ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

SILC-A SECURED INTERNET CHAT PROTOCOL

Anindita Sinha[1], Saugata Sinha[2]

Asst. Prof, Dept. of ECE, Siliguri Institute of Technology, Sukna, Siliguri, West Bengal, India [1]

Network Engineer, Network Dept, Ericsson Global India Ltd, India[2]

Abstract:-. The Secure Internet Live Conferencing (SILC) protocol, a new generation chat protocol provides full featured conferencing services, compared to any other chat protocol. Its main interesting point is security which has been described all through the paper. We have studied how encryption and authentication of the messages in the network achieves security. The security has been the primary goal of the SILC protocol and the protocol has been designed from the day one security in mind. In this paper we have studied about different keys which have been used to achieve security in the SILC protocol. The main function of SILC is to achieve SECURITY which is most important in any chat protocol. We also have studied different command for communication in chat protocols.

.

Keywords: SILC protocol, IM, MIME, security

I.INTRODUCTION

SILC stands for "SECURE INTERNET LIVE CONFERENCING". SILC is a secure communication platform, looks similar to IRC, first protocol & quickly gained the status of being the most popular chat on the net. The security is important feature in applications & protocols in contemporary network environment. It is not anymore enough to just provide services; they need to be secure services. The SILC protocol is a new generation chat protocol which provides full featured conferencing services; additionally it provides security by encrypting & authenticating the messages in the network. The security has been the primary goal of the SILC protocol & the protocol has been designed from the day one security in mind. The network topology attempts to be more powerful than IRC network.

Why SILC has been Used:- We are using different types of chat protocol but they have some weakness. We are going to discuss them now.

- **Instant Messaging (IM):-** It is a collection of technologies used fro real time text based communication between two or more participants over the internet or other types of network. It provides text, voice, video messages.
  Weakness: it has large security risks
- **Internet Relay Chat (IRC):-** it is form of real time internet text messaging or synchronous conferencing. IRC is mainly designed for group communication.
  Weakness: IRC connections are usually unencrypted and typically span long time periods, they are an attractive target for crackers.
- **Extensive Messaging & Presence Protocols (XMPP):-** it is an open standard communication protocols for message oriented middleware based on XML. In XMPP, there is a system approach of development federation protocol is an extension to the XXPP protocol.
  Weakness: In XMPP, presence data are overhead & binary data transfer is inefficient.

II.THE SILC PROTOCOL

SILC is a modern conferencing protocol, provides rich conferencing features with high security. Many of the SILC features can also be found in IM style protocols. SILC removes the need to make such distinction between two protocol styles. It also supports multimedia messages and can also be implemented as a video & audio conferencing system. The protocol is also compact & robust and suites well for mobile environments where the low bandwidth sets special requirements for protocol. The packets & messages in the SILC network are always encrypted & authenticated. It assures that end user cannot even accidently send unencrypted messages while that it is encrypted. This is one of the problems of most of the other chat protocols that provide so called plug-in encryption. They are not secure by default but try to provide security by applying external security protocol such as SSL over the insecure protocol. Another problem is also that the external protocols tend to leave the network only partly secured; usually only two points in the network are secured with SSL, while SSL is not enough to provide security for a chat network as a whole. SILC is secure environment of mutual distrust

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

between entities in the network. It is possible to encrypt messages end to end, s that only the sender and the receiver is able to encrypt & decrypt messages. The SILC network forms so called hybrid ring-mesh network at the router level & star network at the server level. This sort of network topology allows better scalability & faster delivery of packets than traditional spanning tree style network.

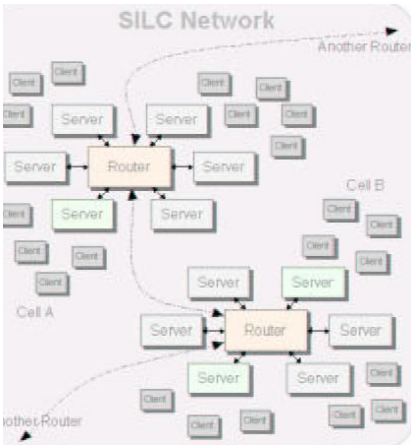

Fig-1:SILC network

III.DIFFERENT TYPES OF SILC PROTOCOL

- *The SILC packet protocol* is a secure protocol is a secure binary packet protocol. The protocol provides secure binary packets & assures that the contents of the packets are secured & authenticated. All Packets in SILC network are always encrypted & their integrity is assured by computed Message Authentication Codes (MAC). Each Packet type usually has a specific packet payload that actually defines the contents of the packet. As per the diagram, the SILC packet is constructed from the SILC packet Header that is included in all SILC packets, data area that includes the packet payloads & MAC area which assures the integrity of the packet. Entire SILC packet is always encrypted, except for the MAC area which is never encrypted.

IP HEADER	TCP HEADER	SILC HEADER	PACKET DATA	MAC

Fig-2: SILC packet format

- *The SILC Key Exchange Protocol (SKE)* is used to exchange shared secret between connecting entities. The result is a key material used to secure the communication channel. The purpose of the SKE protocol is to create session keys to be used in current SILC session. This is the first protocol that is executed when creating connection to, for example SILC server. All the other protocols are always executed after this protocol. This way all other protocols are secured since the SKE creates the session key that is used to secure all subsequent packets. The security properties that are used in the SILC session are also negotiated during the SKE. The security properties include ciphers, hash functions, public key algo, and HMAC functions.
- *The SILC Connection Authentication Protocol:-* Purpose of SILC connection Authentication Protocol is to authenticate the connecting party with server or router. This protocol is executed when for example client connects to server. It is also executed when server connects to router. Its other purpose is to provide information for the server about which type of connection it is. The type of the connection defines whether it is client, server or router. If the authentication is based to public key then for example the client signs data with its private key and sends it to the server. The server then verifies this signature by using the client's public key. The packet is also encrypted in the case of public key authentication. If it is successful the connection is granted.

IV.ENTITIES OF SILC NETWORK

- **Clients: -** A Client is a piece of software connecting to SILC server. The software is usually run by the end user, a real person that is. They are used to actually engage the conversations on the SILC Network and they can be used to execute various SILC command. The clients are distinguished from other clients by unique Client IDs, is not being used by end user. The end user usually selects a preferred nickname to other users on the network. The nick names are not unique, they can be multiple no. Most of other chat protocols have unique nickname. This is where SILC differs from most of the other chat protocols. When client connects to the server the SKEP & SCAP are

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

executed. The result of the SKE protocol is the session key that the client & server use to secure their communication. The session key expires periodically & the rekey process can be executed with or without the Perfect Forward Secrecy.

- **Servers: -** Server's forms the basis for the SILC network by providing a point to which clients may connect. There are two kinds of servers in SILC; normal Servers & router Server. Normal Servers connect to router server, they are not directly connected to other normal server; however clients may connect to router server as well as the servers are distinguished by other servers in the network by unique server ID. There cannot be multiple same Server IDs in the SILC Network at the same time. The servers keep track of local information, knows all locally connected clients & it does not know any global information; however it may cache that information it it was queried. When server connects to its router the SILC key exchange protocol & SILC Connection Authentication Protocol are executed, just like when client connects to server. The SKE results in to the session key that is used to secure the authentication server to the router.
- **Routers: -** The router servers are a server that actually handles the message routing in the network. They are however also normal servers and they accept client connections. Each of the routers in the network is called a cell, which has only one active router but several servers & clients. The switch to the backup router should be transparent & only local connections to the primary router are lost. Router server knows local & global information considering the cell as local & outside cells as global. For example, when client sends WHOIS command, the server may query the information from the router, and if the router does not know all the details that the WHOIS command requires it can query the information from the router or a server which knows all the details, it may cache that information. The router in the network forms a ring[fig-1]. Each router has a primary route to other router in the network. Finally the ring is closed by the last router using the first router in the network as its primary route.

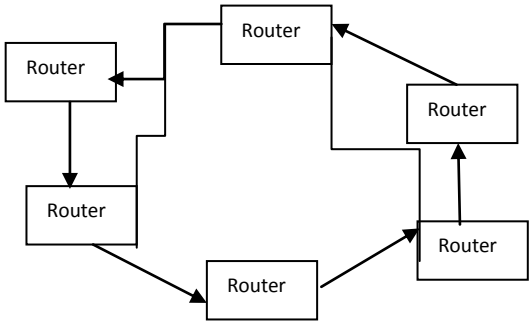

Fig-3: ——— = Secondary route
→ =Primary Route

CHANNEL: - Channel is the place where group of people can engage conversation. The channel is created when first client joins to it, and the ceases to exist when the last client leaves it. When channel exists, any client can reference it using the name of the channel. Channels can have two types of operator that can administrate the channel which are channel founder & channel operator. Channel founder can operate all of the channel's modes and its privileges cannot be removed by any other operator on channel and channel founder. Channel operator is operator that can operate most of the channel's mode and administrate the channel & it can operate all modes which are strictly reserved for channel founder.

- *Channel Message Delivery:* All clients that have joined the channel can send messages to the channel. All channel messages are secured & authenticated by channel key. The channel key is generated by the server when the channel is created; a client joins or leaves the channel. By this process it can prevent to encrypt or decrypt old or new messages. Channel keys are cell specific in the SILC network, that have joined on a particular channel have also own key for the channel, which is not shared by other cells in the network. When message is sent to the channel by a client, it is encrypted with the current channel key in that cell. When the channel messages are sent between routers they are first decrypted with the current channel key, re-encrypted with the session key shared between the routers. The clients who have joined the channel always know the current channel key and can decrypt all channel messages they receive. This method of the channel message delivery is the default way to send channel messages in the SILC network. If the clients on the other hand can trust their servers and routers in the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

SILC network, this is the recommended way of sending channel messages. This method is the simplest method for end user since it does not require any special settings before engaging the conversation on the channel.

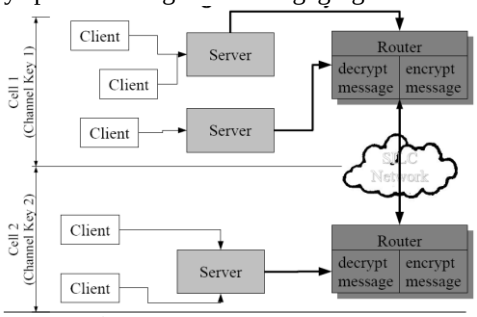

fig-4: Channel message delivery

- *Channel Message Delivery with Channel Private Key:* If the Clients cannot trust the servers and routers in the SILC Network they should not use the default way of sending the channel messages. Instead they should use channel private keys to encrypt & decrypt the channel messages. Channel private keys are keys that are known only by the clients who have joined the channel. Servers & routers do not know the key & cannot decrypt the messages. When message is sent between two routers they are merely re-encrypted with the session key but don't decrypt since the router don't have the key to do that. The clients joined the channel must first agree on the channel private key they are going to use. As the channel private key is actually entirely local setting in the client, it is possible to set several channel private keys for one channel. When encrypting messages with one channel private key only the clients who have that key can decrypt the messages. In this way it is actually possible to have a private group conversation inside the channel while global conversation at the same time.
- *Private Messages:-* Private messages are messages that are sent from one client to another through the SILC network. They are private because they are not sent to anyone else except to the true receiver of the message. Private messages can be used to engage private conversation with another client if channels are not desired. There are several ways to secure private messages. Private messages are encrypted using the session keys established in the SKE protocol. It is also possible to negotiate a private message key between the two clients & encrypt the messages with public key cryptosystem.
- *Private Message Key with Session Keys:* Sending private messages are by default secured with session keys established in the SKE protocol, private message is always encrypted with the session key of the session key of the next receiver of the message enroute to the receiving client. As the diagram shows the private messages sent by Client A to Client B travels through the SILC network & are always decrypted & re-encrypted with the session keys. The client B finally decrypted the private message that is encrypted with the session key shared between Client B & Server Y. the way of securing private message is not perfect & cannot be used in all circumstances. Since this way of securing private message cannot be used at all times the SILC protocol provides other ways of securing private messages.

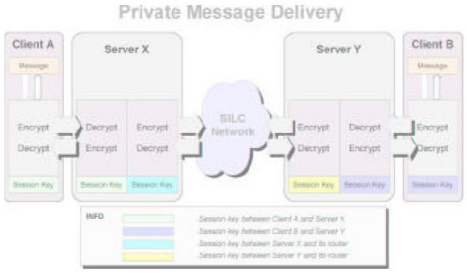

Fig-5: Private message delivery

*Private Message Delivery (Private Message Key):-*Private messages can be secured with private message key as well. This key is known only by the sender of the message & receiver of the message. This way no one else except the sender & the receiver can encrypt & decrypt the private messages. The encrypted message from the sender with the private message key & enroute the server. Without the key, they can't decrypt the message. As per the diagram, Client A encrypts the message with the private key & sends it to SILC network. Alls servers & routers merely pass the message through since they cannot decrypt it, Client B receives the message & decrypt it with the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

private message key. Sending private messages in this process is always secure since the key is shared only by the sender & the receiver. Using this method of private message delivery is recommended if the clients cannot trust the servers & routers in the SILC network.

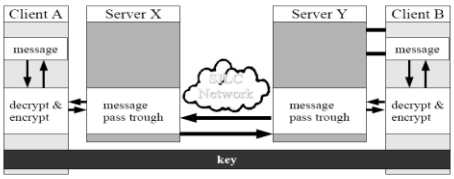

Fig-6: Private message delivery using private key

Messages in SILC: - SILC protocol supports MIME messages as normal channel and private messages. By using MIME messages it is possible to send for example images, music and video and audio stream in SILC. The MIME messages are utilized by using Message Flags, which indicates the recipient that the message is a MIME message & it then knows how to interpret the message & it is also possible to send other kind of messages & to augment features of normal channel & private messages.

- **Messages can be signed(use/ SMSG)**
  [?] fukami : signed msg, you don't have the key
  [S] fukami : signed msg, you 've got the key

- **MIME messages**
  / SCRIPT LOAD silc-mime.pl
  /MMSG-CHANNEL channelname path/to/f
- **Private message protection with keys**

Securing Private Messages:-

- *Shared secret by phone, mail, letter…*
- */KEY MSG USERA set secret*

  /KEY MSG USERB set secret-responder
- *=> secured communication*

- ***FILE TRANSFER (SECURE) PROCESS:*** - The file transfer processes in chat protocols are a absolute requirement. SILC also supports file transfer with the addition that the file transfer stream is secured. When a user wants to transfer a file to another user, the SKE protocol is the first executed to negotiate a session key for the file transfer stream. The FTP used in SILC is the SSH file transfer protocol (SFTP). Even though the name of the protocol relates to SSH, the actual file transfer protocol has nothing to do with Secure Shell. The SFTP is totally independent file transfer protocol & its stream is secured using SILC.

- *Send file p2p using SFTP*
  /FILE SEND path/to/file UserB
  / FILE ACCEPT UserB
  /FILE CLOSE (to close session immediately)

V.ADVANTAGES

i) The file transfer support in chat protocols are absolute requirement now a days, & chat protocol without one is no chat protocol at all.
ii) The support for file transfer in SILC has been designed so that using practically any file transfer is possible.
iii) It is more secured protocol compared to others.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

VI.CONCLUSION

The Secure Internet Live Conferencing (SILC) protocol, new generation chat protocol that provides all the common conferencing services with strong support of security. Its wide range of security should meet the highest levels of security requirements, while not forgetting ease of use. The network topology offers new solution with better scalability over traditional chat protocols. Different types of protocol keys and encryption decryption process make this protocol more suitable for conferencing services.

REFERENCES

[1] http://seminarprojects.com/Thread-silc-secure-internet-live-conferencing#ixzz2T9cu1S26
[2]. http://silcnet.org
[3]. http://ieee.org
[4]. www.itpapers.com
[5]. http://authorstream.com
[6]. http://osun.com
[7]. http://silky.sf.net
[8] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan. 1999.
[9] D. Kormann and A. Rubin, "Risks of the Passport Single Signon Protocol,"
Comp. Networks, vol. 33, 2000, pp. 51–58.
[10] A. Pashalidis and C. Mitchell, "A Taxonomy of Single Sign-on Systems," 8th
Australasian Conf. Info. Sec. and Privacy, Wollongong, Australia, July 2003.
[11] B. Campbell et al., "Session Initiation Protocol (SIP) Extension for Instant Messaging," IETF RFC 3428, Dec. 2002.
[12] P. Saint-Andre, Ed., "Extensible Messaging and Presence Protocol (XMPP):
Instant Messaging and Presence," IETF RFC 3921, Oct. 2004.
[13] J. Rosenberg et al., "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.
[14] B. Campbell, R. Mahy, and C. Jennings, "The Message Session Relay Protocol," draft-ietf-simple-message-sessions-11.txt, July 2005.
[15] R. Mahy, "Benefits and Motivation for Session Mode Instant Messaging,"
draft-mahy-simple-why-session-mode-01.txt, Feb. 2005.
[16] Jabber Software Foundation, http://www.jabber.org
[17] J. Oikarinen and D. Reed, "Internet Relay Chat Protocol," IETF RFC 1459,May 1993.