rfc4474bis-02

IETF 91 (Honolulu)

STIR WG

Jon

First principles (yet again)

Separating the work into two buckets:

1) **Signaling**
   - What fields are signed, signer/verifier behavior, canonicalization
2) **Credentials**
   - How signers enroll, how verifiers acquire credentials, how to determine a credential's authority for identity

- rfc4474bis is our signaling solution
  - But contains guidance for specifications of (2)

What we did since -01

- Added the mandatory signature over a=fingerprint
  - Also discussed how that interacts with baiting
  - We need to discuss a little more, though
- Integrated “canon”
  - Still more thinking to do here
- Split references
- Replaced IANA stub with some actual text
- Added some hooks for STIR prob-statement and threats

Open issues: On “canon”

- Is the latitude for local policy too broad?
  - Today “further transformations MAY be made”
- Today “canon” just covers the From
  - Should it cover the To as well?
    - Is the To more likely to transform than the From?
    - Does it need to, to prevent robocalling etc.?
  - canon=t:<TN1>;f:<TN2>
- Added some text saying that auth services can alter the To and From before signing
  - Obvious, and serves a different purpose than “canon”

Open Issues: On Gatewaying

- Previously, we had discussed the possibility of non-SIP protocols tunneling this cryptographic signature
  - This was a feature of Hadriel's stir-ikes-out
- Do we still want to try to make this work?
  - SS7 UUI, XMPP, others?
  - If so, I suggest this go in some separate specification
- But what about mandatory protection for a=fingerprint?
  - Gateways will cause fail
  - Is that would should happen?

Path Forward

- Should the Date threshold be an hour, or ten minutes, or lower?
  - Text currently inconsistent
- Do we want to do a compliance example?
  - Cullen and I built implementations for 4474
  - Be nice to get something the works
- Editing still needed, big ideas now in place?
  - Surely more legacy language needs an update
    - There's probably some chaff to cut here