STIR for Messaging

IETF 110
STIR WG
Prague, from afar – Mar 2021
J Peterson
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
    • The big question: who would use this?
Is there really a problem?

• Some reports that text-message spam isn’t a problem
  – I don’t know about anyone else, but I get plenty
  – Here’s an example from yesterday
    • Not the first time I’ve gotten this particular spam, even

• Other mitigation strategies exist
  – But STIR still can play a part
Is it in scope of STIR?

• As I said on the list, once “mky” was in scope, binding PASSporTs to media security became part of STIR
  – Differences between “mky” for DTLS/SRTP vs. MSRPoTLS are very unclear to me
    • “msgi” as well draws on the precedent of “rcdi”
      – Both deliver an immediate text/graphic message to users

• So, do we think there’s a material difference here?
Integrity over messages

• Some reluctance to open the can of worms about different integrity for different message formats
  – SMPP, email-style MMS, others

• Can we just do MIME-level security?
  – Yes, provided everything we want to cover is just MIME...

• Has some interaction with whether we want to do OOB
  – As Ben’s recent mail to the list suggested
Next Steps

• No shortage of open issues, but this is really a draft asking if we want to explore STIR for messaging

• Had some review, more welcome
  – Do we need work in this space?
    • If so, where do we set the scope?

• Adoption?