Revisiting RFC4916

• The “connected identity” draft, update to RFC4916
  – How to make Identity work in the backwards direction, since it can’t work for responses
  – Covers mid-dialog and dialog-terminating requests
    • Classic use case is UPDATE in the backwards direction before 200 OK: telling you who you actually reached
• Leveraging STIR to close security vulnerabilities
  – Route hijacking
    • I tried to call my bank, by an attacker somehow interposed
  – “Short stopping” and similar attacks
    • Intermediary networks forging BYE in one direction while the call proceeds in another
  – sipbrandy (RFC8862) needs it
• This does take STIR past the threat model of RFC7375
What’s new in this version

• Mostly cleanup
• Did flesh out a bit more on pre-call connected identity
  – Basic idea: before you click “call”, learn who will be reached
    • Useful for some fraud cases, especially with RCD
  – Focusing on medialess dialogs
    • Basically, sending an INVITE with no SDP and an Identity header, with 100rel in Require, is a request for pre-call connected identity
    • Caller can then do offer/answer if the callee is legit
    • Obviously, this would require significant implementation support, not a small lift
      – Might be worth it for some classes of businesses and institutions
Pre-Call Connected Identity

Will my call reach the bank?

INVITE w/o SDP
Identity + 100rel

UPDATE w/o SDP
Identity (rcd)

Financial Institution

Client

INTER-MEDIARY

Oh, it will, so UPDATE to voice call
Conferencing

• Notes conferencing is something to think on
  - What do we think the expected connected identity behavior is for a conference?
    • What happens when conference participants change?

• Easy-road proposal
  - Declare centralized conferencing basically out of scope
    • Ways you learn about participants are secured separately, effectively only requires Identity to reach the conference bridge
    • Only if you get dialed in by the bridge (3PCC style) is connected identity relevant
  - Claim we get decentralized for free
    • Each participant does connected identity with each other participant
Still to do

• Revised examples
• Any actual normative revisions to RFC4916
  – Elimination of the Identity-Info header, etc.
• Flesh out more a pre-call connected identity approach
Next Steps

• Still plenty to do here
  – But we think we need this, for a variety of use cases

• Adoption, pending recharter?
New STIR Charter Text

The group will also consider extensions that leverage STIR to solve related identity problems around telephone calls and other telephone-number based communication, including call diversion and forwarding, rich identity presentation for delivery to a called party, messaging that uses telephone numbers, connected identity (mechanisms that identify the called party reached to the calling party), and similar use cases related to fraud and security.