SIP Identity using Media Path

draft-wing-sip-identity-media-01

Dan Wing, dwing@cisco.com
Hadriel Kaplan, hkaplan@acmepacket.com
IPR Notice

• Cisco has claimed IPR on this technique

http://www1.ietf.org/ietf/IPR/cisco-ipr-draft-wing-sip-identity-media-00.txt
Motivation: SBCs Break SIP-Identity (RFC4474) Signatures

• RFC4474 signs the SIP body
  – including SDP
• SBCs rewrite SDP (m=/c= lines)

Requirement

• Identity should survive rewriting of SDP
Retaining Identity

• SIP-Identity-Media retains the originating domain’s signature

  SIP-Identity-Media  SIP-Identity (RFC4474)
  dwing@cisco.com  dwing%cisco.com@sp1.example.com
  +14085255314@cisco.com  +14085255314@sp1.example.net
  +14085255314@sp2.example.net

• Works with SBCs that modify SDP
Diagram of Operation

1. Sign user’s identity
dwing@cisco.com
   +14085551212@cisco.com

2. Validate signature

3. Perform ICE, TLS, DTLS-SRTP, or HIP on media path
Call Flow

1. Invite->
2. sign
3. Invite--> Invite-->
4. validate
5. <----------------tls, dtls, or ice-------------->
6. validate
7. ring phone
Questions

draft-wing-sip-identity-media-01

Dan Wing, dwing@cisco.com
Hadriel Kaplan, hkaplan@acmepacket.com
Backup Slides
Technical Differences from SIP-Identity (RFC4474)

• Replay protection requires running ICE (with extension), DTLS-SRTP, TLS, or HIP
  – On endpoint or domain-operated SBC
  – Firewalls or SBCs may block media path until ‘200 Ok’

• Avoids public key operations for intermediate domains (service providers)

• Endpoint does a public key operation
  – Might already be doing it (DTLS-SRTP, HIP)