Journal of Computer Science 5 (9): 661-665, 2009
ISSN 1549-3636

A Platform to Develop a Secure Instant Messaging Using Jabber Protocol

Ghossoon M.W. Al-Saadoon
School of Computer and Communication Engineering, University Malaysia Perlis,
Kompleks Pusat Pengajian Seberang Ramai (Blok A) No. 12 and 14, Jalan Satu,
Taman Seberang Jaya Fasa 3, P.O.S. 02000 Kuala Perlis, Malaysia

Abstract: Problem statement: Open Source technologies are interesting in that they allow free experimentation and integration by anyone and anywhere. A Jabber user can control presence with very little effort. Another user, regardless of external platform, must subscribe to your presence. You have the choice of rejecting or accepting the subscription at the time it is submitted. **Approach:** Other applications of this system were yet to be discovered. Jabber is a work in progress; the community learns and creates applications of the protocol/platform on an almost daily basis. This study aimed to implement a security algorithm for developed instant messaging. **Results:** The objective was to make sure that flow of data from client application or computer is not tapped by a hacker and also to make it difficult for a network data sniffer to explore the situation. In this study there were many aspects must be understood such as: Jabber protocol, programming language and security aspect. For this reason it was proposed to develop a new secure connection and makes sure that the connection between clients and server is safe and secure when the instant massage had been transferred using jabber protocol. **Conclusion/Recommendations:** To develop a new secure connection for instance message using jabber protocol or other names, the Extensible messaging and presence protocol had been used. To make it secure the open secure socket layer will be used for general-purpose encryption. In this study the methodology used to solve security threats like: The ability to control access to IM applications, audit and archive IM conversation, the ability to lockout unauthorized IM and peer-to-peer file sharing connections and Encryption.

Key word: Security aspect, XEP, XMPP, secure socket layer and PSI

INTRODUCTION

This study is to secure a connection which is initialized by Instant Messaging based on Jabber protocol. When a user a sends some text to user B, the text will be encrypted by capture the text before being released into network let say, Internet. A certain algorithm will be used to encrypt the text and produce cipher text which is cannot be read by unauthorized user after encryption took place. The cipher text will pass back for transmission line and go to the destination (Jabber server). Server will decrypt the cipher text back and look for user B. This called as client-server security. Then after the server passing the plain text, it encrypts it back, then passes to user B. User B decrypts the cipher text from server to gain the plain text. This also called as server client security.

The scope of this study is to make sure that the connection between clients to server and also server to server is safe and secure. The Open-Source Software used (OpenSSL) is used to develop such a system which is safe yet cost free. Recommendations about hardware also discussed in this project in making the line are safe. To make sure that this encryption process succeeds, a program called Ethereal has to be used. Ethereal can sniff out data packet and check either the data has been encrypted or not. An algorithm that been selected must be strong enough from being hacked, simple to run and no utilizing lots of CPU power.

Problem definition: Many encryption algorithms (encrypt instant message) has been hacked of advancement in modern technology because Data Encryption Standard (DES) uses (2^55) keys was being unused, need a strong algorithm that can avoid hacker's, so the new encryption method Riajendeal is implemented in stand alone by listen on port (5222), which is a general port used by Psi-Jabber client. The main reasons to use Jabber Protocol are Jabber client which is the best to use in aspect of memory usage, low optimization Central Processing Unit (CPU) power, Graphical User Interface (GUI) and stability. There is a

need for a strong algorithm that can avoid hacker's attack. The algorithm should be balanced in security, performance, affiance and easy to be implemented.

Technologies used: There are four basic technologies that included inside Jabber itself. Those technologies are Jabber Identification (JID), Transport, XMPP Extension Protocol (XEP) and Extensible Messaging and Presence Protocol (XMPP):

- JID: Look likes special identity for Jabber client or user among themselves in the Jabber network. For other Instant Messaging System, JlD can be compared as the "buddy name" or Yahoo and MSN call its user as participator[1]
- Transport: It is a server side plug-in that runs inside the roster. It trying to keep the connection to non-jabber networks like The Microsoft Network (NlS-.r*) Yahoo Messenger (Y N4). Internet Relay Chat (lRC) or I Seek You (lCQ). It actually does two functions; it connects into other network and updates the activity to the liberator. Needs to proridean1, transport about login and password. Transport is types of plug-in which there are many transports for certain network[2]
- XEP: Shorts XMPP Extension Protocol. It mentions exactly how certainty feature so those X\IPP protocol should be implemented. For programmers there are plenty of XEPs as a guideline. XEP also refers as Jabber Extension Protocol (JEP)[3]
- XMPP: Stands for extensible messaging and presence protocol. Also refer as Jabber[4-6]

MATERIALS AND METHODS

Jabber Protocol was developed with security concerns. This methodology put to gather all the security features of Jabber. An Instant Message needs a lightweight, real-time communication protocol to support real-time information capabilities, like (IM), conferences and video conference, news and file transfer. An Instant Messaging needs to provide the availability expected by users and the security that protect privacy, information and to meet the standard requirements.

The main advantage of Jabber protocol is Open-Source, secure and safer, standardizes and can be extensible. Because of the open-source design, Jabber protocols are developed and got improved by thousands of experts and developers. Even university students also took part. After that, there are lot of open-source clients and servers available on the Web. The design architecture of Jabber system is shown in the Fig. 1.

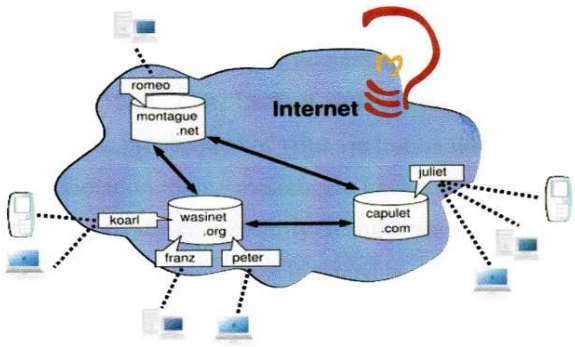

Fig. 1: Ghossoon MW): A typical jabber messaging system

Jabber protocols were approved by the Internet Engineering Task Force (IETF) under the name of Extensible Messaging and Personal Protocol (XMPP) as RFC's 3920-3923, which defining about the Extensible Markup Messaging (XML) streaming protocol including security and basic function of IM.

Security threats on network: To make sure the instance message for uni-map more secure and safe for use so the identification on the network threats are:

- Backdoor Trojan horses, viruses and worms that propagate using instant messaging. IM have a contact list and alerts when a contact comes online. This comes handy for a malware to propagate itself, as this is an easier and sure-shot way to find a victim, than generating random IP address. File sharing, desktop capture and other features provided by messenger also result in vulnerabilities
- Data theft, most of the existing popular IM (Yahoo, AOL, MSN, ICQ) do not provide encryption
- Man-in-the-Middle attack, even encrypted packets may be vulnerable to sniffing attacks and ARP spoofing
- Denial of services attack, one such way of doing this is by flooding a user with large number of messages, especially with graphics (as in emoticons)
- Privacy violation, some messengers have a feature of appearing 'invisible'. This is a privacy-cum-security feature, in the sense that nobody (read: Hacker) is alerted when a user is signed in using invisible mode. But there are tools that find out if a user is invisible (by evoking ACK packets by sending empty packets). This is clearly a privacy violation and must be prevented

The need for secure IM application for Internet usage has created a new market for enterprise IM solutions.

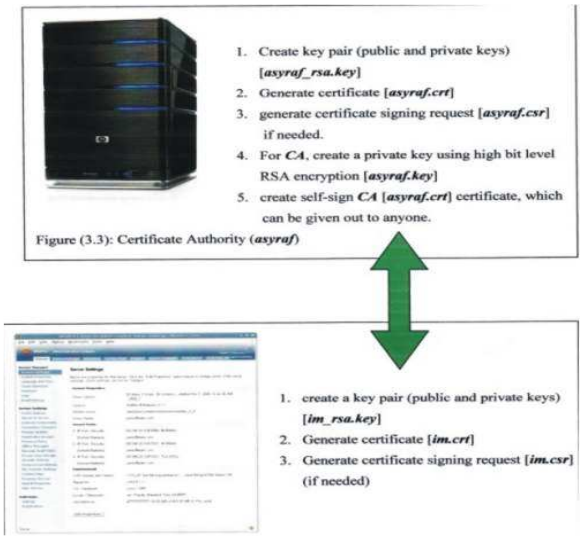

Fig. 2: (Ghossoon MW): Methodology design for SSL connection

These solutions offer those features to provide security:

- Allowing organizations to be able to control the access to IM applications
- Audit and archive IM conversation
- Anti-virus checks, content filtering and anti-Spam protection
- The ability to lockout unauthorized IM and peer-to-peer file sharing connections
- Encryption
- Lock out unauthorized IM and peer-to-peer file sharing connections. Figure 2 explains the methodology design for SSL

Implementation and system design: The design of the UniMap system (implemented in the University Malaysia perlis-unimap-internet instance messages) which consists of main component of Jabber Protocol server and the step to implement the transmission of the instance massage as the following:

Psi jabber client: By referring at Jabber website, Psi was chosen as a client and installed into Window based personal computer. Psi makes use of Qt library for GUI. As for the security features, Psi uses QCA, a crypto QAPI (Application Programming Interface) that supports SSL/TLS, SASL, RSA, hashing, ciphers and so on. Installing Openfire Jabber server into PC then configure it using simple integrated database. Then connect the Psi client initialize the server then registering as new user.

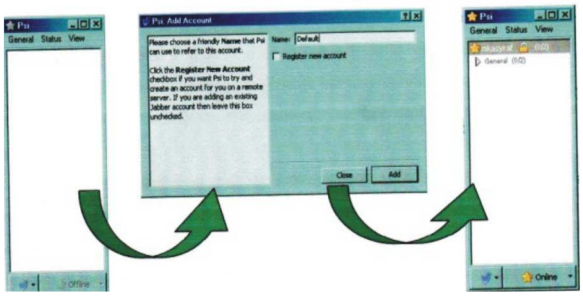

Fig. 3: (Ghossoon MW): Registering new user

Algorithm to add new user:

- Start PC
- Login OS
- Login server and client
- Secure socket layer connection
- Verify the connection
- Registering a new user by click general.
- Account setup
- Add a new user
- Write the name or whatever user wants
- Click ADD then
- Check the verification and
- Finish on how to add a new user

The lock icon shows that the link between client and server is encrypted using SSL technology, as shown in Fig. 3.

Data packet sniffer: Last stage is using Ethereal or Wireshark. It is open-sources packet sniffer computer application. It is used for troubleshooting network, analysis, software and communications protocol development and education.

The function Ethereal or Wireshark provides is same Tcpdump, but it has GUI so it easier to use. Ethereal or Wireshark uses the cross-platform GTK+ widget toolkit and is cross-platform, running on variety computer operating systems like Lunix, Mac OS X and Windows.

Setting up Jabber server and algorithm: The step to setting and implementation of Jabber server as following:

- First step at all, configure the Jabber server. This server is build based on Java language programming. The Openfire installer was run and the application was installed to c: \program files\openfire as default
- Second was set the database using HSQL database engine driver

- Web -based, "wizard" driven setup and configuration tool is built into openfire
- Then simply launched the openfire and used a web browser to connect to the admin console
- The default port for the web-based admin console is 9090. The following URL will usually work: Http:11127.0.0.1:90rz9r0r
- Then connect to the administration web-based panel immediately
- The Openfire installer created a shortcut to a GUI (graphical user interface) will be provided in start menu once installed it. Or run Openftre server by click on Openfire.exe in the directory/ bin in the Openfire installation folder
- Once launched, it guided to automatically open the Mozilla Firefox (maybe vary on other) to the http://127.0.0.1:9090 to finish configuration the server

JDBC driver: Java Database Connectivity (JDBC). Openfire bundles HSQLDB as its embedded database. It was chosen because it has a simpler database and can be configured via the Openfire installer. Because HSQLDB is embedded in Openfire, so there is no need to download the JDBC driver separately. Values for the config file are.

Setting Jabber security: To make the server more secure and to make sure that Secure Socket Layer (SSL) is a function as usual. Secure Socket Layer (SSL) is the most common used protocol in the Internet. For more convenient, OpenSSL was used because it is open source and can be used for the OpenJire server. In this project, there were two sides who were CertiJicate Authority (CA) and the OpenJire server. For CA, there are a public key, a certificate and a private key needed to sign other's public key certificate. For other side, which is the OpenJire server, there should be a public key, a certificate, A CSrt and also a private key. There are few settings available for administrator to choose either to use the secured connection or not.

Open SSL-generating RSA private and public keys using command prompt: The step to generate RSA using command Prompt. It was generating a pair of RSA private key and public key, in this case, named as asyraf_rsa-key. The asyraf-rsa key shows RSA PRIVATE Key. Actually it was both public and private key. The command for generating the key pair of RSA private and public keys, (Fig. 4).

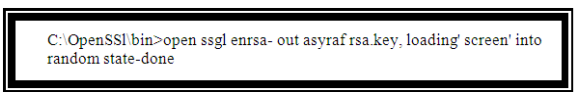

Fig. 4: (Ghossoon MW): Command for generating the key pair of RSA

Key tool-generating keys using "Keytool" using Java command line for openfire server: To make it easier assume this server as “im“hence its domain's name as used for research. From the study tells that "Keytool” doesn't offer the self-signing certificate function. So it must start to generate its own private key and save it in a 'keystore' file. The command that used is keytool-genkeypair. After did it, it must be checking either it already save the private key into the 'key store'.

RESULTS

From the analysis of the results that may be extracted.

In this study "A secure instant messaging" used the Jabber protocol because it is secure based on its implementation of Secure Socket Layer (SSL).

SSL connection has been initialized by generate appropriate certificate and install the certificate into the user who needs security' Fig. 5.

The main advantage for using Open SSL because it can generate certificate and signed certificate as a Certificate Authority. Open SSL consists a lot of encryption classes.

The certificate that been generated by OpenSSL can be used as trusted certificate. The certificate is in X.509 format. It shows who is signing the certificate and what the subject is and how long the validation period is Fig. 6.

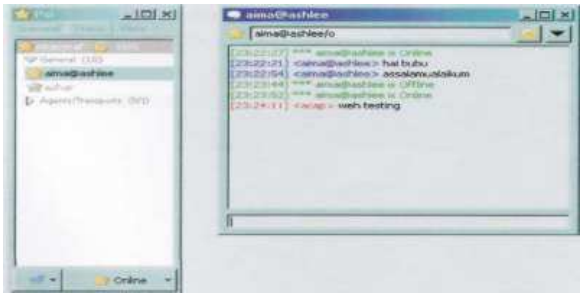

Fig. 5: (Ghossoon MW): Psi Jabber client running and having a chat

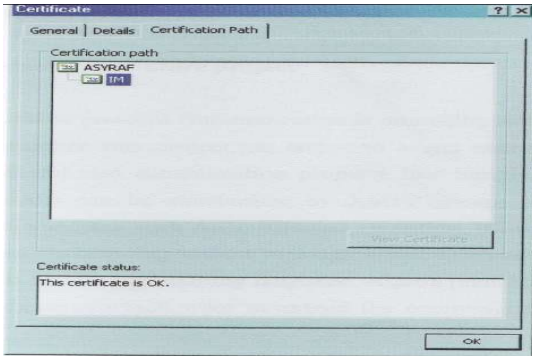

Fig. 6: (Ghossoon M.W.): Certificate

DISCUSSION

When applying jabber protocol in Microsoft Window XP, it will be much easier because of its graphical user interface and its dependency on command line like Linux except for Open SSL. Jabber protocol has many programs to support and keep updating. Patch also available to fix any bugs if there was problem. So the control access of IM is audit and archive. To sniff the unauthorized IM (i.e., hacker) for peer-to-peer file sharing connections and Encryption.

The Jabber Protocol has the flexibility to connect to the other Instant Messaging network. By using certain plug-in, jabber client can be connected to (Google talk) GTalk, AOL, Instant Messaging (AIM), The Microsoft Network (MSN) and Yahoo! And also I Seek You (ICQ).

The data of instant messages are encrypted when the connection is satisfied using the data packet sniffer. The instance message for unimap are more secure and safe for identification on the network threats.

CONCLUSION

The conclusion of this study is gaining the objectives and satisfying results to connect between the client and server using OpenSSL:

- The Jabber Protocols have the flexibility in connecting people in secure way
- Applying the Jabber protocol into the Microsoft window XP to be easier than Linux except for OpenSSL
- The data of instant messages are encrypted when the connection is satisfied using the data packet sniffer. The main advantage for using OpenSSL is the ability to generate certificate and signed certificate as a certificate authority
- Psi jabber client can be customizing by using Qt and gives developer many ways on how to branding it

For the feature works and to strengthen this study, an end to end encryption also the SS|/TLS and also authentication property like Simple Authentication Security Layer (SASL) can be standardize by XMPP group.

Also can use the algorithm to be implemented such AES; Rijndael algorithm, Blowfish.

REFERENCES

1. 2007-2008, Trademark of Jabber.
2. Wynkoop St, Denver, 2002. Advantages of Jabber as a Platform for Developing Collaborative Applications. Jabber. http://www.jabber.com
3. Lee, J., 2004. Jabber: An open protocol for XML messaging presenters. Proceeding of the Dan Gunter and DSD Department Meeting, Jan. 9-9, pp: 1-16. http://acs.lbl.gov/DSDlocal/DSDMeetings/dan-jabber.pdf
4. Softpedia™, 2001-2009, Psi-55917.pdf
5. Hancke, P. and Loesch, 2003. Protocol polymorphism-using polymorphism to present different protocols to different clients in a chatserver. http://www.psyced.org/files/protocolpolymorphism.pdf
6. Mark Yoshikawa, T., 2002. Integrating jabber beans with java servlet technology. http://www.hpl.hp.com/techreports/2002/HPL 2002-139.pdf