Instant Insecurity: Security Issues of Instant Messaging

by Neal Hindocha
last updated January 13, 2003

Instant messaging is an increasingly popular method for communicating over the Internet. Instant messaging (IM) is a real-time supplement to and, in some regards, a replacement for e-mailing. Unlike e-mail, instant messaging allows users to see whether a chosen friend or co-worker is connected to the Internet. Typically, the instant messaging service will alert a user if somebody on the user's list of correspondents is on-line. Instant messaging also differs from e-mail in that messages are exchanged directly almost instantly, allowing for a two-way communication in real-time.

Because of the almost immediate two-way nature of communication, many users feel that the use of instant messaging in the workplace leads to more effective and efficient workplace communications and, therefore, to higher productivity. As a result, IM is increasing in popularity in both professional and personal applications. However, as with most things Internet based, the increasing use of instant messaging has led to an associated increase in the number of security risks.

This paper will describe instant messaging and offer a brief overview of some of the security threats associated with the service. This article is based on a previously published Symantec white paper called Threats to Instant Messaging.

How does Instant Messaging Work?
Instant messaging networks consist of clients and servers. A user installs a client that connects to a server operated by the instant messaging network vendor, such as AOL or ICQ, or Yahoo Messenger. (It should be noted that because they use different protocols, the different instant messaging services are not interoperable. Therefore, ICQ users can only communicate with other ICQ users, not with users of other instant messaging services.) All users that sign up for instant messaging are given a unique identifier, which can be either a name or a number. The user then gives out the unique identifier to people that he or she wants to communicate with via the instant messaging network. The user starts an instant messaging session by authenticating to the server. When two authenticated users want to communicate, the following sequence occurs.

Alice instructs the instant messaging client to send a text-message to Bill. The client creates a packet containing the message and sends it to the server. The server looks at the packet and determines that the recipient is Bill. The server then creates a new packet with the message from Alice and sends it to Bill.

Most instant messengers will continue to send all following messages via the central server. However, some instant messengers create a direct connection between the users after the first message. The use of a central server is beneficial in many ways. For example, Alice is only required to know the unique identifier for Bill. Furthermore, she can send messages to Bill even if he is not on-line. The server will store the message until Bill authenticates with the server, at which time it is sent to him.

Most instant messaging clients have the ability to create buddy lists, or lists of preferred people the user wants to communicate with that keeps track of whether those people are available for instant messaging. For example, when Bill sends Alice his unique identifier, Alice can save it in her buddy list.

From then on, whenever Alice authenticates with the instant messaging server, she can see Bill in her buddy list; therefore, she is not required to remember Bill's unique identifier. She will also be notified if he is on-line, off-line, away from his desk, etc.

Instant Messaging Security Threats

Instant messaging networks provide the ability to not only transfer text messages, but also the transfer of files. Consequently, instant messengers can transfer worms and other malware. Instant messengers can also provide an access point for backdoor trojan horses. Hackers can use instant messaging to gain backdoor access to computers without opening a listening port, effectively bypassing desktop and perimeter firewall implementations. Furthermore, finding victims doesn't require scanning unknown IP addresses, but rather simply selecting from an updated directory of buddy lists. In addition to client-initiated file transfers, all the major instant messaging networks support peer-to-peer file sharing where one can share a directory or drive. This means that all the files on a computer can be shared using the instant messaging client, leading to the spread of files that are infected with a virus or other malware. As we shall see, this characteristic also makes information being communicated along IM vulnerable to unauthorized viewing.

Worms

Email worms are part of daily life for any computer security professional. However, these threats can be dealt with swiftly by effective gateway monitoring and by installing desktop AV protection. Therefore, once detection is available for a particular worm, infected emails will be stopped at the gateway. In the case of instant messaging, however, antivirus software does not currently monitor traffic at the gateway level. If a worm starts to spread using instant messaging, it cannot be stopped before it reached the user's computer.

The number of instant messaging worms is rising steadily. This is made clear when one considers the list of recent IM worms:

W32.Choke (June 6, 2001)
W95.SoFunny.Worm@m (July 3, 2001)
W32.Goner.A@mm (Dec. 4, 2001)
W32.Led@mm (January 22, 2002)
W32.Seesix.Worm(May 15, 2002)

Despite the growing threat, there are still no antivirus applications that directly monitor instant messaging traffic on a server level. This is due to the difficulty in finding Instant Messaging traffic, as it is often embedded inside HTTP packets. However, a few antivirus applications plug in to instant messaging clients, scanning files as they are received. The lack of applications scanning instant messaging network traffic is partly due to the difficulty in monitoring instant messaging traffic, as well as the constant modifications to the clients and the protocols they use. Unfortunately, this makes instant messengers an open door to the computer, as unscanned traffic will bypass most server-based security measures. Only the antivirus product running at the desktop level can catch the worms.

The way in which these worms replicate varies. Some of the worms spread via email as well as instant messaging. Others spread only via instant messaging. However, currently instant messaging worms all still require user interaction for execution. None make use of an exploit to allow auto-execution upon receipt. Therefore, if instant messaging users

are more aware of the threats and how to prevent them, the success of these worms would be significantly reduced.

Backdoor Trojan Horses
One can share every file on another person's computer using an instant messenger. All the popular instant messengers have file sharing capabilities or the ability to add such functionality by applying patches or plug-ins. As the instant messaging clients allow peer-to-peer file sharing, a trojan horse can configure the instant messaging client to share all files on the system with full access to everyone, and in this way gain backdoor access to the computer. The benefit for a hacker using an instant messenger to access files on a remote computer instead of installing a backdoor trojan horse is that even if the computer is using a dynamic IP address, the screen name will probably never change. Furthermore, the hacker will receive a notification each time the victim computer is on-line. Keeping track of and accessing infected computers will therefore be very easy for the hacker. In addition, the hacker does not need to open new suspicious ports for communication, but can instead use already open instant messaging ports.

There are currently a handful of trojan horse programs that target instant messaging. Some modify configuration settings so file sharing is enabled for the entire hard drive. These types of trojans pose a large threat, as they allow anyone full file access to the computer.

There are also classic backdoor trojan horses that utilize instant messengers to send messages to the author of the trojan, giving the hacker information about the infected computer. This information includes things such as system information, cached passwords, and the IP address of the infected computer. In addition, the hacker can send messages to the infected computer via instant messaging instructing it to perform some unauthorized action.

Backdoor trojan horses that allow access to the computer by utilizing instant messenger clients may be harder to prevent than classic backdoor trojans. Classic backdoor trojans open an outgoing listening port on the computer, forming a connection with a remote machine. This can effectively be blocked by a desktop firewall. However, if the trojan operates via the instant messaging client, it does not open a new port. As a result, the user has generally already created an allow rule in their desktop firewall products for instant messaging traffic to be outbound from their machine, thereby allowing the backdoor trojan horse using the same channel to go unblocked. The number of backdoor trojan horses utilizing instant messengers is increasing steadily.

Hijacking and Impersonation
Hackers can impersonate other users in many different ways. The most frequently used attack is simply stealing the account information of an unsuspecting user.

To get the account information of a user, the hacker can use a password-stealing trojan horse. If the password for the instant messaging client is saved on the computer, the attacker could send a trojan to an unsuspecting user. When executed, the trojan would find the password for the instant messaging account used by the victim and send it back to the hacker. The means for sending back the information to the hacker varies. They include using the instant messenger itself, IRC, and email.

Furthermore, since none of the four major instant messaging protocols encrypt their network traffic, attackers can highjack connections via man-in-the-middle attacks. By

inserting messages into an ongoing chat-session, a hacker could impersonate one of the chatting parties. Though more difficult, one can also highjack the entire connection by using a man-in-the-middle attack. For example, a disconnect message, which appears to come from the server, can be sent to the victim from the hacker. This will cause the client to disconnect. The hacker can also use a simple denial of service exploit, or other unrelated exploits, to keep the client disconnected.

Since the server keeps the connection open and does not know that the client has been disconnected, the hacker can then impersonate the victim user.

Stolen account information for any instant messenger can obviously be very damaging. Because the hacker can use this information to disguise himself as a trusted user, the people on the victim's buddy list will trust the hacker and may therefore divulge confidential information or execute malicious files. Losing a password for an instant messenger account can therefore be dangerous for more people than just the user who lost the password.

Denial of Service

Instant messaging may make a user's computer vulnerable to denial of service (DoS) attacks. These attacks may have different end results: some DoS attacks make the instant messaging client crash, others will make the client hang, and in some cases consume a large amount of CPU power, causing the entire computer to become unstable.

There are many ways in which a hacker can cause a denial of service on an instant messenger client. One common type of attack is flooding a particular user with a large number of messages. The popular instant messaging clients contain protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that allow the hacker to use many accounts simultaneously, or automatically create a large number of accounts to accomplish the flood-attack. Adding to this is the fact that once, the flood-attack has started and the victim realizes what has happened, the computer may become unresponsive. Therefore, adding the attacking user accounts to the ignore list of the instant messenger client may be very difficult.

Even though denial of service attacks are more of an annoyance than they are dangerous, they can be used in combination with other attacks, such as the hijacking of a connection.

Unauthorized Disclosure of Information

Information disclosure could occur without the use of a trojan horse. Since the data that is being transmitted over the instant messaging network is not encrypted, a network sniffer, which can sniff data on most types of networks, can be used to capture the instant messaging traffic. By using a sniffer, a hacker could sniff the packets from an entire instant messaging session. This can be very dangerous, as he may gain access to privileged information. This is particularly dangerous in the corporate environment, in which proprietary or other confidential information may be transmitted along the instant messaging network.

Information Disclosure – A Case Study

Some instant messaging clients allow all communication to be saved in log-files. Even though this is a feature that is often requested and required by companies, it can sometimes be very dangerous to keep logs, as the logs may include sensitive company

data. This was made evident in a case that occurred at the beginning of 2001, where a hacker stole logs from an instant messaging client belonging to the CEO for a company called eFront. The hacker posted the logs to several places on the Web, thereby creating one of the worst possible corporate nightmares. The logs included sensitive company data regarding business partners, employees and affiliate websites. After the posting of the logs, several members of the senior staff for eFront resigned.

The eFront case shows how dangerous it can be if a hacker is able to monitor instant messaging sessions. Even though the log-files were stolen in this case, sniffing the data-packets could have caused the same damage.

Blocking Instant Messaging

The most effective way of preventing instant messaging to jeopardize the security of a network and the machines upon it is to deny it access to the network in the first place. Preventing the use of instant messaging is difficult. Simple port blocking firewalls will not be effective because clients can use common destination ports such as HTTP port 80 and FTP port 21. Most of the clients will even auto-configure themselves to use other ports than the default one if they are unable to communicate over the default port.

Firewalls with protocol analysis may prevent instant messaging clients from communicating via common destination ports, such as port 80, because instant messaging traffic is different from HTTP traffic. However, the latest versions of all the various clients embed the traffic data within an HTTP request, bypassing protocol analysis.

The client and responses essentially prepend an HTTP header to each packet sent, thereby circumventing any protocol analysis firewall. With some clients, such as ICQ and AIM, HTTP headers are added only when an HTTP proxy is being used. However, AOL provides access to such a proxy for free, namely www.proxy.aol.com, and the clients auto-configure themselves to use this proxy if direct access is being blocked on all ports.

Even though, in the case of AIM and ICQ, blocking the address can prevent access to the proxy, there are many other proxy servers freely available on the Internet. A simple search on the Internet will return hundreds of freely available proxy servers. Keeping up with blocking each one is an administrative nightmare. Corporate policies are the best way to prevent employees within companies from using instant messaging. In order to ensure that instant messaging does not jeopardize the security of the organization's systems, it should be clearly stated in any and all security policies that instant messaging will be permitted only with the express knowledge and consent of the organization.

Securing Instant Messaging

That said, many organizations would prefer to give their employees access to instant messaging, particularly as it can be a valuable communications tool. In this case, it is vital that the organization ensure that the IM service that is employed is as secure as possible. Securing instant messaging is not an easy task. One of the best ways to secure the information being transmitted along an IM network is to encrypt it. There are currently several companies that offer encrypted instant messaging communication. There are also instant messaging clients available that are compatible with some of the major networks that apply encryption to the instant messaging traffic.

In addition to encrypting the communication, the main thing a corporation should do to secure instant messaging is to keep logs. However, as seen in the eFront case, it is absolutely vital to keep the logs secure.

Furthermore, if file transfer via the instant messaging network is not required, then an instant messaging system that does not allow for files to be transferred should be utilized.

Conclusion

Because hackers generally target specific computer systems, they aren't the biggest threat for any instant messaging network as a whole. On the other hand, worms are non-discriminate and target all computer systems of a particular network. As a result, they appear to pose the biggest threat for the future. We have seen worms that use security exploits and become widespread in a very short amount of time. Code Red and Nimda are examples of worms that used security exploits to spread themselves quickly.

It is unlikely that instant messaging will exceed email as the primary vector of infection in the near future, as far more people use email than instant messaging. Furthermore, the major instant messaging networks still use proprietary protocols so that a worm that spreads via one service, such as MSN Messenger, will not affect users of another service, such as Yahoo! Messenger. However, this does not mean one can disregard the threat that instant messaging poses. As we have seen, there are already worms in the wild that spread via instant messaging. And If clients become interoperable, or users primarily utilize one network, instant-messaging worms may become more widespread.

The number of worms for instant messaging is increasing each month, and looking at the success of some of these worms, clearly instant messaging is an up and coming platform for malicious threats. Furthermore, there are many exploits available for the various clients. As a result, security professionals and end users alike need to be aware of the security issues involved with instant messaging. As with any Internet-based technology, the best way to make ensure the security of instant messaging services is to educate users of the risks involved and the means of mitigating those risks, preferably before a serious incident occurs.

Neal Hindocha started working as a virus researcher for Symantec in 1999. He currently works in the Symantec Security Response department, focusing on security threats.