ZRTP

ZRTP is a cryptographic key-agreement protocol to negotiate encryption keys required to establish an end-to-end secured VoIP (Voice over IP) phone call.

Inventors

The first release of ZRTP protocol specifications has been invented and published in 2006 by a group of well-known cryptography experts lead by Philip Zimmermann, original inventor of PGP:

- Philip Zimmermann, original inventor of PGP
- Jon Callas, Chief Scientist at PGP Inc, previously co-worker of Bruce Schneier
- Zooko Wilcox O'Hearn, peer to peer hacker and cypherpunk
- Colin Plumb, famous old school cryptography expert
- Alan Johnston, famous VoIP telecommunication expert

Public specification

The protocol, subject to public security reviews for more than 4 years, improved with continuous enhancements and security analysis by scientific and security communities from all around the world.

Latest updated protocol specification is available for download from IETF website in ZRTP specification page.

ZRTP call flow

Technically speaking, ZRTP has a great advantage over SRTP with SDES key exchange: it does not require any kind of SIP specific protocol extension in order to work properly, because all its operations are "in-band", performed in the same communication channel through which the voice is transported. After the SIP telephony handshake is completed successfully (the called peer answers the phone), ZRTP key handshake is started, followed by the exchange of encrypted audio:

Call authentication with Short Authentication String

Basically ZRTP makes an automatic key exchange between peers that support such encryption protocol and secure the voice communication channel. In this way it provides the users the ability to verify that there is no man in the middle, by verbally comparing two strings. The two strings will be displayed on the caller phone and the called phone, and they have to be exactly the same.

Example on how Short Authentication Strings are shown on different ZRTP applications:

SAS on Mobile PrivateGSM Professional*

* PrivateGSM Professional is provided by PrivateWave and use Zorg ZRTP implementation

SAS on Desktop zFone*

Images courtesy of Eric Y Chen
* zFone is provided by Philip Zimmermann and
use libzrtp reference ZRTP implementation

The strings, that the caller and the called must compare to verify that the communication line is secure, are called Short Authentication Strings (SAS) and come from the PGP Word List (a list of words for conveying data bytes in a clear unambiguous way via a voice channel).
For usability purpose, the SAS can be verified only once, then each party can mark the other as “trusted”. In this way the parties do not have to verify the SAS in every calls. This great feature is provided by the key continuity feature of ZRTP.

Entropy collection
Entropy collection of random data is the fundamental in encryption system, also ZRTP could be a weak protocol without proper randomness source.
ZRTP specification recommend to increase the strength of entropy generation system by feeding the raw entropy pool with some audio voice samples.
The audio voice sample is not sent during key exchange, but recorded from microphone.
This way ZRTP implementation always has a fresh and strong entropy collected from a physical source of entropy such as the microphone.
Zorg provide an API to let Secure VoIP implementor to dynamically add new entropy, we recommend to follow strictly all Random Number Generation reco mmendations of ZRTP RFC.
Other information
More informations on ZRTP can be found simply by googling it but the most significant to understand it are:

- IETF Official ZRTP protocol specifications - Official technical specification
- Philip Zimmermann's zFone Project - Provide the first opensource and reference ZRTP implementation and the well known zFone ZRTP for Linux, Windows and Macintosh.
- Wikipedia ZRTP - Wikipedia page on ZRTP
- GNU ZRTP - GNU c++ lightweight ZRTP implementation integrated into Twinkle
- GNU ZRTP4J - GNU java lightweight ZRTP implementation integrated into SIP Communicator
- VoIP Security Alliance on ZRTP
- Wireshark Network Analyzer ZRTP protocol