ZRTP and Zfone

End to End Encryption for VoIP

Problems

- RTP is unencrypted on the wire
- SRTP provides encryption but there's no standard way to negotiate keys
- Non-standard keying methods are done in the signaling channel and are not interoperable

How ZRTP Works

- Performs keying itself in-band in the media channel
- Uses ephemeral Diffie-Hellman key exchange during call setup
- Shared secret is used to generate keys and salt for SRTP
- Uses SRTP for media encryption
- Keys are hashed and presented to users to verify as “Short Authentication Strings”
- Keys are destroyed at the end of the call

ZRTP Benefits

- Complete End-to-End Encryption!
- Signaling channel independent
- No reliance on:
  - Public Key Infrastructure
  - Central Authorities
  - Pre-shared secrets
- Provides Perfect Forward Secrecy
- Absence of MITM can be verified at any time by comparison of the Short Authentication String
- Anti-MITM via key continuity

ZRTP Detriments

- Complete End-to-End Encryption!
  - Not good for CALEA compliance (but does it even need to comply?)
  - Not good for business requirements such as call recording
- Patented ...but wait!
  - Royalty-free licensing
  - Licensing requires conforming to spec
  - Spec includes anti-backdoor features
- ZID of the endpoint is sent in the clear

Zfone

- Implementation of ZRTP which works with any soft-phone
- Hooks the network stack and modifies RTP session inline
- Gave me the idea for SteganRTP (:

References

- ZRTP
  - http://zfoneproject.com/zrtp_ietf.html
- Zfone
  - http://zfoneproject.com/