draft-ietf-stir-rfc4196-update-01 Connected Identity

STIR WG IETF 115

Nov 2022 (London)

Revisiting RFC4916

- The “connected identity” draft, update to RFC4916
  - How to make Identity work in the backwards direction
  - RFC4916 covered 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
  - “Call stretching” 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
  - (Charter now reflects that)

There's a new version

- Significant departure from RFC4916 model
  - Now allows Identity in provisional and final responses: especially 180, 183, and 200
- Major revision to support that
  - Introduction of "rsp" PASSporT type
  - Rules for interaction with diversion
  - Also, we did not remove the from-change of RFC4916
    - But do we need it?

The “rsp” PASSporT Type

- A PASSporT type that can only be sent in responses
  - Not necessarily limited to SIP, but, covered here with SIP as the focus
  - “rsp” is signed like “div” – the signing PASSporT has authority for the “dest” field rather than the “orig”
- In the sunny day case, where there is no diversion, pretty simple really
  - When you receive a SIP request with an Identity header, you can send a response (18x, and 200) with an Identity header
    - Ultimately, you may get a couple 18x’s, so the 200 cements the called party identity
  - Good enough for SIPBRANDY ”mky” protection and other cases we care about
    - SIPBRANDY encourages UAC and UAS to act as AS/VS, say

Two caveats on “rsp”

1. Provisional responses are not reliable without 100rel
   - No guarantee this will work, in other words
2. There’s no SIP way to “reject” a response
   - Not even with a 401/407 – in other words, the AS can’t authenticate the response sender with a Digest challenge
     - AS also needs a Via (to be in transaction response path)
   - And if the VS wants to reject a PASSporT, none of our fancy status codes can be used in response to a 200 OK, say
- If you want to be able to reject Identity in the backwards direction, you need UPDATEs per RFC4916
  - But this is way simpler for the simpler cases

”rsp” Interaction with “div”

- In less sunny day cases, the “dest” in the original PASSporT is not the responding party
  - This is where “div” comes in
    - Additional Identity headers in responses can also contain “div”s received at the terminating side
  - Effectively, reflect the “div” chain back to the caller
    - Caveat: that reveals call logic – policy might not always allow
- If the “dest” in “rsp” is not the “dest” of the original PASSporT, MUST NOT send a “rsp” without at least one “div” also in an Identity header
  - Again, requirement is that the response AS actually sees the “div”s – not necessarily trivial
  - But if it doesn’t work, it doesn’t work – won’t always be possible

The case for from-change

- Easier to get the AS in the call path of a request than a response – and you can challenge a request
- It's not like there aren't cases where you'd want an UPDATE to reflect a new party on the other end
- In diversion cases, mid-dialog and dialog-terminating requests in the backwards direction will have the wrong From without from-change
  - So, if you're signing a BYE, your "orig" won't match the From header field value
    - Then again, a lot of people do sign P-Asserted-ID instead of From…
  - I guess the question is… so what?
    - Originating UA will know what Identity to expect – it can become part of the session state

So…

- So... Is this a good direction?
  - If so, will elaborate some more
    - Fancier ways to get the AS to sign responses
    - What new route hijacking attacks against this?
    - New option tag for criticality of connected-identity?
    - PAID in responses (for verstat purposes)?
    - Is there a use for “opt” here?
- Do we still need RFC4916 from-change in scope?
  - If so, we need build examples to reflect elimination of the Identity-Info header, etc.

Next Steps

- Still plenty to do here
  - But we think we need the functionality, for a variety of use cases
- Comments, revisions, etc.

Backup: Will the response AS work?

- A lot of AS's are actually just HTTPS interfaces hanging off an SBC
  - Call is going through them both ways anyway, and they munge stuff as it goes by either way
- Strict SIP AS's will need to be in the Via
  - Obviously no fancy redirects or anything possible, just straight proxying
  - Still, though, that just means the VS on the way in needs to add an AS Via for the way out (if they aren't already the same box)