rfc4474bis-04

IETF 93 (Prague)

STIR WG

Jon

What we did since -03

- Added some new text about PAI and "canon"
- Added a new mechanism, Identity-Extension

Open Issues: Signing PAI

- Sometimes, a TN lives in PAI (RFC3325)
  - Should it be signed instead of the From in those networks?
- New text:
  - Allows "canon" to reflect the PAI
  - In PAI-using networks, verifiers should be able to reconstruct the canon
    - Text notes the potential "canon" privacy leakage
- Does it really make sense even?
  - Trust domains (Spec(T), RFC3324) have transitive trust
  - What's the need for an end-to-end assertion
  - Should they interoperate with rfc4474bis environments
    - Does the PSTN itself?

Signing anything else

- CNIT and extensibility in general
- Defined a new Identity-Extension header
  - If present, contains a signature over fields in the SIP request
    - Which fields? Determined by the extension
    - Extensions identified with an IANA namespace
  - For CNIT, could be display-name, or anything else
- Signature is getting a little cluttered…

Eric's Comments

- Eric Burger sent some comments last night
- The gist is that there is protocol work here and "policy," and that these should be in separate documents
  - Concerned about the authentication service concept
  - For example, saying an authentication service MUST authenticate users before attesting their identity is "unenforceable and outside the scope of the IETF"
  - Also concerned about anonymous URIs of various kinds
- RFC4474bis does not set policies
  - It provides mechanisms designed to work with various policies

Next Steps?

- I noticed some brokenness in "canon" for To

  - This is actually left over from like IETF 91
  - Some text, but still inconsistencies

- Last call this, or wait?