IETF 67 SIP meeting

draft-ietf-sip-connected-identity-02

Current status

- Finished WGLC (based on 01)
- 02 fixes all issues raised during WGLC, except one
- The exception concerns rejection of SIP requests by an RFC 4474 Verifier
- Although 02 does deal with this, it is not clear that there is community buy-in for this solution (more a lack of comment rather than violent opposition)

The issue

- What to do if mid-dialog request gets rejected by RFC 4474 Verifier?
  - RFC leaves it to policy whether to reject a request with 428 if Identity not present
  - RFC mandates rejecting with:
    - 436 if can't dereference URL in Identity-Info
    - 437 if there is a problem with the cert, or
    - 438 if the signature doesn't match

Discussion

- 428 avoidable if policy not to reject mid-dialog requests. Connected-identity draft can and does mandate this.
- 436/437/438 are bigger problems, because RFC 4474 mandates their use.
- Repeating a rejected request without Identity is not generally an option, because Authentication Service is typically at proxy, not at UAC.
- Rejecting a mid-dialog request just because certificate is not trusted (437) seems harsh

High level options

- No update to RFC 4474
  - Abandon dialog if get rejection – unsatisfactory?
  - Just ignore – unsatisfactory if connected-identity is not the sole purpose of the mid-dialog request
  - Retry with anonymous@anonymous.invalid – may mislead the user
- Connected-identity updates RFC 4474 for mid-dialog requests only (as proposed in 02)
- New document updates RFC 4474
  - For mid-dialog requests only, or
  - For all requests

Possible updating to RFC 4474

- Changes to Verifier behaviour – options:
  - MUST NOT issue a 428 response to a mid-dialog request
  - Make it a matter of policy whether to reject with 437 or accept a request with an untrusted signature
  - SHOULD NOT reject a mid-dialog request with 437
  - Remove Identity and Identity-Info when forwarding request with an untrusted signature

Issues with update to RFC 4474

- Weakens the security properties of RFC 4474
- Removal of Identity and Identity-Info from forwarded request that fails to verify denies a downstream Verifier the opportunity to verify
- On the other hand, leaving them there might mislead the UAS into assuming they have been verified – unless we require some positive indication like P-Asserted-Identity to be inserted to indicate that verification has occurred

Proposal

- Recommend that policy should be not to send 428 response to a mid-dialog request
- Abandon dialog if get back 428/436/437/438 response to a mid-dialog request
- Benefits of simplicity and maintaining the full security properties of RFC 4474
- Cons:
  - Possibly too harsh in case of 437
  - Receiver of 428/436/437/438 will not be able to send BYE, so verifier will need to do so