STIR for Messaging

IETF **113i**

STIR WG

Virtual – Apr 2022

J Peterson

draft-ietf-stir-messaging-02

- A draft about leveraging STIR for text and multimedia instant messaging services
  - Helpful for those that use telephone numbers as identifiers, specifically for the originator of messages
    - For the moment, that's a scope restriction of the draft
- Why?
  - Message spam is a problem, and while email-style content analysis helps, it doesn't help for encrypted messaging
  - STIR certificates bestow authority for communication from a TN
    - Would make little sense to develop a separate PKI for messaging from telephone numbers

Integrity over messaging

- Two paths for STIR:
  1. SDP-negotiated message stream security
     - Aiming for RCS-like (or RTT-like) deployments
  2. Individual message (MESSAGE) security
     - Protects individual messages at the MIME level
       - Avoid worrying about SMPP or whatever
       - Useful for some emergency services applications
       - Still some doubts about whether this is too pat an answer
         - » At this point, I think it's worth putting out there and seeing how things are used

What is New

- Added some text on freshness
  - Traditional STIR expiry thresholds may not apply to store-and-forwarding message systems
    - But, PASSporTs have timestamps, message systems should be able to use this to prevent replays
- Added some text on CPIM metadata
  - Basically pointing to RFC8946
- Some other general wordsmithing

Open Issues

- Conferencing redux
  - Had some discussions about potentially looking at MLS
    - Pending a discussion about what it would look like for SIP overall to use MLS
    - Let’s not wait for that…

Next Steps

- Had some review, more welcome

- Close to WGLC here?