INSTANT MESSAGING SECURITY

February 2008

TABLE OF CONTENTS

SUMMARY

Instant messaging (IM) is a fast growing communications medium popular with both home and corporate users. Though IM is an effective and easy means of network-based communication, it introduces a number of security risks if proper security measures are not applied. This paper discusses the security risks associated with using this popular communication channel, and provides a set of best practices that can be implemented when deploying the technology in a business environment.

I. WHAT IS INSTANT MESSAGING?

Instant Messaging (IM) is a form of electronic communication enabling ad hoc and "live" collaboration through sending and receiving messages almost instantaneously across a network connection[1]. With the introduction of messaging tools such as ICQ[2] and MSN Messenger[3], more and more people are enjoying the convenience and ease provided by real-time messaging systems in their day-to-day life. IM has also found a place in business, for services such as communicating with customers and partners, offering customer support, receiving real-time alerts, as well as management and project coordination. IM tools support any process where quick response and rapid problem solving are needed, and where faster communication than emails or telephones is useful.

In general, the user needs to download and install an IM client on his or her client device (which can be a desktop computer, smartphone or PDA) and set up a user account before he or she can communicate. An IM server acts as a database where contact points are located. For public IM services such as ICQ and MSN Messenger, the servers are hosted on the Internet. For corporate IM systems, IM servers might be hosted within the organisation's internal network.

[1] http://www.tech-faq.com/instant-messaging.shtml

[2] http://www.icq.com/

[3] http://www.msn.com/

USAGE TRENDS OF IM IN BUSINESS

According to an instant messaging trend survey conducted in 2007[4], IM is not only popular with home users, but is also increasingly common in the workplace. More than 27 percent of those surveyed responded that they used instant messaging at work. About 19 percent of IM users indicated that they sent more instant messages than emails to co-workers and colleagues, whereas 55 percent of teenagers now get help with their homework through IM. In addition, half of the at-work IM users said they believed IM makes them more productive at work. However, nearly 79 percent of workers using IM in the office indicated that they have used IM for personal matters.

[4] http://press.aol.com/article_display.cfm?article_id=1343

II. POTENTIAL THREATS

Public IM services are rapidly becoming an alternative channel for the spread of viruses and malicious code. Common public IM services usually lack native encryption to protect information being transmitted, and they also allow bypassing of corporate content inspection filters. Furthermore, the lack of a comprehensive audit trail might not meet certain security or regulatory compliance requirements.

The following are potential threats when using IM services:

1. A Vehicle for the Spread of Malicious Code

   Enterprise use of IM is growing in both volume and importance. IM users report that they can benefit from a faster decision-making process, higher productivity and lower telecommunication costs. Concurrently, IM threats (typically viruses), are rapidly gaining attention as attackers begin to shift their focus from better-protected email systems to IM networks. Spam messages can also be spread via IM. The spam that a user receives via an Instant Messaging Services is referred to as "spim"[5].

2. IM software Vulnerabilities

   Just like any other software application, popular IM clients have a history of common security vulnerabilities. Installing an IM client may introduce new vulnerabilities to a computer system.

3. Leakage of Sensitive Information

   Confidentiality is a major concern when using a public IM service for communication. In public IM networks, messages exchanged between users are often routed through IM server farms controlled by the service providers themselves. If client IM software has a peer-to-peer capability, users can communicate with each other without passing through IM servers. No matter

[5] http://www.quickonlinetips.com/archives/2005/10/spim-instant-messaging-spam/

which mode is being used, IM traffic is vulnerable to eavesdropping because most public IM clients do not possess any encryption capability. Therefore, it is possible that sensitive information can be read or sniffed by unauthorised users. The situation can be even worse when public IM services are used to communicate with individuals outside an organisation.

The protocols used by public IM services are often considered rogue protocols, because they are specifically designed to evade standard security controls. Not only can IM clients be configured to connect through SOCKS or web proxy servers, but the protocol is also capable of finding its way out through the firewall on its own by looking for an open port, such as TCP port 80, or by tunnelling its traffic inside HTTP requests, making it unrecognisable from standard web traffic. The scripting and file transfer capabilities of IM systems might also expose an organisation to leaks of sensitive information. Therefore, organisations should establish proper policies and controls on the use of IM.

4. Monitoring and Retention Headaches

   Monitoring IM messages and retaining messages for business records is no easy task. Deciding which instant messages need to be logged and recorded is probably more difficult in the IM environment because an entire thread of messages is needed to provide meaningful context for a particular message.

5. Accountability

   In a public IM network, the identities of IM senders and receivers cannot be verified. Public IM accounts are vulnerable to hijacking or spoofing, allowing an intruder to impersonate a conversation with legitimate users.

III. CONSIDERATIONS WHEN CHOOSING AN ENTERPRISE IM SOLUTION

There are now a number of enterprise IM solutions available in the market that give organisations the ability to build and manage their own internal IM service. The following security features should be considered when choosing an enterprise IM (EIM) solution[6]:

1. Authentication Controls: Any enterprise IM solution should integrate with the company's existing authentication mechanisms, such as interfacing with a Microsoft Active Directory.
2. Confidentiality Controls: Because sensitive information such as budget or sales volume data might be transmitted within an enterprise IM system, EIM products should provide strong encryption to protect all messages travelling within company networks.
3. Anti-virus Controls: An EIM product should offer close integration with an anti-virus solution, so as to ensure that all files transferred over EIM channels are virus free.
4. Logging / Auditing Controls: All communication within the organisation might need to be logged to ensure employees aren't abusing the service, or to satisfy certain regulatory requirements. The selected EIM product should also meet the organisation's logging requirements.

In addition, the organisation needs to define an acceptable IM usage and privacy policy, and communicate to all employees the risks of using IM in business. If IM communications are to be logged and monitored by the company, this policy should also be clearly disseminated to employees.

---

[6] http://www.instantmessagingplanet.com/enterprise/article.php/11208_2236051_1

IV. BEST PRACTICES

TIPS FOR ENTERPRISE USERS

Given that there are a number of potential security risks in deploying an IM system, the use of instant messaging should be restricted to business purposes only, and prior approval should be obtained before any system (public or private) is deployed. If an organisation decides to use an IM system, the following security controls should be implemented:

1. Observe all Security Procedures

   As the rule of thumb, all relevant security requirements **[including the Security Regulations, Baseline IT Security Policy and IT security Guidelines (the blanketed text is for ITGInfoStation version only]** should be observed when using IM.

2. Develop an IM Usage Policy and Clearly Disseminate to all Users of IM

   An IM usage policy should clearly state whether the use of IM is acceptable within the organisation and, if it is, what the restrictions are. The IM usage policy should be technology and product neutral. Messages generated via IM should be regarded as business records, irrespective of whether they are generated on a public system or on an internal enterprise system. If the use of IM is for business purposes, an internal retention policy or external regulations should be followed.

3. Implement IM Hygiene Solutions

   IM hygiene solutions are a collection of services that allow organisations to enforce IM usage policies by monitoring usage, managing IM traffic and filtering content to block unwanted messages, computer viruses and offensive materials, as well as logging all IM messages for audit purposes.

4. Educate Users on the Best Use of IM and Strengthen Desktop Protection

One of the major threats posed by IM in the corporate network is IM-based malicious code attacks. IM viruses are usually transmitted either as executable file attachments or as hyperlinks in IM text, directing victims to malicious web servers. In most cases, these viruses are not automatically executed. Rather, they exploit social engineering tactics to convince victims to open unknown files or click on suspicious links.

Dedicated IM hygiene products are one solution for protecting and managing IM usage. By filtering active hyperlinks as well as all file attachments, these products can effectively eliminate a large portion of the attack vectors used by IM viruses. Desktop anti-virus products can also help detect most of these threats.

Training end-users to be more sceptical about incoming instant messages, even those from their own buddy lists, should also be part of an overall strategy. The usual precautions of quickly patching software vulnerabilities, running anti-virus software and personal firewalls are all effective against IM threats.

In view of the above, user education and desktop protection should be taken into account when planning the deployment of IM in the enterprise.

5. Implement an Enterprise IM (EIM) Solution Instead of Using Public IM Clients

   If IM services are required for business purposes, organisations should explore the possibility of deploying their own Enterprise IM architecture within the network environment. This will allow comprehensive monitoring and storage of data, and help provide reassurances regarding internal user identities. In addition, a closed system can still be made available to key customers and vendors on the outside, but all external IM should go through a gateway where it can be monitored and managed. Enterprise IM solutions provide organisations with their own clients and servers that have built-in enterprise security features including blocking, logging, auditing, monitoring, routing and encryption.

6. IM Client Protection

Users should disable all network services provided by the IM service, enable all notifications when incoming messages/calls/files are received, disable sharing of resources, and disable remote activation of microphones and video cameras.

TIPS FOR END-USERS

The following tips are designed for end-users using IM as regular communication tool[7]:

1. Do not set your IM client to automatically accept file transfers. If you do, you place yourself at very high risk of automatically accepting virus-infected files unknowingly.
2. Before opening any file received via IM, you should verify with the sender that he or she did actually send that file to you. In addition, make sure the file has been scanned by anti-virus software before opening it.
3. Never click URL links within an IM that is sent from untrusted / unknown contacts. There have been reports of viruses being spread by users clicking on an IM URL[8].
4. Never send personal or sensitive information by IM. Even if there are compelling reasons to do so, ensure sensitive information is encrypted.
5. Keep your IM software (and other system components) up-to-date with the latest patches, enable personal firewall protection, and install anti-virus software with the latest virus signatures, and malicious code definitions, as well as detection and repair engines.

---

[7] http://chris.pirillo.com/2007/11/17/instant-messenger-virus/

[8] http://antivirus.about.com/od/virusdescriptions/a/kelvir.htm