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
STIR Backwards

Did I actually reach the bank?
What’s new in this version

• Details on use of connected identity in provisional dialogs
  – Require for 100rel
• Separate discussion of mid-dialog and dialog-terminating requests
  – Why we can’t make this work for CANCEL
• Interaction with “div” ppt’s
  – Should we return “div”s with Identity in the backwards direction?
    • Could let callers know why their call reached an unanticipated destination
    • Some concerns about revealing forwarding logic... problematic?
Still to do

• Revised examples
• Any actual normative revisions to RFC4916
  – Elimination of the Identity-Info header, etc.
  – (should this be a bis?)
• Flesh out more a pre-call connected identity approach
  – Could be deferred to another draft, even
Next Steps

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

• Recharter needed?

• Adoption?