An Analysis of XMPP Security

Instructor: Prof. Richard Sinn

Group : Chico

Members: VanitaMohite

Sudhir Sharma

CMPE 209 –Network Security

Fall 2008 Semester

San Jose State University

Date: 28th October, 2008

Table Of Contents

1. Introduction:.....3

2. XMPP Implementation: 3

2.1 Core Components:..... 3

2.2 Security Components: 5

2.3 XMPP for IM and Presence: 6

3. Security in XMPP: 7

4. Conclusion: 9

5. References:.....9

Abstract:

XMPP is Extensible Messaging and Presence Protocol which is widely used for Instant Messaging (IM). This paper will provide a brief idea on the utilization of this protocol in the IM. This protocol uses XML to transfer the data over the network, so it is prone to attacks. We will see how the security measures are taken to handle the attacks.

1. Introduction:

XMPP is widely used for instant messaging, voice chat, text chat, video calls, light weight middleware, etc using the XML data [1].It is founded by the Jabber Software Foundation and is open technology. Though there were few IM's existing in the market due to their closed service drawback there came the need for new open service IM. Hence XMPP came into picture in which XML is used for streaming. It makes use of the client server architecture, where the client access the server over a TCP/IP connection and client uses the XMPP.

2. XMPP Implementation:

XMPP has three main components as:

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

Let us see each component in detail.

2.1 Core Components:

The core component consists of the client, server and the gateway of the foreign network. In the network the client is connected to the server using the gateway. The client uses the XMPP and the server is responsible to accept the message and be connected to the client. A secure network is been created between the client and server and also protocol manipulation is done on both the sides.

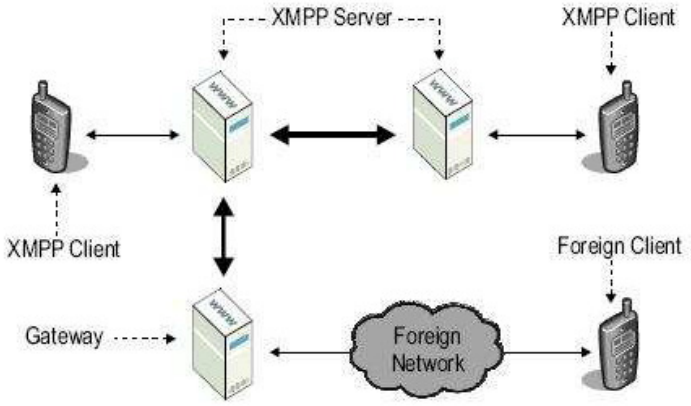

Figure 1: XMPP core components [4]:

For the interaction between the client and server the TCP connection is been setup first. The client has direct connection with the server when the XML streaming is done. The unique addresses can be recognized and a single TCP connection can hold more than one session at a time. Routing policy of the application level is defined on the server side. When the data is transferred in XMPP using XML, there is XML stanza that uses the XML format to transfer the message in to a XML stream. It consists of different attributes as id field, to field, from field, XML: lang field and type.

The following are the three attributes that are discussed:

<message/>:

The message is been transferred in between the client and server using the "store and push" mechanism. The message is been pushed to the other entity from one end point to the other end point.

Example: <message from'vanita@us.ibm.com/laptop'
to='sudhir@us.intel.com' />
<body>Good Day</body>
</message>

<presence/>:

If the entities have subscribed to any information, this attribute helps to broadcast particular information to multiple recipients.

Example: <presence from='vanita@us.ibm.com/laptop'
to='sudhir@us.intel.com' />

<id/>:

The id attribute works like the request and response used in the HTTP. If there is a file transfer then one entity can make a request for the necessary file and then the response can be received by sending the requested file.

Example: <iq type='get'
from='vanita@us.ibm.com/laptop '>

```
        <query xmlns='ecomm:register'/>
    </iq>
```

All the data that is been transferred in the XML stanza using the above mentioned five entities is been transferred using the tag <stream/>.This specifies that all the data mentioned in stream tag is the XML data to transfer. During this transfer there is a possibility of an error, if there is occurrence of any error it is recorded in the <error/ > attribute this details are sent.

There are five advantages using this XMPP:

1. When the messages are sent to the sender, even the user is offline the messages can be kept for a longer time. It prevents the loss of data when user is offline.

2. The location of network services is found using DSN SRV. It uses the id attribute to discover the service for the XML stanza.

3. A user is attached to any required resources using the address of the resource, this helps user for not using any other protocol to share the other resources.

4. The xml: Lang attribute helps to use any international language, making it a convenience for the user.

5. The TCP connection holds the guarantee from end to end transfer of data, unlike the UDP that can drop the messages during the transfer.

The data that is transfer has to be in a human readable format, which makes the message header larger in the TCP connection, the binary data is heavier during the transfer.

2.2 Security Components:

The following are the security layers that are implemented in XMPP. Mutual Authentication and integrity are the two major mechanisms that are implemented to gain confidentiality.

Figure 2: Security layers in XMPP [4].

For XMPP the first security layer is the TLS (Transport Layer Security). TLS helps to encrypt the data and the data is confidential in between the two parties. The SASL (Simple Authentication and Security Layer Protocol) which is the second protocol that helps in validating the end parties, so that they are authenticated users to carry on the client- server or the server-server communication.

The main advantage of using TLS in XMPP it prevents the tampering and eavesdropping [4]. While the client is negotiating with the SASL, the TLS connection must be established and then can be the XML stream be secured.TLS has its own name space and is triggered using the "STRATTLS " extension. A general process is followed for a successful TLS and SASL connection:

1. XML streams can be initiated only when client has a TCP connection to the server.
2. Client receives the STARTTLS extension from server and also the authentication mechanisms with it.
3. When the extension is received the response is sent from the client.
4. The acknowledgement is sent from server to the client to continue.
5. TCP connection is established when both complete the TLS setup.
6. Now a stream is sent to server
7. A stream header is sent to client for a SASL authentication.
8. A client decides on a authentication process.
9. Client receives a base 64 encoded message from server.
10. Client authenticates the message with provided credentials.
11. A session token is received by client for security
12. The server again receives the response from client
13. Now the client receives message of the authentication.
14. Now the client continues with the stream transmission.

Below is the pictorial view of the successful connection in the TLS and SASL.

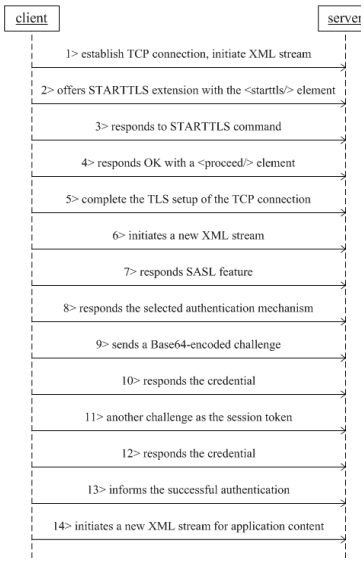

Figure 3: A successful security setup with TLS and SASL [4]

2.3 XMPP for IM and Presence:

XMPP came into existence for the instant messaging, but along with this there came the presence service too. As mentioned above the process looks simple, the client and server establish a connection using TCP. Then the server authenticated the client and puts challenges using the LS and SASL and then the XML stream is sent across and the transmission of data continues. But the real time scenario is a bit different. There are five types of messages that are sent in XMPP:

1. Unicast
2. Broadcast
3. Multicast
4. Normal
5. Error

Each type of message has its own purpose. Each message consists on message tags as subject – what s the topic of discussion, body – the matter of the message and thread where user can continue with the same subject.

There are seven states for presence message:[4]

1. Unavailable
2. Subscribe
3. Subscribed
4. Unsubscribe
5. Unsubscribed
6. Probe
7. Error

There are three elements for presence message:

1. Show: In the contact list the user can show the available message to other users. The user if busy can put the do not disturb message.
2. Status: Other than the predefined messages the user can put his own message to make it visible for his contact list.
3. There is a privacy issue for the presence service. This may or may not be used by the user as he may or may not want any subscriptions.

The contact list of the user can be maintained on client to reduce the load on server, or leave it on server side.

3. Security in XMPP:

Security has always been a key issue for any technology and XMPP is no exception. Following are the security consideration in XMPP.

3.1 High Security:

High security is the mutual confidentiality that is maintained in both the parties when a certification based authentication is provided [2].Whenever a certificate is issued; only the authorized certificate should be accepted.

3.2 Certificate validation:

Whenever a certificate is issued it should be reviewed by both the parties. There are three possibilities:

1. If the certificate is accepted by the trusted anchors only then the party should share their information.
2. The certificate could be validated from the certificate authority that the other party is unaware of.
3. The party has the self signed certificate.

3.3 Client- server communication:

The client must support the TLS and SASL protocols to connect to the server. The encryption of the XML stream is done using TLs and the authentication is carried out by the SASL. After the service record is verified only then should the client communicate to the server. The IP address which the client communicates should be kept private so that the channel is prevented from intruders.

3.4 Server- Server communication:

Unlike the client, server should support the TLS and SASL protocol for ease of communication. With the use of SASL in the server communication, authentication and integrity of the data is ensured. The server should also support the server dialback using DNS in which the server is protected from direct snoofing over the network.

3.5 Protocol layers:

There are four protocols in order used in XMPP as mentioned in the security implementation. They are as [2]:

1. TCP
2. TLS
3. SASL
4. XMPP

TCP is base layer where the connection between the client and server is done.TLS encrypts the XML stream and SASL does the authentication and XMPP is the application layer.

3.6 Lack of SASL channel Binding with TLS:

SASL does not guarantee the authentication and integrity in the lower layers of the protocol stack. Due to this the channel binding in the lower layers lacks and SASL cannot verify the two parties for communication. If there are such lower layers then the communication should be avoided.

3.7 Technology implementations:

For different security features different algorithms are used.
Authentication: Digest MD5
Confidentiality: TLS RSA with 3DES, EDE, CBC and SHA cipher
For Both: TLS and SASL [2].

3.8 Firewalls:

TCP is widely used for XMPP communication. For client to server port 5222 is used and for server to server communication port 5269 is used. This makes admin job a bit easy, if he sees something fishy he can disconnect the XMPP communication.

3.9 Base64:

Base64 helps to recognize the trusted client and server. The server validates the client and if any data is extraneous then is should not be accepted. This helps is maintaining the data integrity and passing correct data.

3.10 Stringprep Profiles:

NAMEPREP is the profile used in XMPP from STRINGPREP in which the domain identifiers are processed. There are two profiles as:

Nodeprep: This is used identifying the nodes. The user can user a different name in the multiple chat session, so he should not be given access to others information.

Resourceprep: This identifies the resource and is mentioned in the address as the node. The user can share a name in multiple chat session and can have multiple logins and send messages.

4. Conclusion:

XMPP the open technology for instant messaging is used for various different purposes as chat, etc. The architecture helps us to know how the security is enhanced to keep the integrity and confidentiality of data. The security measures are also explained in XMPP. There is still research going on by the Jabber Software Foundation (JSF) to improvise the technology.

5. References:

[1] XMPP Security. Retrieved, on 09/14/2008, from http://xmpp .org/tech/overview.shtml.
[2] XMPP Security. Retrieved, on 09/14/2008, from http://www.ietf .org/rfc/rfc3920.txt.
[3] Peter Saint-Andre. Streaming XML with Jabber/XMPP
Found in: IEEE Internet Computing, Published by the IEEE Computer Society
[4] Pin Nei. An open standard for instant messaging: eXtensible Messaging and Presence Protocol (XMPP).Found in: www.tml.tkk.fi/Publications/C/21/nie_ready.pdf.