rfc447bis

STIR WG / IETF 95
Buenos Aires, Apr 2016
Jon
Divide and Conquer

• draft-ietf-stir-passport now specifies the JSON object (replacing former verified-token)
  – Chris will talk about this later
  – It defines a “bare minimum” scope of protection
    • Syntax based on JWS
      – Works with protocols other than SIP
• Much of our task now is keeping passport synchronized with RFC4474bis as we finish
Changes since -06

• Passport alignment
  – Shifting to “otn” and “dtn” claims, etc.
  – Stronger typing: Chris will discuss

• Fix for the Date header

• Extensibility

• A toe-hold for “opportunistic” STIR

• Last couple months been a bit quiet... because everyone is happy, right?
Date Fix

• So, some intermediaries munge the Date header in the field
  – You are bad and you should feel bad
• The fix here is to allow auth services to resend requests with “canon” when verification fails
  – “canon” contains the base64 encoded JWS header/claims component of PASSporT
  – Date can be constructed from “iat” and used by the verifier to maintain integrity
  – Also, “canon” in general useful for debugging
  – This does have a privacy implication, though
Extensibility

• Largely this too is in baseline passport
• Identity header now has a “ppt” parameter
  – This mirrors a “ppt” appearing passport header
• What about different MIME types apart from baseline?
  – PASSporT could differentiate these...
    • It will be a different “typ” in PASSporT
  – But we need a SIP layer indication too
    • Gotta fix this – unless it’s just “canon”, then it’s already fine
  – Did we get extensibility right?
Opportunistic STIR?

- (for those that missed DISPATCH on Monday)
- Could STIR sign requests without vouching for the originator’s identity?
  - Added some “don’t rule this out” text to rfc4474bis
  - Would provide an auth service sig over the key fingerprints/hashes in SDP without identity
  - Ideally implemented in endpoint auth services
    - They might in turn use self-signed keys, even
    - Can be supplied in addition to “real” Identity header
Future work

• “mky” claim syntax still requires alignment
  – This will just defer to the passport spec
• Resolve extensibility in SIP for new PASSporT MIME types
• But otherwise, are we there yet?
• We need to get out the thumbscrews
  – After the -09, we will want detailed review
  – Last call, etc. – we need to get this done