Overview

• ZRTP is the protocol for Phil Zimmermann’s Zfone
• Further documentation at http://www.philzimmermann.com/
Zfone

• Beta software available
  – www.philzimmermann.com
• Functions as a “bump in the cord” for SIP-VOIP clients
  – Supports Gizmo, eyeBeam, etc.
• Intercepts RTP stream, and converts to ZRTP
• Modeled after PGPfone, Eric Blossom’s COMSEC phone, AT&T 3600
• Protocol that implements Zfone
• Needs no PKI
  – Conceptually similar to SSH
  – Uses AES + 3kbit Diffie-Hellman Exchange
  – Hash commitment + chain of retained shared secrets
    • Allows voice-based Man-in-the-Middle rejection
    • Creates continuity between endpoints
• Independent of signaling layer
  – Can operate with other VOIP systems
Advantages

• Simple media encryption
• Well-tested components
  – SRTP, DH, hash commitment
• Layers with other security
• Even with no user-level MitM protection, protocol has endpoint continuity
  – MitM needs to be on first call, and stay in all calls to avoid detection
    • Note -- in some cases can force shared secret loss
What ZRTP does not do

• Identify your endpoint
  – How do you know this is Jon Callas?
  – PKI doesn’t solve this, either.

• Upper-level VOIP security
  – CallerID protection, etc.

• Protect against attackers with arbitrarily large powers
  – “Rich Little” attack
  – “Court Reporter” attack
  – Interpolation of hash secrets in milliseconds
  – Mental Telepathy, etc.
What does ZRTP do?

• Secures media from one endpoint to another
• Allows end-users to use DH materiel to thwart MitM
• Without end-user participation, validates that the endpoint is the same
• Creates very high bar for potential MitM