Chapter 14

UNAUTHORIZED LISTENING AND LOOKING

INTRODUCTION

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/look 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 [1].

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 [1].

This chapter describes instant messaging and offer a brief overview of some of the security threats associated with the service. It covers the unauthorized listening and looking of IM: Yeah! Eavesdropping!

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 [1].

> **Note:** 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 [1].

The user starts an instant messaging session by authenticating to the server. When two authenticated users want to communicate, the following sequence occurs:

- Shana instructs the instant messaging client to send a text-message to Bernard. 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 Bernard. The server then creates a new packet with the message from Shana and sends it to Bernard [1].

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, Shana is only required to know the unique identifier for Bernard. Furthermore, she can send messages to Bernard even if he is not on-line. The server will store the message until Bernard authenticates with the server, at which time it is sent to him [1].

Furthermore, 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 Bernard sends Shana his unique identifier, Shana can save it in her buddy list. From then on, whenever Shana authenticates with the instant messaging server, she can see Bernard in her buddy list; therefore, she is not required to remember Bernard's unique identifier. She will also be notified if he is on-line, off-line, away from his desk, etc. [1].

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 [2] 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 you shall see, this characteristic also makes information being communicated along IM vulnerable to unauthorized viewing and listening [1].

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