

Lab 1.6.1: Using Collaboration Tools— IRC and IM

Topology Diagram



Learning Objectives

Upon completion of this lab, you will be able to:

- Define Internet Relay Chat (IRC) and Instant Messaging (IM).
- List several collaborative uses of IM.
- List several misuses and data security issues involving IM.
- Use IRC to demonstrate collaboration.

Background

E-mail permits multiple users to collaborate, share ideas, and transfer files. However, unless the user constantly monitors the e-mail account, unread e-mail may go unnoticed for a long period of time. When people have wanted immediate contact, the telephone has been the technology of choice. Unfortunately, the telephone cannot be used to transfer files. What collaborators need for communication in the human network is a tool that has the flexibility of e-mail with the responsiveness of the telephone. Internet Relay Chat (IRC) and Instant Messaging (IM) fit nicely into these requirements. Using the Internet or a private corporate network, users can easily exchange ideas and files. IMing and Chatting are both methods of real-time communication; however, they are implemented differently.

Instant Messaging provides one-on-one communication with "accepted" individuals. To initiate an Instant Message, one person needs to "invite" another. The recipient of the invitation needs to know—and accept—the IM session based on the other user's screen name. IM clients allow you to have an approved list of users, often called a Buddy List. If you want to communicate with more than one person at a time, you can open additional IM windows. Each of these windows represents a two-person communication.

Internet Relay Chat, on the other hand, allows multiple people to interact. Chat also provides a degree of anonymity. To start chatting, you establish a connection to a chat server and join a discussion on a particular topic. When you join, you are said to "join a room." In the chat room, you typically create your own identity and can give as little information about yourself as you choose.

While the following discussion focuses primarily on IM, a brief hands-on lab with our "model Internet cloud" will demonstrate the ease of IRC.

IM requires a device providing services that allows users to communicate. This device is referred to as the *Instant Messenger Server*. The users on the end devices, such as a computer, use a piece of software called the *Instant Messenger Client*. This arrangement is called a client/server relationship. IM

clients connect to an IM server, and the server joins clients. This relationship is called an IM network. There are many different IM networks available, each with a dedicated following of users. Popular IM networks include America On Line (AOL) Instant Messenger (AIM), Windows Live Messenger (MSN), Yahoo! Messenger, and ICQ (I Seek You). Figure 1 shows the AIM client application connected to the AIM network.



Figure 1. AIM Client

Features

IM services have several common features:

- When an IM client connects to the IM network, any existing connections can be alerted through a contact list, a list of other people that you communicate with through the IM Client.
- File sharing between IM clients enables work collaboration.
- Text messaging between clients is possible, and can be logged.
- Some IM networks offer audio services.
- Newer services that some IM networks are beginning to provide include video conferencing, Voice over IP (VoIP), web conferencing, desktop sharing, and even IP radio and IPTV.

Protocols

Each IM network uses an agreed-upon method of communication, called a protocol. Many of the IM networks use proprietary protocols. AIM and ICQ (purchased by AOL) use the proprietary Open System for Communication in Realtime (OSCAR) protocol. Both Microsoft and Yahoo! have proprietary protocols but have partnered services for joint connectivity.

Throughout this course we will learn about many different protocols. The Internet Engineering Task Force (IETF) has attempted to standardize IM protocols, notably with the Session Initialization Protocol (SIP). SIPv2 was originally defined in RFC 2543, and made obsolete by RFC 3261. As with proprietary IM protocols, there are numerous open source protocols.

Some IM client applications, such as Gaim and Trillian, can differentiate between the various IM network protocols; IM servers can also incorporate this support. The IETF formalized an open standard, Jabber, based on the Extensible Messaging and Presence Protocol (EMPP). Applicable IETF references are RFC 3290 and RFC 3291. Encrypted communication is supported.

Social misuse of IM has been a concern for parents, and many IM networks encourage parental control. Child restrictions include limiting IM contacts and providing supervision while online. AIM and Yahoo! Messenger provide free supervision software tools. Some parental supervision tools include background logging, online time limits, chat room blocking, blocking specific users, and disabling certain functions of the client.

Security

Multiple security issues have been identified with IM. As a result, many organizations either limit or completely block IM from entering the corporate network. Computer worms, viruses, and Trojan horses, categorized as malware, have been transferred to IM client computers. Without strong security methods, information exchanged between users can be captured and disclosed. IM clients and IM servers have experienced application vulnerabilities, which have resulted in vulnerable computers. Even legitimate users can congest network throughput by transferring large files.

How does a system administrator protect his or her network from IM vulnerabilities and misuse? The SysAdmin, Audit, Network, Security (SANS) Institute recommends several countermeasures. The following list is from the SANS web site, <http://www.sans.org/top20/#c4>:

C4.4 How to Protect against IM Vulnerabilities and Unauthorized IM Usage

- Establish policies for acceptable use of IM. Ensure that all users are aware of those policies and clearly understand the potential risks.
- Standard users should not be permitted to install software. Restrict Administrative and Power User level privileges to support personnel acting in their support capacity. If a user must have Administrative or Power User privileges, create a separate account to be used for his or her daily office functions, Internet surfing, and online communication.
- Ensure that vendor patches are promptly applied to IM software, interrelated applications, and the underlying operating system.
- Employ antivirus and antispyware products.
- Do not rely on external IM servers for internal use of IM; provide a commercial grade IM proxy or internal IM server.
- Create secure communication paths when using IM with trusted business partners.
- Appropriately configure intrusion detection and prevention systems. Understand that many IM applications are capable of enabling associated communications to masquerade as otherwise legitimate traffic (for example, http).
- Consider deploying products specifically designed for IM security.
- Filter all http traffic through an authenticating proxy server to provide additional capabilities of filtering and monitoring IM traffic.
- Block access to known public IM servers that have not been explicitly authorized. (Note: This offers only partial protection due to the number of potential external servers.)
- Block popular IM ports. (Note: This offers only partial protection, due to the number of potential protocols and associated ports, and the ability of applications to bypass port restrictions.)
- Monitor using an Intrusion Detection/Prevention system for users creating tunnels for IM or bypassing proxies.

The Future of IM

The future of IM is promising, enabling users to adapt new technologies for collaboration. For example, mobile IM supports mobile users, providing IM services to hand-held cellular phones. Most popular cellular phone manufacturers have their own form of mobile IM. Another popular hand-held appliance is the Blackberry. The Blackberry supports common IM tools, such as text messaging, as well as push e-mail, telephony, and web browsing.

Scenario

The topology diagram shows two computers connected to a “cloud.” In networking, a cloud is often used to symbolize a more complex network, such as the Internet, which is not the current focus of this discussion. In this lab, you will use two computers that must first obtain communication software from the network cloud. After installing the software, the cloud will still be necessary to provide communication services. In subsequent chapters you will study in great detail the devices and protocols that are inside the cloud. Inside the cloud is a server called *eagle-server* as well as other networking devices. This lab uses eagle-server as the IRC server, and Gaim as the IRC client. Gaim is used for this lab, but any IRC client may be used if available. An IRC client is available for download from eagle-server, URL <http://eagle-server.example.com/pub>.

Estimated completion time is 45 minutes.

Task 1: Configuring the Chat Client

The IRC protocol is an open standard, originally described in RFC 1459, communicating across plain text links.

Step 1: Verify that there is an IRC client on the lab computer.

If not, download and install gaim-1.5.0.exe (windows executable) from URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter1. Accept the default settings during the installation. After verifying that the Gaim chat client is installed, use the following steps to configure Gaim:

Step 2: Open Accounts window.

1. Open Gaim and select the Login window, icon **Accounts**. The Accounts window is shown in Figure 2.

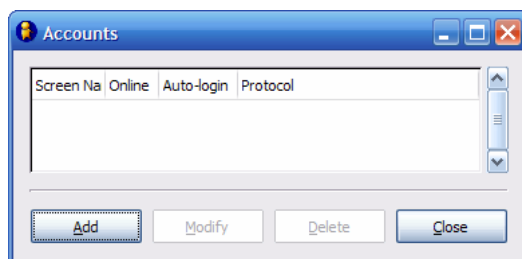


Figure 2. Gaim Accounts Window

2. On the Accounts window, click **Add**.

Step 2: Add a new account.

1. See Figure 3. On the Add Account window, expand the “Show more options” option. Fill in required information:

Protocol: IRC
Screen Name: (how others will know you)
Server: eagle-server.example.com
Proxy Type: No Proxy

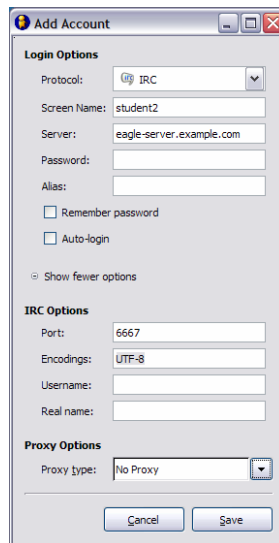


Figure 3. Gaim Add Account Window

2. When finished, click **Save**.
3. Close the Accounts window.

Task 2: Connection to Chat Server

Step 1: Sign On.

Return to the Login window, where the new account to eagle-server should be visible. Click **Sign-on**. Two windows should open. Figure 4 shows the IRC connect status window. Figure 5 shows the main Gaim IM client window, used for chatting or IM.

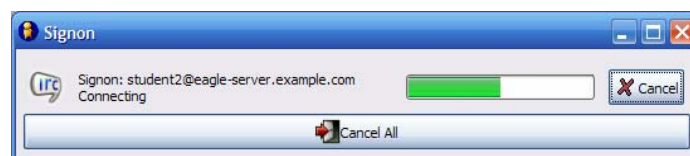


Figure 4. IRC Connect Status Window

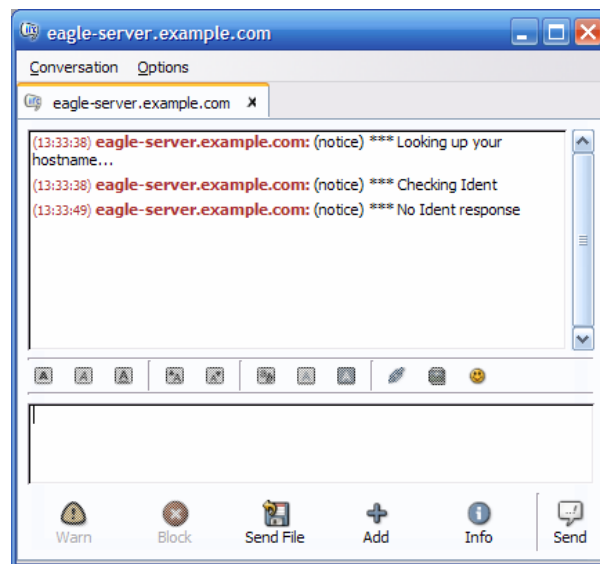


Figure 5. Gaim IRC Client Window

Step 2: Join the Chat.

When the IRC client connects to the IRC server, the status window closes and a Buddy List window displays. Click **Chat**, as shown in Figure 6.

Note: To join a chat channel, the Channel name *must* start with #. If the Channel name is incorrect, you will be in a chat room alone (unless other students made a similar error).

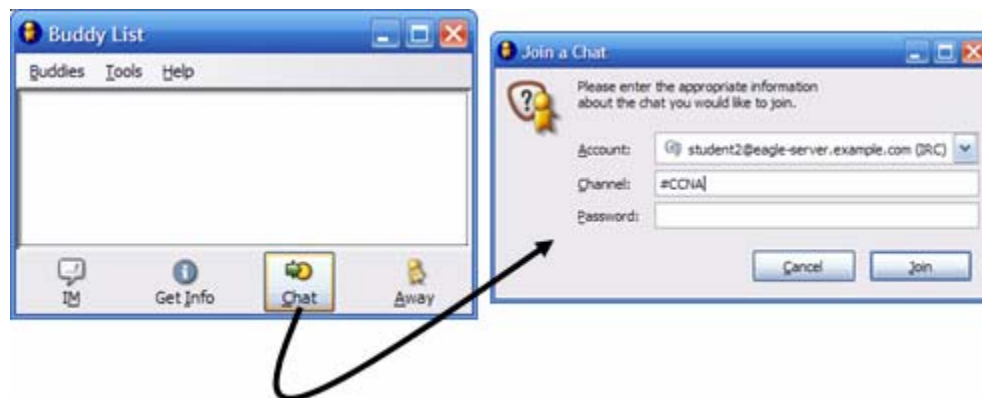


Figure 6. Joining a Chat

Task 3: The Chat Session

Figure 7 shows a brief chat between users *Root* and *student2*. Multiple students can join and interact with each other.

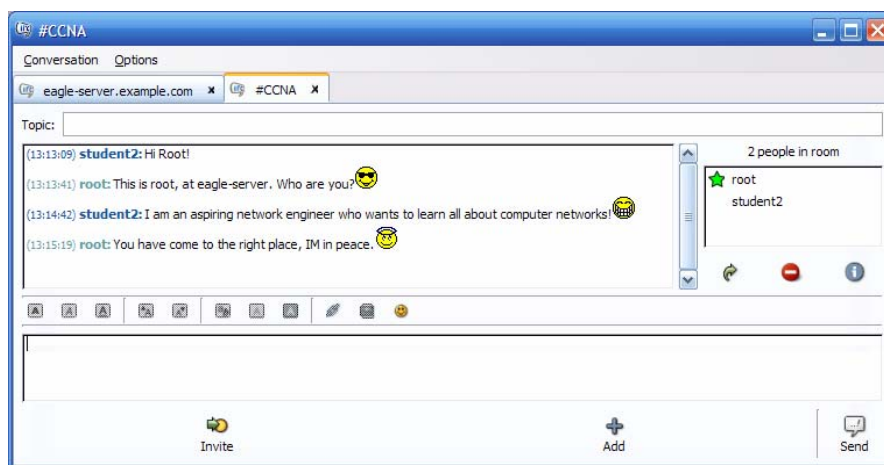


Figure 7. Participating in Chat

During the chat, consider how you—as a parent or network administrator—would manage this type of connection.

Task 4: Reflection

On a network with an Internet connection, the Gaim IM client can be used to connect to several different IM providers. Most teenagers and young adults today are familiar with IMing between friends and sharing files, but the communication between the client and server may not be understood. As a future network engineer, you should understand the social and security issues with IM and IRC.

Task 5: Challenge

While you are connected in chat, transfer files between partners. Use a continuous ping from the host to the eagle server to monitor network throughput. Observe the response time before and during the file transfer. Write a brief description of the network response time—during file transfers and without file transfers.

Task 6: Clean Up

Check with your instructor before removing Gaim and shutting down the computer.