

Enhancement of a Secured Instant Messenger and Message Broadcasting with Voice

John Niyi Iyanda* Olaniyi Abiodun Fayemi
ICT Unit, Joseph Ayo Babalola University, Ikeji-Arakeji. Osun State. Nigeria,P.M.B 5006, Ilesa. Osun State. Nigeria
E-mail: johniyanda@gmail.com

Abstract
Instant Messaging (IM) is a useful communication and work collaboration tool between individuals, groups, or enterprises. Unfortunately, most IM systems lack the needed security mechanism capable of ensuring the secure communications of IM client-client and IM client-server. In order to find a solution to secure IM communications, Secure Instant Messaging and Presence Protocol (SIMPP) was designed and implemented so as to allow users to chat through plain text and also voice call. Open source jabberd software was revised to create a SIMPP server that can work on any operation system platform.
Keywords: Security, Instant Messaging, communication, SIMPP, jabberd

INTRODUCTION

Language is an integral part of human culture. There are many aspects that make up communication, but humans are unique in that we have an organized spoken language, which allows us to communicate on a deeper, more personal level. As we move further into the electronic age, we rely more and more on technology. In the language realm, this technology has taken us from face-to-face communication and letter writing, to inventions such as the telephone, the cell phone, online chat rooms, and finally, one of the newest and fastest growing forms of communication, Instant Messenger. Looking at how quickly IM has spread, we must ask how well it stacks up next to these other forms of communication that we have at our disposal.

Every day, people in the office and at school are instant messaging to communicate with their peers. Use of the technology, which allows for synchronous, virtual communication, has been steadily rising over the past five years (Meredith B. Phillips 2004).). Instant Messaging, also known as online chat, represents the most impressive online revolution since the advent of email. Instant messaging (IM) is a form of communication over the network, either Ethernet or Internet that offers an instantaneous transmission of text-based messages from sender to receiver (Theresa Davey, Anastasia Envall 2000). It can also be described as a set of communication technologies used for text-based communication between two or more participants over the Internet or other types of networks. IM–chat happens in real-time. Of importance is that online chat and instant messaging differ from other technologies such as email due to the perceived quasi-synchronicity of the communications by the users. Some systems permit messages to be sent to users not then 'logged on' (offline messages), thus removing some differences between IM and email (often done by sending the message to the associated email account). In push mode between two or more people using personal computers or other devices, along with shared clients, instant messaging basically offers real-time direct written language-based online chat. The user's text is conveyed over a network, such as the Internet. It may address point-to-point communications as well as multicast communications from one sender to many receivers (Amy Voida, et. al., 2002). More advanced instant messaging allows enhanced modes of communication, such as live voice or video calling, video chat and inclusion of hyperlinks to media.

Instant messaging falls under the umbrella term online chat, since it is also text-based, bi-directionally exchanged, and happens in real-time. IM is distinct from chat in that IM is based on clients that facilitate connections between specified known users (often using a contact list, buddy list, or friend list). Online 'chat' includes web-based applications that allow communication between (often directly addressed, but anonymous) users in a multi-user environment.

IM allows effective and efficient communication, allowing immediate receipt of acknowledgment or reply. However IM is basically not necessarily supported by transaction control. In many cases, instant messaging includes added features which can make it even more popular. For example, users may see each other via webcams, or talk directly for free over the Internet using a microphone and headphones or loudspeakers. Many client programs allow file transfers, although they are usually limited in the permissible file-size.

It is usually possible to save a text conversation for later reference. Instant messages are often logged in a local message history (Erickson T. 2000), making it similar to the persistent nature of emails. The most commonly used tools that facilitate presence awareness are the various Instant Messaging (IM) applications, though there is an increasing trend towards recognising that IM is itself just one (communication-oriented) of many facets of presence management. Instant Messaging is one of the fastest growing areas of the internet for the past few years that allows millions of users around the world to contact friends and colleagues in a

convenient way, with more immediacy than e-mail and without the expense of a phone call (Nardi, B., et. al.,2000).

1.1 A SECURED INTRANET BASED INSTANT MESSENGER DEVELOPMENT

However, most IM systems are not secure. For instance, in the MSN Messenger, any user that has successfully logged into the system communicate in plaintext with other users are not properly protected (Mynatt, E.D., et. al.,1999). In year 2000, IETF released the RFC 2778 standard which defines IM systems to be composed of two types of services, Presence Service and Instant Messaging Service, as shown in Fig. 1. The Presence Service, shown in Fig. 1(a), is responsible for the presence exchanges where the Watcher will receive presence information provided by the Presentation. Presence information includes users' status and willingness to accept or decline a chat session. The Instant Messaging Service, shown in Fig. 1(b), is responsible for the inter-client real-time message exchanges.

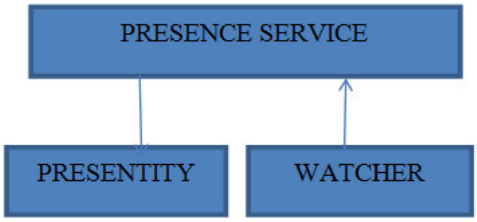

Fig. 1(a) Presence Service

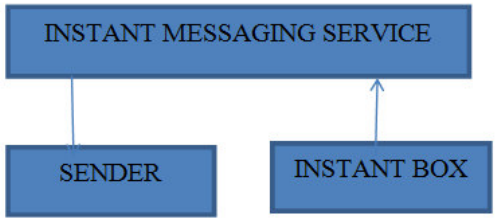

Fig. 1(b) Instant Messaging Service

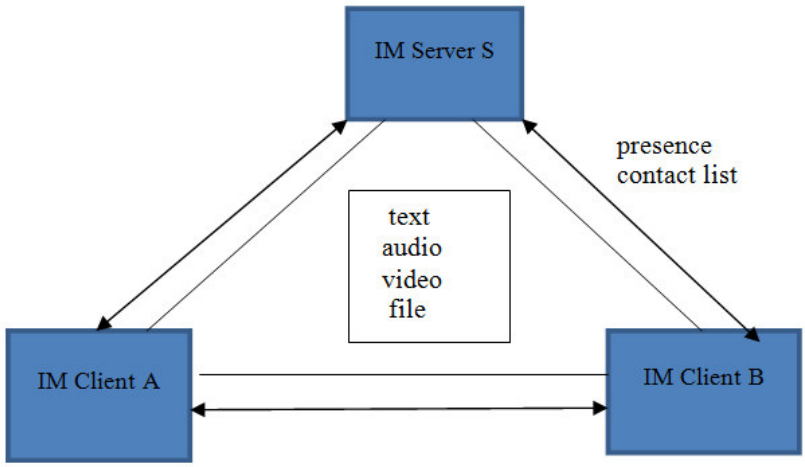

Fig. 1(c) Three-Way IM communication model

Under the IM service models, data communications between any two clients should pass through the server. If the system could only assure client-server communication security, it would overlook the privacy and security considerations of the message contents revealed at the server after message has been transmitted between clients and from clients to the server.

1.2 THE DANGER IN USING SOME UNSECURED INSTANT MESSENGER INCLUDES

1. It announces information, including IP address, about the user and his machine whenever he logs on. Probably one of the more worrying aspects of IM is that it announces the user's actual IP address along with the port it is using. "It [ICQ] sort of hides the IP address of the remote user, but since you char directly with them you can get the IP address by simply running 'netstat' or a related utility". If the user is connected via an "always on" method such as DSL, the IP address is assigned to that user rather than coming from a large pool as in a dial-up connection. This opens up the machine to potential targeting.
2. Just like e-mail, it is a prime target for nuisance messages, or "spam". To be fair, IM providers have thought about this, and are taking steps to minimize this problem. Spam may be considered to be more of an annoyance than a danger. However, it can cause a loss of productivity, especially in a business setting, and there is really no way to completely block these types of messages.
3. The biggest key to file transfers and virus control is the same as for e-mail. First, know who you're getting files from. You must make sure they're from a reliable source. This will reduce your risk, but even more

importantly, you must run anti-virus software and keep it current. Viruses appear and mutate at an alarming rate, and regular updates of your anti-virus software is essential to keeping yourself protected. Finally, and most importantly, make regular backups. With all the care in the world, you could still be hit by a virus. If you can't restore your files, you turn what could have been an annoyance into a disaster.

4. The services that create file servers on user machines can be very hard to trace "… firewalling them is very difficult, short of using non-routed IP addresses and using proxy servers and NAT at the gateways to the Internet you can't block it. Probably the simplest is to monitor network traffic going/coming from workstations and then zero in on the top 10, 20, 100, or whatever and talk to the users. … Scanning your network regularly with tools like nmap and strobe will alert you to open ports".

1.3 PROGRAM ENHANCEMENT METHODOLOGY

The work is based on developing a Local Network Voice Charting machine that can work in organisations which includes schools, government establishment, and other corporate organisations.

To achieve this aim, various requirements to develop the system or software must be identified and can be seen at two levels of abstraction which are:

A) High Level Requirements:
- To develop a real time secured application that allows two or more people to communicate through charting
- To develop an application which allow a user to call another user and communicate to each other through microphone and the speakers.
- To develop a Graphical user Interface (GUI) application that is capable of sharing files
- To develop an application that keep track of messages using message logging so that past messages can be retrieved at any time
- To develop a GUI application that is Multilanguage so that it can be relevant in many countries
- To develop a cross platform support application that is capable of working on an environment like windows, Mac, Linux and Solary.

B) Low Level Requirements:
- To develop an application capable of monitoring the client system in case of an unauthorised user.
- To develop an application that can work without any internet connection due to the fact that it is a local network application.

It is a server client technology in which a system will serve as a server while other system connected to it will be the client. The server system will have a program running on it, and this program is tag a server program. The purpose of this application is to co-ordinate the activities of the application running on the client machine. Other functions of the server application include:

- Taking the log record of the chart activities that is going on each of the client application
- Sending a broadcast messages the all the client that are connected at that particular time
- Gaining control on the whole client computer system by have the ability to shut down, disconnect or reconnect the client system

The client application will be on each system that is connected to the server, which will contain a single use. Each of the users will have the ability to communicate and chart with any other users that he added to his own profile.

The application will also contain a database which will allow each user's profile to be stored separately.

After that completion on the application, a local network will be used to test the functionality and debug the application.

The programming language adopted for this project is java due to his high functionality and its network capability.

Because of Java's robustness, ease of use, cross-platform capabilities and security features, it has become a language of choice for providing worldwide Internet solutions.

MySQL Database will serve as a back end which will contains all the data needed by the application including each user details, users' profiles, server information, log records and all other necessary information. MySQL is choosing due to it robustness and lightness.

The program is designed for a secure transfer of task of information from one client to another through the server. When a client connect to the server the IP Address of the client system is taken and registered after which a protocol is established. The client will now allow the user to enter the name he or she wants to bear. The names will now portrait the user. Then the user on any client server can also see any other available user on their local system. User can now send their information (chart) by either voice or plain text messages.

1. The Login Screen

This is the first frame that is automatically loaded when the user launches to the program. The Login Screen offers the link to the database where all the information about the chatting is stored. This Interface, accept the valid username and the password from the Administrator, and if the username and the password are correct, it will dismiss and allow Admin User to continue his or her operation.

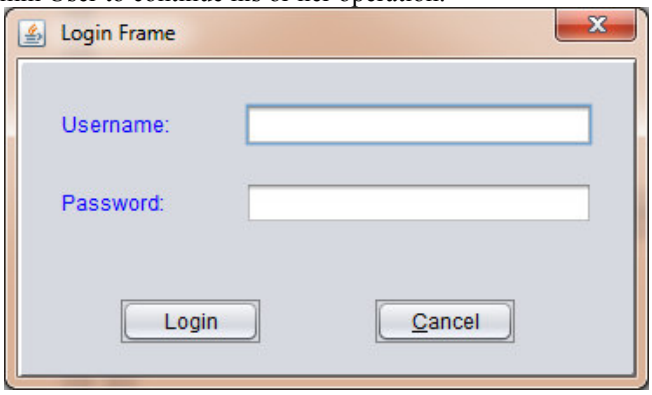

Fig. 2 The Login Screen

2. The Main Frame

The Main Frame is loaded immediately after the Login Page is dismissed. The Main Frame contains major information. This information includes the view list of the connected client system, the list of the online users that are available at the moment. Also the log messages that keep track of transaction that is going on, on both the client and the server system

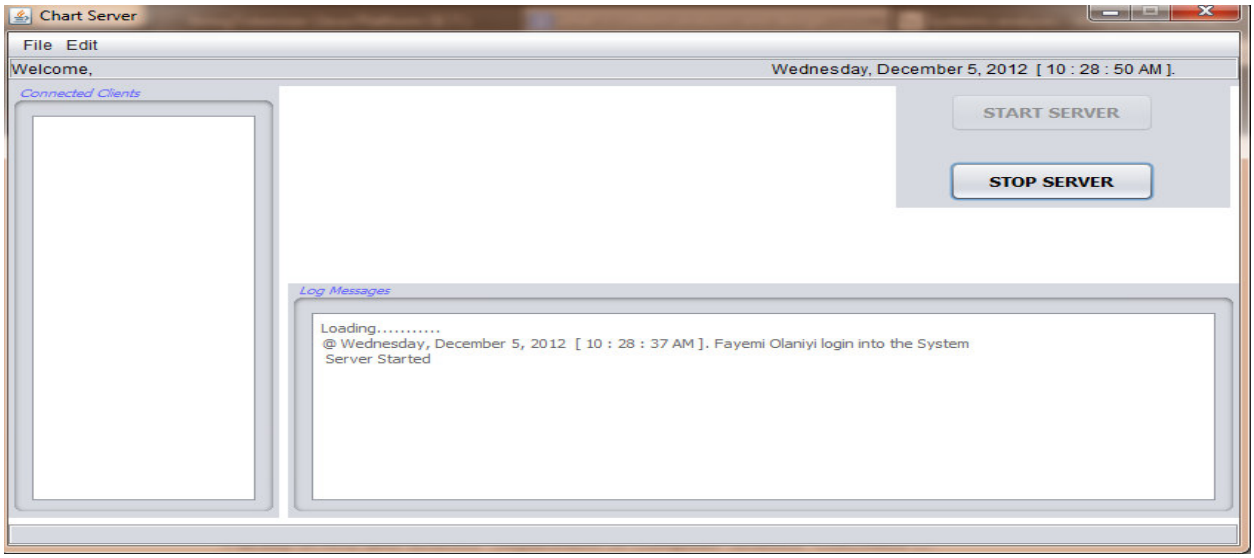

Fig. 3 The Main Frame

3. The Connected Client Panel

This Panel is located at the left hand side of the Main Frame. It allow Admin user to view and control the client system.

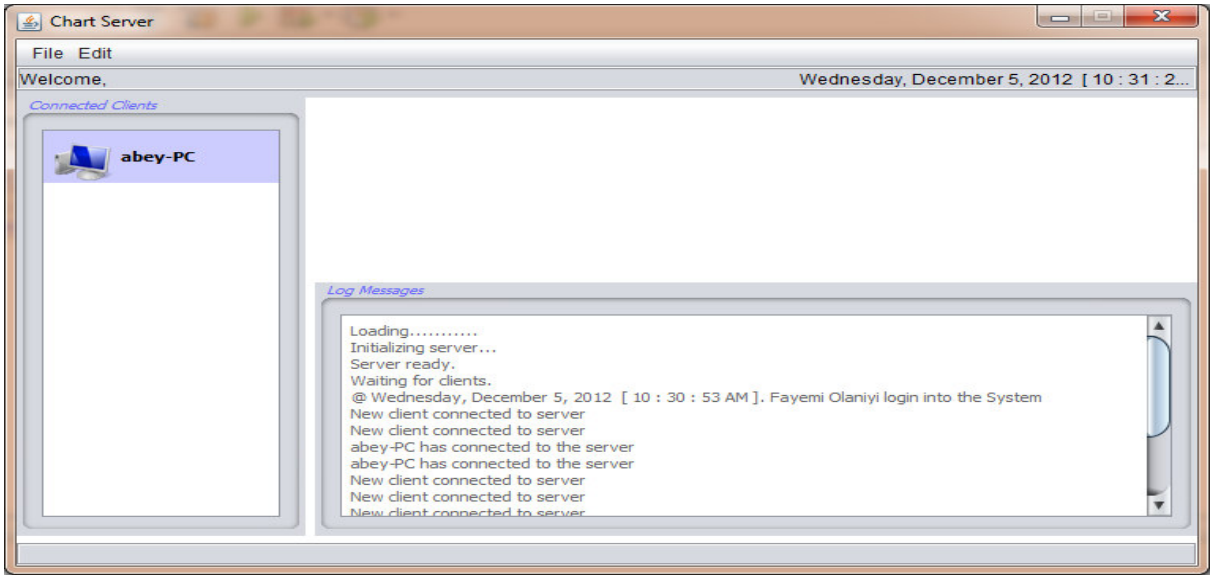

Fig. 3 The Connected Client Panel

4. The Connection Screen

This is Frame contain the Nick Name the user want to use, the location of the server in case the server is more than one and they are on different location. It also contains the fixed Sever Port, and whether the user wants to connect through proxy server. If the user is connecting through proxy server, He must supply the Proxy Host and the Proxy port of the Server System.

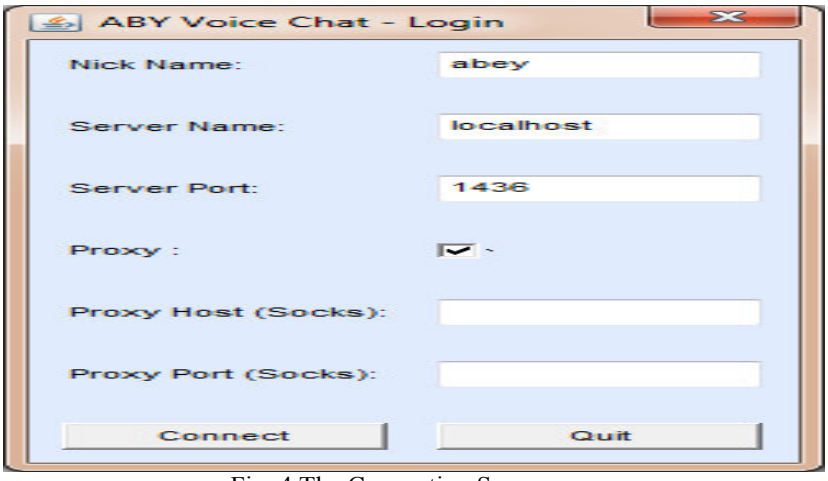

Fig. 4 The Connection Screen

5. The chart Screen

Instant Messaging, like e-mail before it, is poised to dramatically change the way that people communicate (and, indeed, this change has already begun). For business use, I'm not sure that its benefits outweigh its risks. The more users there are the more chances for security holes. It is very difficult to control access and block ports, when they are constantly changing. "The potential for abuse, wasted time and bandwidth, as well as potential legal issues probably outweigh any benefit that might be received from them. They are not oriented to team work in the sense of groupware such as Lotus Notes or Novell Groupwise".

For home use, the risks are lessened. Home machines don't usually have the disk space or the bandwidth to make them the most attractive targets for being used as servers. Also, with a limited number of users, it's much easier to control the things that are being accessed. The only real issue here is that the home user must be savvy enough to be able to make the right configuration choices and maintain the machine through anti-virus updates, patches and backups, which is something that the average home user is not always consistent about doing.

All in all, Instant Messaging programs are very risky and should be avoided if possible. There are risks of exploitation through data, bandwidth, and disk space as well as questions about privacy, legal issues and

liabilities.

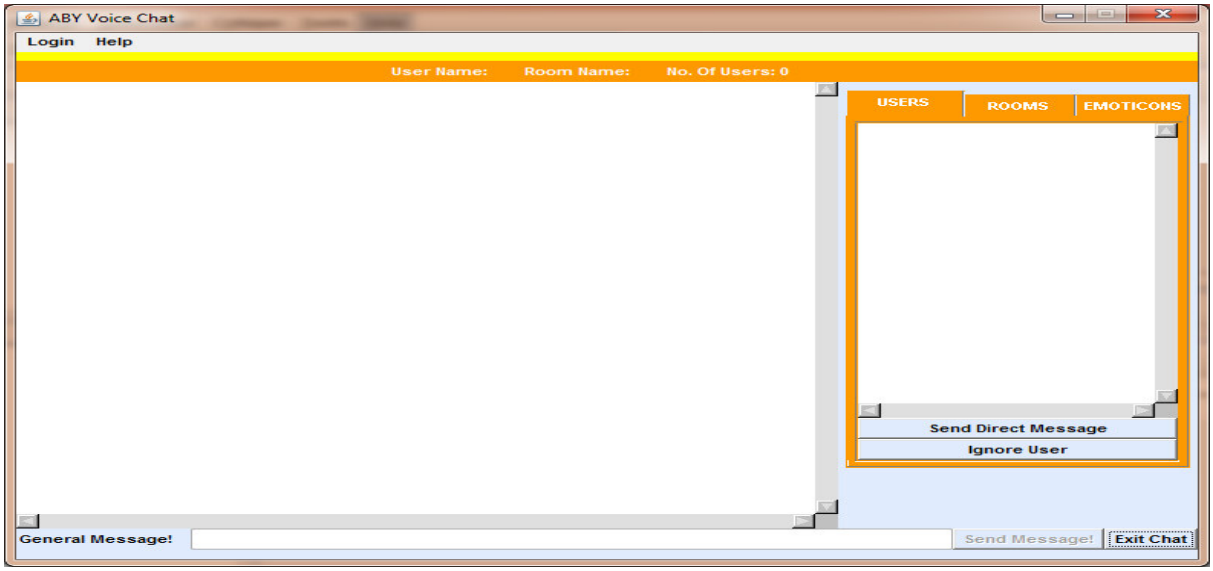

Fig. 5 The chart Screen

CONCLUSION

Instant messaging is becoming an increasingly popular method of communication because of the role it plays in the organisations. However, organizations are facing two problems with IM services; adoption has been driven by the end user and not the top management, and that the client applications were initially built for home users, not businesses - consequently they emphasize functionality over security. With its popularity, the number of security threats that the instant messaging systems poses is also on a rise. A number of viruses have been propagated via instant messengers. Some of the popular ones include: W95.SoFunny.Worm@m, W32.Aplore@mm, W32.Goner.A@mm

W32.Choke,JS.Menger.Worm, W32.FunnyFiles.Worm, W32.Annoying.Worm, W32.Mylife, W32.Maldal (some versions), W32.Seesix.Worm, W32.Led@mm, VBS.Msnb.Worm. The main reason for such threats is the insecure network traffic that it generates. Many popular IM clients use unauthorized ports to ease connection difficulties, which perforates the firewall and provides an alternate conduit for viruses, spam and other unauthorized files. Also, most of the existing messengers do not have sufficient authentication and encryption schemes. There is no guarantee that the message recipient is genuine as it was claim to be, and tracking massages to an actual person may prove to be very difficult. Open connections is another concern. When engaging in file transfers, voice chat, or other file sharing activities, the IM client reveals the users' true IP address. This may cause hacking into host system or denial of service attack. Due to the fact that the application to be develop will run on a local network, the risk and the threat from hacker will be greatly reduced.

REFERENCES

[1] Amy Voida, Wendy C. Newstetter, Elizabeth D.(2002). Mynatt1 When Conventions Collide: The Tensions of Instant Messaging Attributed.

[2] Erickson T. (2000). Making sense of computer mediated communication: Conversations as genres, CMC systems as genre ecologies. In Proceeding of the Thirty-Third Hawaii International Conference on System Sciences. Los Alamitos: IEEE Press.

[3] Mynatt, E.D., Adler, A., Ito, M., Linde, C., & O'Day, V.L. (1999). The network community of seniornet. In Proceedings of the Sixth European Conference on Computer Supported Cooperative Work (pp. 219-238). Dordrecht: Kluwer Academic Publishers.

[4] Nardi, B., Whittaker, S., & Bradner, E. (2000). Interaction and outer action: Instant Messaging in Action. In Proceedings of the ACM Conference on Computer Supported Cooperative Work (pp. 79-88). New York: ACM Press.