INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A Review of XMPP based chat Servers with a vision of Security Enhancement using Cryptography

Poonam Taneja[1], Asha Mishra [2], Pawan Bhadana[3]

[1] M.TECH SCHOLAR, B. S.A Institute of Technology & Management
MDU University Village Alampur , Ballabgarh – Sohna Road, Faridabad -121004 (Haryana) INDIA
mahitaneja0507@gmaill.com

[2]ASSISTANT PROFESSOR, B.S.A Institute of Technology & Management
MDU University Village Alampur , Ballabgarh – Sohna Road, Faridabad -121004 (Haryana) INDIA
asha.mishra@faculty.anangpuria.com

[3]ASSOSIATE PROFESSOR, B.S.A Institute of Technology & Management
MDU University Village Alampur , Ballabgarh – Sohna Road, Faridabad -121004 (Haryana) INDIA
pawan.bhadana@faculty.anangpuria.com

Abstract: *Security has become a major issue into the development of Instant Messaging. A secure chat scheme is readily accessible and very useful to communicate with people that might be anywhere in the world. In this paper security issues related to instant messaging is discussed. In this paper a brief review on has been done on Instant Messaging (IM) and eXtensible Messaging and Presence Protocol(XMPP).This paper also highlights various kinds of security problem of existing public chat server and explores the XMPP specifications and technology. It also provides an insight of various text based encryption methods and helps to decide the optimal method to be used for enhancing IM security with minimum overhead. The proposed approach tries to enhance security of existing open XMPP based chat server*.

Keywords: *IM, XMPP , ENCRYPTION TECHNIQUES ,SECURITY ISSUES OF IM*

1. INTRODUCTION

An Instant Messenger (IM) [1] is a type of communication service over the internet, which enables people to communicate with each other in real-time. Instant Messenger is the private network communication between two users, whereas a chat session is the network communication between two or more users. Chat sessions can either be private , where each user is invited to join session, or public ,where anyone can join the session. Basic functions in IM are the ability to identify users online and to exchange small text messages. IM services are now very popular as an instant way of communication over the internet, especially IM for customers (public), which is also called Chat Interface Module (CIM). It used two faces for communication i.e. security and interpretation .The eXtensible Messaging and Presence Protocol (XMPP), is an open Extensible Markup Language protocol for near-real- time messaging , presence , and request/response services . which has evolved through an open development within the jabber open source community and still under development. XMPP is widely used for instant messaging, voice chat ,text chat, video calls using the XML data[3].Though there were few IM's existing in the market due to their closed services drawback they need new open services IM. Hence XMPP came into picture in which XML is used for streaming .It makes use of client server architecture, where the client access the server over a TCP/IP connection and client uses the XMPP. It has three main components:

1. Core components
2. Security components
3. XMPP for IM and Presence

The security measures consider during the design and development of the targeted secure chat.[3] The secure chats have a permission system to the data that determines if a user is permitted to access it. An idea of a secure data is to provide secure storage of the server data as well as maintaining authorized access for the authorized users also. In order to maintain this level of security, there is a need to design a strong and secured data by implementing data Integrity and confidentially. Some encryption schemes are used to encrypt messages using the public key or private key.

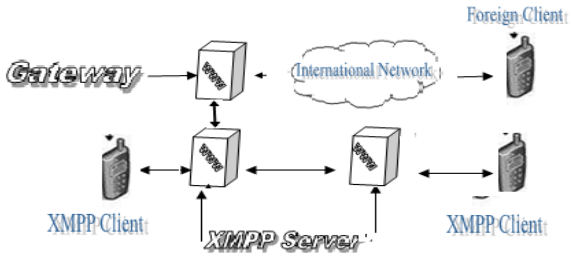

Figure 1: The XMPP Architecture

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

2. IM ARCHITECTURE

Although XMPP is not any specific network architecture it is usually implemented via a client –server architecture where in a client utilizing XMPP accesses a server and servers also communicate with each other . Most communication in IM systems are client – server based messages among users are also typically relayed through the server . If user A wants to communicate instantly with user B , both must log into the same IM services. Messages from A to B will be delivered by the server depending on B's privacy settings.

2.1 Security threats to IM: The evolution of IM system suggests some security and privacy issues.

2.1.1 Insecure connection. Current popular IM(Instant messaging) network lies in open ,insecure connections .During the login time if no security at all then this open the door to many other security vulnerability including denial of service, man- in- the -middle-attacks etc.

2.1.2 Eavesdropping. IM services typically transmit message in clear –text over the public Internet An eavesdropper can intercept messages at various point in the communication pipeline .for example, packet sniffer software can intercept the content of many messages near the IM centralized message routing server.

2.1.3 Identity Theft and Impersonation.

The lack of linking to true identifiers in the IM client makes it difficult to detect identity theft when it occurs. If a identity thief is able to crack a user's IM username and password and log in under stolen name, the victim's IM buddies may not be able to tell the difference.

3. XMPP ARCHITECTURE

The XMPP architecture is composed of three elements, XMPP client, XMPP server, and gateways to foreign networks. Fig-1 illustrates this architecture. A server acts as an intelligent abstraction layer for XMPP communications. Its primary responsibilities are to manage connections for other entities, in the form of XML streams to and from authorized clients, servers and other entities. Connection management and messages routing. A gateway is a special – purpose server-side service whose primary function is to translate XMPP into protocol used by a foreign (non-XMPP) messaging system, as well as to translate the return data back into XMPP.

3.1 XMPP security mechanism

The XMPP system mainly includes four aspects: authentication, authorization and data protection and recognition. Authentication is to determine whether the petitioner can use his request content. Data protection refers primarily to data in the transmission process will not cause any problem, including data confidentiality and integrity. XMPP use authentication and encryption methods to provide coverage of four element of a security framework.

Authentication is the first line of XMPP security, provided sufficient access control for most IM tasks. It accomplishes this with three different algorithms for client authentication:

3.1.1 Plan authentication.

Plain is the first authentication method that provides some level of security .Its primary advantage is the extreme simplicity of implementing it. Plain authentication works by sending a plain text copy of the user's password to the server in the authentication set query. The server directly compares the password to the one stored in the user's account. If they match, the server sends the client an empty result query packet indicating the client has been authenticated with the server. If it does not match, the server sends a standard error IQ packet.

3.1.2 Digest authentication

To avoid sending password as a plaintext, the digest authentication adds an extra step to the process .The server starts its stream using the <stream: stream> packet containing a random session ID string in the packet's id attribute. To generate a digest authentication, you take the session ID from the server's initial <stream: stream > tag and concatenate it with the user's password .The resulting string is then hashed using the SHA-1 message digest algorithm. The drawback of digest authentication is that the user's password must be sent to the server during register protocol as plain text. And the server must store the user's password as plain text.

3.1.3 Zero-Knowledge authentication

The most secure, and most complex method supported by the XMPP protocols is zero-knowledge authentication. The zero-knowledge authentication method is complex and its adoption in servers and clients have been slow because of this. Zero-Knowledge authentication removes the requirement for servers to store the user's password.

3.2 XMPP Encryption Technique

XMPP includes a method for securing the stream from tempering and eavesdropping [1]. This channel encryption method makes use of the Transport Layer Security (TLS) protocol along with a "STARTLS" extension, providing data confidentially and integrity. Encryption helps reduce the threat of eavesdropping. The goal of the TLS protocol is to provide privacy and data integrity between two communication applications. It contains two layers : the TLS Record Protocol and the TLS Handshake Protocol. TLS Record Protocol provides two basic properties:

1) The connection is private, Symmetric cryptography is used for data encryption.
2) The connection is reliable. Because it include a message integrity check using a MAC key and secure hash functions e.g. .SHA, MD5 etc.

4. SECURITY CONCERN FOR IM

The security of the IM is considered when organizing public key systems, conflict to attacks of particular keys from aside. Several attacks are based on hacking of encrypt plaintext using decryption key. So to provide the security of IM architecture here we use XMPP security mechanism to ensure that IM avoids attacks from hackers or unauthorized person.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Following are the security consideration in XMPP:

- High Security provides Certification base authentication is used between both parties.
- Technology implementations for different security features different algorithm are used such as Authentication: Digest MD5Confidentiality: TLS RSA with 3DE, EDE and SHA cipher.
- Base64: Base64 helps to recognize the trusted client and server. This helps is maintain the data integrity and passing correct data.

5. RELEATED WORK

Zhenxing cui*,Zhihua Gu [1] explains threats of Instant Messenger and security analysis of XMPP .Security has become a major disincentive to the development of instant Messaging. This paper focused on security issues related to instant messaging. It firstly introduced IM and XMPP, and then mainly discussed kinds of security threats to IM Systems and the security mechanism of XMPP, lastly, raised several security considerations in implementation of XMPP.

Linan Zheng [2] defines Instant Messenger Architectures and Concepts Instant Messaging (IM) is an Internet-based protocol application that allows one-to-one communication between users employing a variety of devices. Recently, Instant Messaging has already obtained there mark-able success as P2P communication tool. In some places, it already took the place of e-mail as the first choice for long distance communication. In the mobile area, the Short Message Services (SMS) and Multimedia Messaging Service (MMS) also attract thousands of subscribers by the richer and richer set of services. Jabber is the most widespread open source platform, using an XML encoded protocol, especially tailored to provide instant messaging and presence services over the Internet.

Pie Nie [3] defines eXtensible Messaging and Presence Protocol (XMPP), which is the first effort in creating an open standard for instant messaging and presence information. XMPP was introduced by the Jabber Software Foundation (JSF) and formalized in the IETF. This paper explores the XMPP specifications and technology, accompanied with examples of the application program. Both advantages and disadvantages are analyzed. They explain why the XMPP is designed in this way and
How it fits the requirements of the users.

Kuldeep Chouhan and S. Ravi [3] proposed a concept of encryption that prevents a message from unauthorized person to view or modify the message. It used the public key to send messages between users, when message is sent out ,the client programs downloads the public key and encrypt the intended message and then applies digital signature which is created with the private key and then sends the encrypted message out. when the packet is received by a specified person ,the client program automatically applies the private key on the text and output the message so that the user can see it decrypted with a public key. The RSA algorithm was utilized in encrypting and decrypting small messages sent between user .A secure chat program allow for two users to connect to the server and encrypt the message with each other's public keys.

Mohd. Kamir yusof,,Ahmad Faisal Amri Abidin and Mat Atar Mat Amin [4] presents secure instant messenger architecture. In this paper hash algorithm was applied to the secure module. The purpose of this encryption is to ensure that unauthorized person cannot view the original data or information on the network. The security of the IM is considered when organizing public key systems, conflict to attacks of particular keys from aside. Several attacks are based on hacking of encrypt plaintext using decryption key. So to provide the security of IM architecture here we use XMPP security mechanism to ensure that IM avoids attacks from hackers or unauthorized person.

Dr. Stephan Rupp, Linan Zheng [5] This paper gives some basic concepts of IM System and analyzes the basic architecture, protocol, and communication procedure based on Jabber to briefly describe the working flow of typical IM system. At the end, by comparing ICQ, MSN and Yahoo Messager - 3 most popular IM software in the nowadays market, we can get a deeper understanding of their features and working principle. Instant Messaging (IM) is an Internet-based protocol application that allows one-to-one communication between users employing a variety of devices. Recently, Instant Messaging has already obtained the remarkable success as P2P communication. Jabber is the most widespread open source platform, using an XML encoded protocol, especially tailored to provide instant messaging and presence services over the Internet.

6. PROPOSED WORK

In this we analysis there are still some limitations of existing chat server and to optimize the problem of existing chat server we use secure chat server.

6.1 Disadvantages of Existing Chat Server:-

1) Chats in most cases are routed through a server system, where the services is provided and that is a single point where all messages can be intercepted [3].
2) Chat programs can provide an open avenue of attack for hackers, crackers ,spies and thieves. Eavesdrop: intercept messages.
3) It does not provide protection against faking to be the client talking to another. Removing sender or receiver, inserting himself in place.

6.2 Proposed Approach : Secure Chat Server

In the literature study analysis of securing chat data is necessary to verify the clients. The most constantly approach is request for a client name and password to authenticate the client. In this section. Secure chat program used in SEC application fig. 2 shows the communication model for secure chat server.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

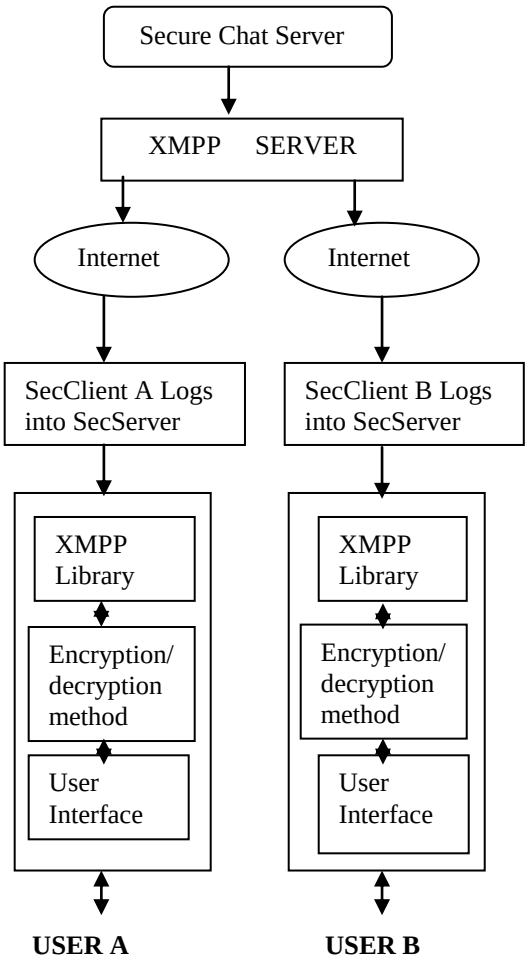

Figure 2: SEC Communication Model

It sets up the shared secret between the two SEC client, which is used to share the cipher text using encryption methods. When we add some extra features to the existing chat sever then the performance of our work will enhance.

7. CONCLUSION

In this paper, we review the Instant Messenger and its security threat that does not provide protection against faking to be person client is talking to another. And use of XMPP protocol for IM that helps to know how the security enhanced to keep the integrity and confidentiality of data. In this paper, we propose a new approach in which we develop the new secure encrypted chat process using XMPP communication model with additional encryption module for data security. In encryption technique, interception occurs but, the interceptor cannot decipher the message. In next paper, A new secure chat server is implemented to make the IM application more secure for data transmission without any key management scheme.

REFERENCES

[1] **Zhenxing cui*,ZhihuaGu,"Threat to IM and Security Mechanism Ananlysis of XMPP", in proceeding of conference on department of computer science & technology wuhan university of technology, wuhan.**

[2] **Pie Nie "An open standard for instant messaging:eXtensible Messaging and Presence Protocol(XMPP)", proceeding of TKK T-110.5190 Seminar on Internetworking, 2006-05-4/5.**

[3] **Kuldeep Chouhan and S. Ravi "Public Key Encryption Technique Provide Extreme Secure Chat Environment", proceeding of International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 510 ISSN 2229-5518.**

[4] **Mohd. Kamir yusof, Ahmed Faisal Amri Abidin and Mat Atar Mat Amin "An Architecture For Securing a Private Instant Messenger", proceeding of Smart Computing Review ,vol.2,no.1,Feb 2011.**

[5] **Dr. Stephan Rupp, Linan Zheng "Instant Messaging: Architectures and Concepts" ACS Seminar –Instant Messaging: architectures and Concepts.**