SIP-TLS for iOS based SIP Clients in Enterprise Networks to Support Custom CAs

Vinayak Kwari
MTech in CNE
Dept of CSE, RVCE Bangalore-59
Email:vinayakkwari@yahoo.co.in

G.S. Nagaraja
Professor, Dept of CSE
RVCE Bangalore-59
Email:nagarajags@rvce.edu.in

Swethambari L Kant
Manager, Avaya India Pvt LTD
Bangalore-68
Email: swethalk@avaya.com

AbstractSecurity to the data while transmitting over the internet is important, especially when the enterprises are very much concerned about their privacy while communicating over the Internet and any leakage of the confidential data may result in loss of revenue and cause huge embarrassment to the companies. To secure the web interactions, the protocols like SSL and TLS are used. Earlier SSL was used for providing the security to web interactions, due to the security flaws in the SSL the world has moved to opt for the TLS as the security protocol. The current workis to provide the security to the SIP data in VoIP applications at the transport level. This is achieved byproviding TLS support to the application and it enables applications to secure theirdataform eavesdroppers, who may try to modify the data for their beneficiaries. Although there are several implementations of SIP-TLS, this work has been carried out to support the custom CAs in enterprise networks during authentication phase of the TLS handshake. TLS protocol has two layers the TLS record protocol and the TLS Handshake Protocol. TLS record protocol operates on top of some reliable transport layer protocol like TCP. Current implementation of TLS will provide the security to the SIP data in terms of confidentiality, Authenticity and integrity. Handshake protocol will perform the necessary handshake between client and server and negotiates the set of security parameters to secure the current connection. Authentication service is provided using the X.509v3 Certificates, which will provide the mutual authentication between the client and servers. After successful authentication, the clientand server will derive the appropriate keys form the security parameters exchanged .These keys are then used to exchange the data in the secure way.

Index Terms—Certificates,Custom CA,Public CA,SIP, Trust,TLS, Signature

IJSER

1 INTRODUCTION

The security to the SIP (Session Initiation Protocol) data is very important, as it is a signaling protocol for the VoIP applications. SIP is a text based protocol [4], matches HTTP (Hyper Text Transfer protocol) protocol in syntax of messages that establishes, modifies, and terminates the VoIP calls between the two telephony endpoint. SIP works in conjunction with the other protocols like SDP (Session Description Protocol), describes the media parameters for the session. If an attacker is able to modify the data in SIP messages, for his beneficiaries then there can be loss of information [11], [12].SIP messages may contain information that a user or a server wishes to keepprivate. For example, the headers may reveal information about the communicating parties or other confidential information. The SIP message body may also contain user information (addresses, telephone number, etc) that must not be exposed.Evaesdropping a connection and decoding signaling messages may lead to Loss of privacy and confidentiality. So the solution for this kind of security threats to the SIP data is, Encrypt transmitted data using encryption mechanisms like IPsec and/or TLS [13]. This paper talks about an approach for protecting the SIP data using TLS. This solution for the enterprise networks supports the Custom Certificate authorities in addition to the well known public CAs.

Here Custom CA means, the enterprises can have their own public key infrastructure (PKIX), and the root certificate authority in this PKIX is called as custom CA [3]. And this custom CA will issue certificates for the servers in the enterprise networks. There iscost advantage for enterprises when they go for the Custom CAs. Because they donot have to pay for the Public CAs to get certificates for their servers. TLS is a security protocol which is an Internet standard version for the proprietary version of Netscape's SSL protocol. Although the TLS is primarily used to secure the web-interactions,suchas HTTP interactions. It can also be used for the protection of SIP sessions. The implementation of TLS for SIP is different from the implementation of TLS for web-interactions.This difference is brought to the spot-light in the next sections. TLS has two sublayers in it, TLS handshake Layer and TLS Record Layer [1]. The handshake Layer is responsible for performing handshake with the server and setting up the cryptographic session parameters, to be used later for protection of the application data.

Following is the details about the messages exchanged during the Handshake process and it it’s depicted in fig 1. Messages with * in the figure indicate, they are either optional or situational dependent.

Client Hello: This message contains Session ID, Client random, compression algorithm, client version, Cipher suites. Cipher suites in this message are the proposal to the server to select one among them.

Server Hello: This message contains the Session ID, Server random, server version, compression algorithm and cipher suite. The cipher suite in this message is the choice of the Cipher suite from the server among those in the client hello message.

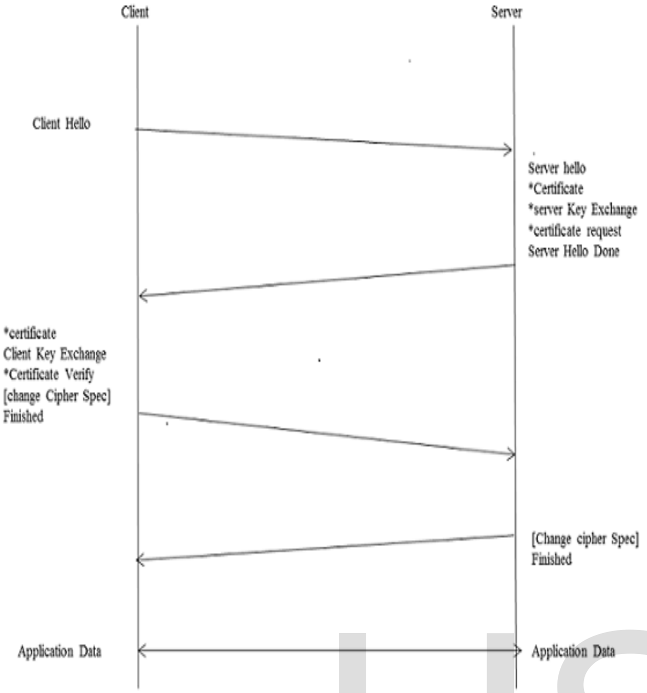


Fig 1 Message Flow diagram for TLS Handsahe

Certificate message: This message from the server contains the certificate. This certificate contain the server public key **Server key-exchange message:** The Server Key Exchange message is sent by the server only when the server Certificate message (if sent) does not contain enough data to allow the client to exchange a pre-master secret. This is true for the following key exchange methods: DHE_DSS, DHE_RSA, and DH_anon

Optional Certificate request message: This message is sent by the server to ask the client for its certificate to be sent

Server Hello Done: This message is sent by the server to indicate the end of the server hello message and associated messages

Optional certificate message from the Client: This message is sent by the client to send its certificate to the server, if server has asked client certificate by sending the Certificate request message

Client Key Exchange: This message is sent by the client to exchange the premaster secret with the server.

Certificate Verify message: This message is only sent by the client if the client certificate has signing capability and it is to verify that the public key in the certificate of client matches with the private key that is with the client ie it provides the explicit client certificate verification.

Change Cipher spec message: This message is sent by the client to indicate that the client has upgraded its session with the newly negotiated parameters. And indicates the server to do the same

Finished Message: This message is sent by the client to verify that session parameters are correctly negotiated between the client and server. This is the first message that gets protected with the newly negotiated parameters.

After this both the client and server have successfully negotiated the cryptographic session parameters and these parameters are used by the TLS record layer to apply the security mechanisms onto the application data.

2 SYSTEM ARCHITECTURE

System architecture: System architecture identifies the structure, behavior and view of the system that is under development. It is the plan that comprises of components and relationship between those components. It actually helps in mapping the conceptual model of the system into hardware and software components

The current project provides the security for the sip data in the VOIP applications. SIP is an application layer protocol [2]. That is used for signaling in VOIP application. The components of the VOIP application are shown in the fig 2the following section will give brief description about each of these components

1. Application UI:

This component of the application provides user with visual interface for accessing this application. The user will send events to the underlying layers by actions like tapping of the button, dialing numbers etc. These events are then processed by the underlying layers to perform the intended actions

2. Signaling handling module:

This module is an interface between the application UI and the SIP stack. This module transforms the events from the UI and invokes appropriate module in the SIP stack and it also handles the results from the SIP stack and passes it to the appropriate UI element

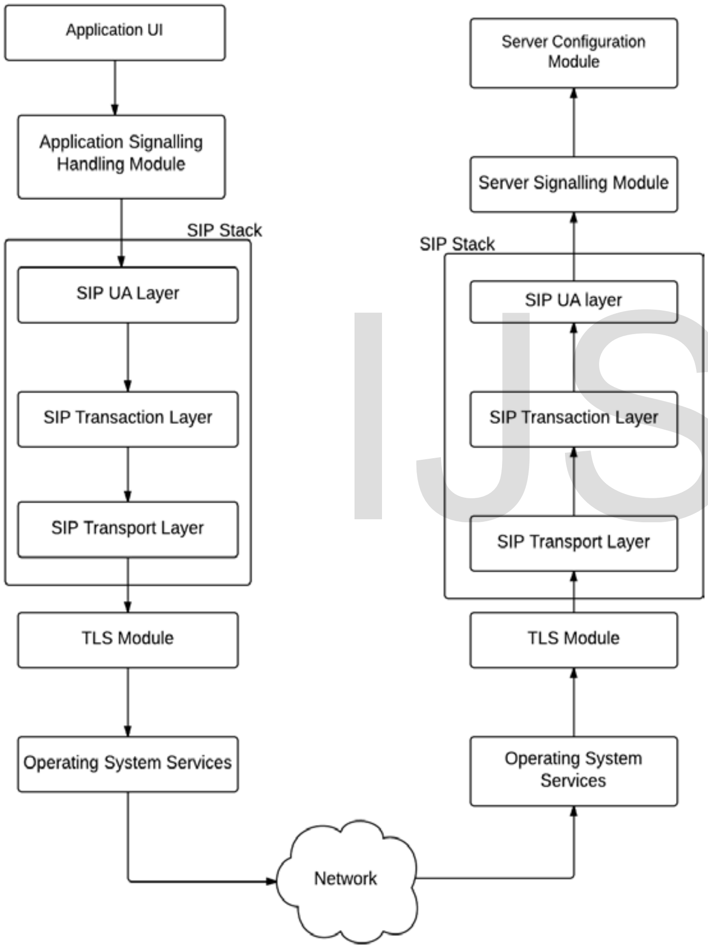
IJSER

3. SIP Stack:

a. Transaction User (TU) :

Transaction user is the layer above the transaction layer in the SIP stack. The transaction user can be user agent client (UAC) and servers (UAS), stateless and state-full proxies and registrars. Since this project is for clients, the transaction user will be either UAC or UAS [2].

Whenever the transaction user wishes to send the request it creates the client transaction instance and passes it the request along with the IP address, port and transport to which to send the request. Also the transaction user will process the incoming requests and sends the response to those requests.



IJSER

Fig 2 system Architecture

b. Transaction Layer:

Transaction layer is the logical module that is used by the TUto send the request to particular destination. Transaction Layer has two sides in it, ie client side and server side. The client side is known as client transaction and server side is known as server transaction client transacton sends the request and
server transaction sends response.The client transaction ecievess the request from the TU and reliably delievers the request to a server transaction. The client transaction is also responsible for the receiving the responses and delievering them to the TU and it filters out any response retransmissions or disallowed responses

The purpose of server transaction is to receive the requests from the ttransport layer and delievering them to the TU, and it filters out any request retransmissions from the network. The server transaction accepts responsesfrom theTU and delievers them to the transport layer for transmission over the network

c. SIP Transport:

The transport layer is responsible for actual transmission of the requests and responses over the network transports. The client side of the transport layer is responsible for sending the request and receiving responses. The user of the transport layer passes the client transport the request, an IP address, port, Transport and possibly TTL for multicast destinations.

The client side transport layer of SIP is responsible for inserting a value-of "sent-by" field into the via header field of the SIP messages. Also the transport layer is responsible for managing the persistent connections for transport protocols like TCP, STCP or TLS over those. The connections are indexed by the tuple formed from the address, port and transport protocol at the far end of the connection and this index is set when the connection is opened by the transport layer. And this index is set to the source IP, port and transport when the connection is accepted by the transport layer. The server side of the transport receives the requests on the IP address, port and transport combination, which are resolved by the DNS look up of published SIP or SIPS URI of the server. The server transport upon receiving the request attempts to match them to the server transaction, if present. If there is no matching server transaction then the request is transferred o the core.

4. Transport Layer Security (TLS):

Transport layer security provides security features for the SIP data, ie it protects the data from the hacker. TLS provides three main security features to the application data they are encryption, authentication of the peer and Message authentication. TLS sits just above the transport protocol (i.e. TCP) and applies cryptographic algorithms to the application data before transmitting it to the next layer. So thus the data maintains confidentiality and integrity while it is in transit
to the destination. The handshake part of the protocol authenticates the peer of the connection, performs key exchange with the peer and establishes the necessary cryptographic parameterslike session encryption key, session authentication key and Initialization vectors. These parameters are then used by the TLS record layer to apply cryptographic algorithms on the data.

5. Native Transport :

This layer actually performs the process to process delivery of the data over the underlying network. This layer uses TCP, SCTP or UDP. If TLS is used then the protocol used here has to be TCP or SCTP. The transport protocols provide the application with the ability of accessing the underlying network TCP provides the reliable delivery of data but it can be slow whereas UDP is fast but there is no guarantee of delivering the data

3 Algorithm

Implementing the TLS for SIP is quite different from implementing TLS for web-interactions [5]. In latter case, there can be provision to explicitly ask the user about trusting particular server certificates, in case evaluation of the certificate fails and that failure can be recovered by setting some exceptions to the certificate evaluation procedures. But this should not be done for the TLS implementation for SIP. Because SIP is used in real time calls and the authentication of the SIP-TLS server should be verified successfully.

Below is the algorithm for the implementation of TLS for SIP:

1. Make TCP connection to the SIP-TLS server
2. Create Streams and apply security settings to streams [10]
3. Start the TLS Handshake with the SIP-TLS Server
4. When Server Certificate comes validate the certificate against the Certificate Trust store of the system [6].
5. During validation Server certificate is checked to see whether it meets criterias in the security settings imposed on the streams.
6. If Server Certificate validation is successful then proceeds with the connection. Otherwise close it
7. If client certificate request has come then send the client certificate to the server
8. If handshake is successful then continue with the connection, otherwise close it
9. Send and Recieve application data over streams.

4 Implementation details:

This implementation of TLS is for iOS based SIP clients and programming language used for implementation is Objective C. iOS security framework provides the necessary APIs for the implementation of TLS. iOS has given the set of APIs,
to impose the necessary security settings on the streams, streams handle the data transmission and reception over the network.IP-Address and port of the SIP server is taken as input to the program

First a BSD socket is created to establish a TCP connection to the SIP server. Then two uni - directional Streams are created from the socket, if TCP connection is successful. Otherwise the errors are logged and connection is closed. To these Streams the security settings are applied and then the handshake is started [9]

If TLS handshake is completed successfully then stream events will occur [9] . When the stream event HasBytesAvailable occurs it means that the data is available in the streams andapplication has to read that data. When stream event [9] HasSpaceAvailable occurs then it means that the applicationhas the chance to write the data onto the streams. And if, any errors occur during reading and writing of data then those Errors are handled when stream event ErrorOccured occurs. Certificate based authentication phase of TLS helps in authenticating the peer entity. This authentication phase verifies the certificate chain of trust [7], [8].

Basically the implementation of TLS for SIP is done for the enterprise networks and the enterprise can have its own CA to issue certificates for its servers or some enterprises can have only the self-signed certificates for their servers or some can have the certificates issued to their servers bythe well-known public CAs [14]. So all these CAs are supported in the current implementaation.This is achieved by having the corresponding Root CAs for those server certificates being installed on the endpoint side. The deployment of Root CAs on the endpoint is achieved using the capability of underlying Operating system on which the SIP application runs.

5 Test Results:

The testing has been carried out to test the implementation unit against the various combinations of server and root certificates.The various fields in the server certificate are validated to see whether the information in the certificate is trust worthy or not. For example if the certificate is expired, certificate subject name doesnot match the URI of the current connection, signature verification of the certificate fails, certificate chain is broken then in all these cases the handshake should fail. Also the handshake will fail if root certificate corresponding to server certificate is not present on the endpoint. All These cases are included in testing of current implementation of TLS and it is verified that the implementation has passed these test cases.

Handshake will succeed if server certificate satisfies all the necessary criterias that we impose during the evaluation of server certificates.

6 CONCLUSIONS:

Security for the SIP data from the possible security attacks is necessary as it is the signalling protocol for VoIP applications and the same has been accomplished in this work by implementing the TLS protocol for SIP application. And it is obvious from the test results that SIP data has been protected against the security attacks

IJSER

REFERENCES

[1] Transport Layer Security 1.2 Request for comments 5246 Network Working Group T. DierksIndependent,ERescorla RTFM Inc August 2008

[2] Session Initiation protocol Request for comments 3261 Network working group J Rosenberg dynamicsoft, H. Schulzrinne,Columbia U, G. Camarillo Ericsson, A. Johnston WorldCom,J. Peterson Neustar, R. Sparks dynamicsoft,M. Handley ICIR,E. Schooler AT&T June 2002

[3] Internet X.509 Public Key Infrastructure Certificate and certificate

Revocation list profile (CRL) Request for comments 3261 Network working group D. Cooper NIST, S santesson Microsoft, S Farrell Trinity College Dublin, S Boeyen Entrust, R housley Vigil Security, W. Polk NIST. May 2008

[4] Enterprising with SIP — A Technology Overview Version 3 February 2006

[5] A trust communication with SIP protocol Hammamet, Tunisia May 16-May 19ISBN: 978-1-4244-7716-6Samer El Sawda, University Paris VI, FrancePascalUrien, EcoleNationaleSupérieure de Télécommunication Paris, FranceRami El Sawda, GREYC, UMR 6072 CNRS, University of CAEN, France ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010

[6] An article about Certificates and trust http://msdn.microsoft.com/enus/library/windows/desktop/aa376515(v=vs.85).aspx

[7] Chain of Certificates and trust Verification, Wikipedia article http://en.wikipedia.org/wiki/Chain_of_trust

[8] Certificate, key, Trust Services Reference Guide, Apple Developer Library. http://developer.apple.com

[9] CFNetwork Programming Guide, Apple Developer Library. http://developer.apple.com

[10] Secure Transport, Apple Developer Library. http://developer.apple.com

[11] D,Richard Kuhn, Thomas J. Walsh, and Stef-fen Fries, "Security considerations for voice over IP Systems", Computer Security, January 2005

[12] A. Gisler, M. Lortez and A. Stricker, "SIP Security", Diplomarbeit, ZurcherHoschschle Winterthur, 2003

[13] A Steffen, D Kaufmann, A. Stricker, "SIP security", Security Group, Journal: ZurcherHoschschle WinterthurCh-8401 Winter 2004

[14] R. Granito and A. Hovsto (editors). "Guidelines for the use and management of trusted third party services", JTC 1.27.19

IJSER

IJSER

IJSER