draft-peterson-stir-rfc4196-update-04
Connected Identity

STIR WG IETF **111** ~~interim~~ 112 Virtual

~~July~~ ~~Sep~~ Nov 2021

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

No new version

- Back-burnered for recharter discussion
  - This has gotten bounced for time the last couple meetings
- Last iteration mostly focused on pre-call case
- To do list for this draft is pretty long…

Still to do

- Incorporate some previous discussions about privacy/anonymity
  - Definitely some risks about data collection if there aren't sound policies for accepting a pre-dialog
- Add some thoughts about directory for lookup of participating entities
  - Used in concert with pre-dialog
- Revised examples
- Any actual normative revisions to RFC4916
  - Elimination of the Identity-Info header, etc.
- Flesh out the 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.