belledonne communications.

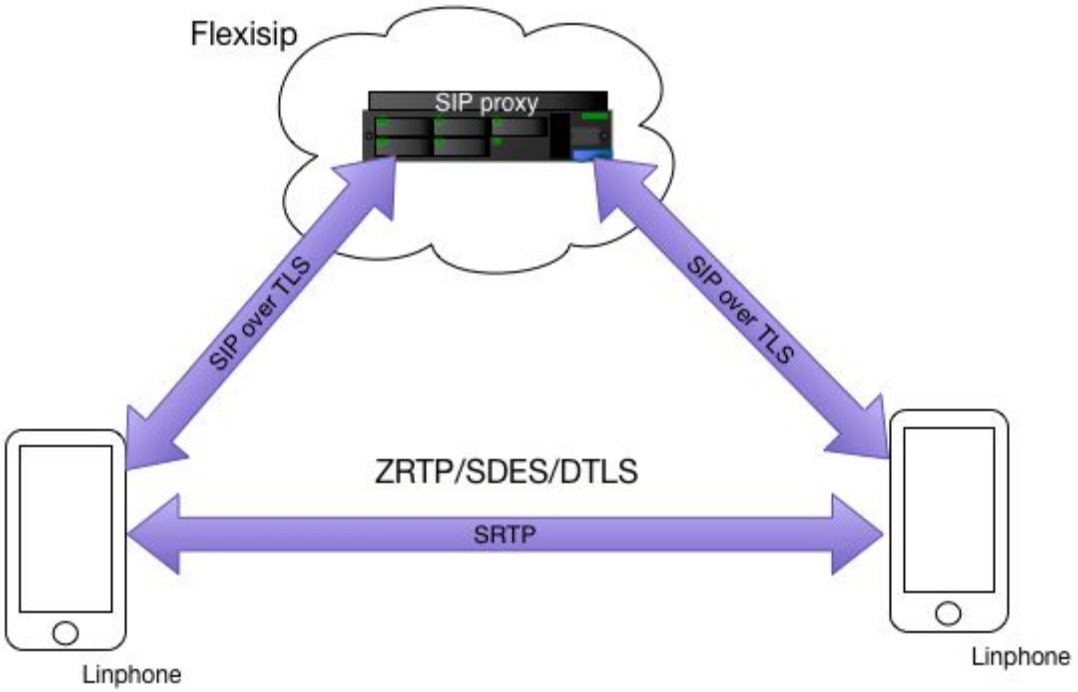
Secured Communications using Linphone & Flexisip

Solution description

Office:	Headquarters:	Company legal information:
Le Trident Bat D - 34, avenue de l'Europe 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	12, allée des Genêts 38100 Grenoble - France Tel. : +33 (0)9 52 63 65 05	SARL au capital de 4000 € SIRET : 520 318 437 00016 EU VAT Number : FR89 520 318 437

Intro

Digital communications including voice, video and messaging are sensitive user data that need to be protected against unauthorized access. Both Linphone and Flexisip provide built-in security capabilities allowing to create a secured communication service across public internet. This document describes key technologies taking place into a Linphone/Flexisip SIP network.



Index

- Intro
- Index
- Trusted Registration and Call Setup
- Trusted voice & video communications
  - SDES (Session Description Protocol Security Descriptions)
  - ZRTP (Media path key agreement for unicast secure RTP)
  - Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)
  - Trusted messaging & file sharing
- Conclusion
- Contact

Trusted Registration and Call Setup

First level of security is to make sure both end-user registration and call setup are performed in a secure way. These operations involve both Linphone and Flexisip SIP proxy. Linphone client establishes and maintains a SIP-TLS connection to the flexisip server. The Linphone client verifies the SIP server's authenticity based on x509 server certificates checked against a list of trusted root authorities provided at compilation time.
This first step warranties the integrity and the confidentiality of all the information exchanged between the Linphone client and the Flexisip server.

The second step is to perform the authentication of the SIP messages coming from clients. The Flexisip server is responsible for this task, using either digest authentication from a password database, or better by using TLS client-based authentication: in latter case the client certificate presented by the Linphone client must be valid and must match the identity (From header) claimed in the SIP messages.
The choice between the two methods (http digest or TLS client based authentication) is a matter of configuration in Flexisip and Linphone client.

Trusted voice & video streams

Voice and video over RTP are encrypted using AES with either a 128 or 256 bits key length. The way RTP packets are encrypted is described in rfc3711. For ciphering key exchange, Linphone implements 3 differents IETF standards.

SDES (Session Description Protocol Security Descriptions)

This is the original way to exchange ciphering keys. Basically, idea is to exchange encryption keys during call setup. Rfc 4568 describes a new SDP attribute used to encode an AES key in base64. As SDP messages are secured by SIP over TLS, key exchanges can be considered as secured as long as SIP network integrity is guaranteed.
Main concern about SDES is that security entirely relies on SIP network. A SIP network is generally composed by one or several SIP proxies. As SIP/TLS is a point to point encryption solution, each SIP proxy has access to media ciphering keys in clear text. Trusting SDES requires that all the SIP proxies involved in the routing of the call or message are trusted.

ZRTP (Media path key agreement for unicast secure RTP)

To reduce security pressure on SIP proxies, ZRTP (rfc6189) proposes an end to end encrypted key exchange based on Diffie-Hellman. ZRTP protocol messages use same media path as regular RTP packets. Main concern with Diffie-Hellman key exchange is that it can be subject to Man in the Middle Attacks. To prevent this, ZRTP proposes a mechanism based on a Short Authentication String. This SAS has to be checked by each participant using voice during the first call, and guarantees that there is no man in the middle attack.
Unlike SDES, having a compromised SIP proxy would have no effect on the integrity or the confidentiality of the audio & video streams exchanged between two clients.
Linphone brings its own implementation of ZRTP in the bZRTP library. As for SIP/TLS, the cryptographic engine used is the one from mbedTLS library (formerly known as PolarSSL).

Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)

Like ZRTP, SRTP-DTLS (rfc5764) provides end to end encryption, but based on public/private key to encrypt key exchanges. X509 certificates are used for authentication. Main advantage of this protocol is interoperability with Webrtc.

Linphone implementation is also based on mbedTLS.

Trusted messaging & file sharing

With Linphone, messages can be either secured by SIP-TLS, or if end to end encryption is required, using ciphering keys derived from previous ZRTP session is possible. The exchanged text messages or files are then encrypted using keys specific to each user. This last option requires a ZRTP voice call to be placed prior to initiating a messaging session.

Conclusion

Making a secure VoIP architecture requires several technologies to be implemented at both client and server side. Because they have been developed jointly, Linphone and Flexisip are the perfect couple to address high level of security. Also, the complexity of voice over IP must not obfuscate the security of the full architecture. Flexisip and Linphone have been designed with simplicity of use in mind, so that system administrators and developers can have a clear understanding of the security options they have.
Beyond to the reference architecture exposed in this document, Belledonne Communications's mission is also to adapt it to customer's specifics needs.

Contact

Worldwide sales

sales@belledonne-communications.com

Office

Belledonne Communications
Le Trident Bat D - 34 avenue de l'Europe
38100 Grenoble - FRANCE

Tel +33 (0)9 52 63 65 05
Fax +33 (0)9 57 63 65 05

info@belledonne-communications.com