenger. The implication is that an IM vendor (or more likely someone exploiting the same technique) could use this buffer overflow to execute malicious code[4].

- As more sophisticated network worms like NIMDA combine different types of attacks to increase their chances of success, IM clients offer an inviting opportunity for attacker mischief. New Trojan horse applications that use outbound tunneling from the infected machine bypass traditional corporate firewalls, or even desktop firewalls[5].

2. Attempts to trick the user ("Social Engineering") into running malicious code.

Since IM allows users to directly communicate with other users, the opportunity for one IM user to trick another into doing something causing computer compromise is all too easy. This "attack" on the computer user is often referred to as "Social Engineering". Several examples of social engineering attacks against IM have been demonstrated.

- The "Coolnow" worm sends a message to an MSN Messenger IM user encouraging them to click on a particular web link[6]. This link is to a web page that exploits a bug in Internet Explorer to silently download and run the virus code. The user has to be fooled into clicking on the link, but the web page itself can look entirely harmless.
- The W32/Hello worm sends its own Visual Basic code directly to the target, as a file transfer. It tries to trick the user to click on the file to execute it. This worm attacked the MSN Messenger client. If the user runs it, it uses the MSN Messenger Contact List to find new targets[7].
- The ICQ Filename Truncation Vulnerability allows attackers to disguise malicious files. A vulnerability existed in Mirabilis' ICQ IM client where only a certain number of characters in the file name were displayed when querying the user to accept a download. Thus, a file named something like "mypix.jpg .exe" might appear as "mypix.jpg". A user might be fooled into thinking that the file was a harmless picture, when in reality it was a malicious executable[8].

3. Insecure IM infrastructure undermines security and allows leakage of sensitive information which is stored on IM Servers.

No organization would allow all corporate email to be sent using external email servers. The sensitive nature of the email communications requires that each organization run their own servers and mandate security settings for approved email clients. This internal control

---

[4] 27 August 1999, http://www.securiteam.com/securitynews/2EUQJRFS3U.html

[5] "No Desktop is an Island", 12 November 2001, Network Computing, http://www.networkcomputing.com/1223/1223f45.html

[6] 14 February 2002, http://www.europe.f-secure.com/v-descs/coolnow.shtml

[7] 23 April 2001, http://vil.mcafee.com/dispVirus.asp?virus_k=99077&

[8] 1 November 1999, http://www.securiteam.com/exploits/2GUPRRFQ0U.html

allows IT to ensure that confidential communication remains confidential. Instant Messenger infrastructures typically do not offer this same level of confidentially.

- Instant Messenger chat sessions have the appearance of a real-time discussion, much more so than email, which can appear more like the exchange of memos. This "real time" paradigm can cause people to forget (or ignore) the fact that the entire IM session is archived on the IM server[9]. These archived logs contain the entire history of the discussion. Disclosure of sensitive IM discussions held by executives of the Internet firm eFront led to major corporate embarrassment and legal difficulties[10].
- IM servers can be located on corporate IM servers, but often are at one of the major IM providers, such as AOL or Yahoo! These vendors are not in the business of guaranteeing security for corporate chat sessions, but rather cater to a home user market. Sometimes, information on these servers is compromised: a highly publicized security breach in 2001 resulted in the exposure of information like user IDs and server logs[11].
- Some IM clients silently reconfigure security settings like Internet Explorer Security Zones to make their systems "easier to use". It can be tricky for IT to ensure that well-planned security configuration settings will not be compromised when IM clients are installed[12].

Protecting Instant Messenger Clients

If IM is to achieve broad penetration in the business world, the security aspects of IM must be addressed. OKENA presents a solution to the security policy risks inherent in popular IM platforms through the use of IM-specific policies in its StormWatch application security suite.

StormWatch also allows a simple and rigorous implementation of corporate IM policy – allowing administrators to define *and enforce* how applications like IM behave. These protective policies allow mitigation of all of the IM risk areas:

- The risk of vulnerability exposure of insecure IM clients,
- The risk of end users to be fooled into running dangerous programs received via IM file download, and

---

[9] "Business: IM is getting out of control", 25 April 2002, ZDNet, http://zdnet.com.com/2100-11-529435.html?legacy=zdnn

[10] "ICQ logs spark corporate nightmare", 15 March 2001, C|Net, http://news.com.com/2100-1023-254173.html?legacy=cnet

[11] "Hackers penetrate ICQ Web servers", 26 June 2001, Computerworld, http://www.itworld.com/Sec/2199/CWD010626icqhack/

[12] "Langa Letter: More Instant-Messaging Security Holes", 1 October 2001, http://www.informationweek.com/story/IWK20010927S0021. "Fred Langa warns that hyper-aggressive IM installations may end-run your online safeguards."

- The risk of confidential information being sent out of the organization's IT infrastructure via IM.

The default StormWatch Desktop protection policy includes a "Defense-In-Depth" approach to IM client security:

1. All network client or server applications are protected from buffer overflow exploit attempts. Attempts by an attacker to overflow a buffer in an IM client and run code will be detected and stopped.
2. By default, IM clients are prohibited from downloading executable code. Even if an IM user wants to download an executable – for example, if a remote user tries to send it to him – StormWatch will stop the download. A social engineering virus that tricks a user into clicking on a link that downloads an attack program will likewise be blocked. If a bug in an IM client or web browser would normally silently download the attack code, StormWatch will still block the download.
3. Executable code downloaded by any network application – email, web browser, or peer-to-peer file sharing programs – is monitored closely when it is run. StormWatch enforces a highly restrictive security policy on this downloaded content, and tightly bounds what it is allowed to do. For example, downloaded executable programs will be prohibited from accessing the Outlook address book. Even if the StormWatch policy is changed to allow IM download of executable files, and if a user can be tricked into running a virus, StormWatch will prevent the virus from propagating via email.
4. All network client or server applications are prohibited from running sensitive system commands, such as command shells or disk partitioning programs. Malicious code that might be downloaded by a user is not allowed to execute these potentially damaging programs.
5. StormWatch protects other network applications, such as web browsers and email clients. If an IM client modifies the security configuration settings of one of these other applications, StormWatch will prevent attacks against that application from downloading and executing attack code. The same types of protections StormWatch offers for IM clients protect other applications as well.
6. StormWatch allows IT security to specify which IM servers may be used by IM clients, which IM clients can be used at all, and whether encryption (for example, via SSL) of IM sessions is either prohibited or mandatory. This allows IT to centrally specify and enforce which IM clients are approved for use, how those IM clients are to be configured and used, and which IM servers will host the IM session.

Policy-based IM Control

StormWatch is easily configured to control which IM clients are allowed to communicate with which IM servers. For example, an organization could configure a security policy to allow users only to connect to the organization's internal IM servers. This will ensure that confidential information is not sent outside the organization's network.

Since StormWatch protects servers as well as desktops, the organization's IM servers can be protected in exactly the same manner as its desktops. Buffer overflow or other attacks against the servers will be detected and blocked. IM log files can be easily placed "off limits", by prohibiting other applications from accessing the files. Not only can all access to the IM server applications be logged, but access can be controlled as well.

Above and beyond the immediate security concerns posed by IM are the questions of corporate policy and how to enforce it. Instant Messenger is fast becoming a ubiquitous corporate tool, not because its use is mandated at a corporate level but because end-users are proactively seeking it out. Administrators are therefore faced with retroactively defining a policy for how IM can and should be used within the enterprise. Only an application-centric security product like StormWatch can help ensure policy compliance by actually enforcing how the application behaves.

StormWatch provides a complete, robust, "Defense In Depth" protection for both Instant Messenger clients and servers. OKENA offers a range of white papers and presentations on how StormWatch protects servers and desktops. Please visit http://www.okena.com for more information.

Copyright © 2002 OKENA, Inc. All rights reserved.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of OKENA, Inc. OKENA, Inc. assumes no responsibility for any errors that may appear in this document. No part of this documentation may be reproduced without the express prior written permission of the copyright owner.

OKENA, STORMWATCH, STORMSYSTEM, STORMFRONT, STORMTRACK, INCORE, INTRINSIC SECURITY, and AN UPTIME APPROACH TO SECURITY are trademarks or registered trademarks of OKENA, Inc. in the U.S.A. and certain other countries. Other names and products are trademarks or registered trademarks of their respective holders.

71 Second Avenue, Waltham, MA 02451
Tel: 781-209-3200 Fax: 781-209-3199
E-mail:info@okena.com

www.okena.com

6905 Rockledge Drive, Suite 600
Bethesda, MD 20817
301-896-9388