

draft-ietf-stir-rfc4196-update-03

Connected Identity

STIR WG IETF 117

Jul 2023 (SF)

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)

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

There's a new version

- WGLC happened
- Thanks to Russ for a review
 - Removed changelog
 - Clarified non-dialog forming responses (3xx, etc.)
 - Filled in some of the back matter (IANA etc)
- I-D name really no longer applies – this will not formally “update” RFC4916, but eh
 - The RFC won't have the i-d name in it anymore

Next Steps

- Now post-WGLC
- Advance to IESG if everyone is cool with the fixes in my last revision