STIR for Messaging

IETF **111**

STIR WG

SF, from afar – Jul 2021

J Peterson

draft-ietf-stir-messaging

- Now a working group item
- 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
     - Previous group discussion was to protect individual messages at the MIME level
       - Avoid worrying about SMPP or whatever
     - Draft now just says that
       - Though likely underspecified – really just suggests taking a digest over the whole body
         - » Should be more narrow?

What Else is New

- Added some text on RTT
- Added some caveats on what “end to end” means
  - Inheriting the constraints of SIPBRANDY
- Cut out some TBDs and added some starting Sec Considerations
  - Will probably need privacy considerations too

Open Issues

- Conferencing (multiparty messaging)
  - For Path 1 (dialog streams), even two-party messaging requires connected identity
    - Which I'll be talking about in a minute (rfc4916bis)
    - The multiparty messaging is more of a problem
      - Various strategies for dialog conferencing in SIP overall
        - » Centralized v. decentralized
          - I gather RCS is centralized conferencing
        - » Or punt this to the connected identity draft?
  - For Path 2 (MESSAGE, etc.) should be okay?
    - Each individual message gets signed as appropriate

Next Steps

- Resolve open issues
- Had some review, more welcome

- WGLC after another rev or two?