ZRTP: Media path key agreement for Secure VoIP

Philip Zimmermann prz@mit.edu
Alan Johnston alan@sipstation.com
Jon Callas jon@pgp.com

http://zfoneproject.com

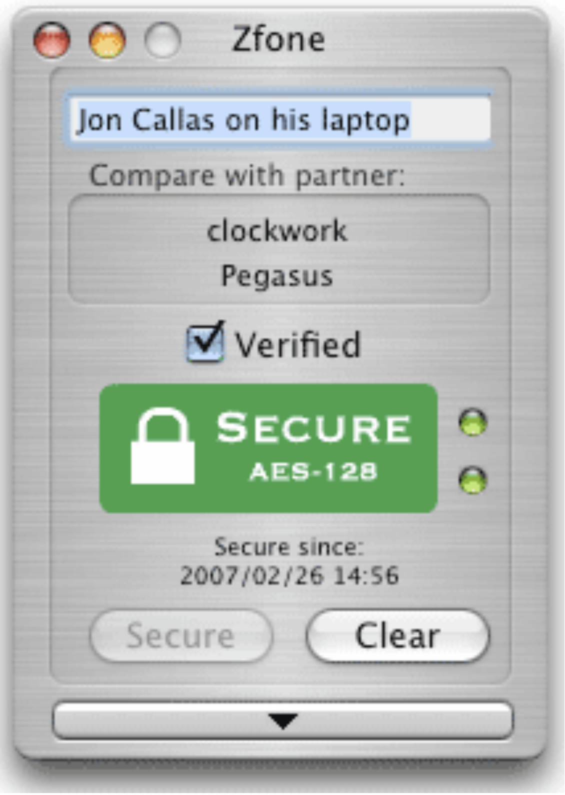
Crypto 2007

draft-zimmermann-avt-zrtp-04.txt

Goals of ZRTP

- Perfect forward secrecy
- Provide confidentiality to unicast voice conversations
- No reliance on signaling for authentication or key management
- No use of certificates or PKI
- Opportunistic encryption
- Fully compatible with existing VoIP endpoints
- True Peer-to-Peer Architecture
  - No servers needed
- Can be implemented as "bump in stack" and thus deployed *immediately*
  - Running code

Design of ZRTP



Jon Callas on his laptop

Compare with partner:

clockwork
Pegasus

☑ Verified

SECURE
AES-128

Secure since:
2007/02/26 14:56

- Use media path to negotiate session keys for Secure RTP media
- Ephemeral DH key agreement with hash commitment.
- Hash commitment constrains MiTM attacker to only one guess for short authentication string
- Alice and Bob verbally compare short authentication string to detect MitM
- Key continuity using cached secrets between calls, analogous to SSH