PASSporT divert

- IETF 103 (กรุ้งเทพา) STIR WG
- Nov 2018
A feature many people have asked about
  – How do we handle **retargeting**?
  – To header field of SIP is signed by PASSporT
    • Original SIP header value may be altered with retargeting
    • Looks like a cut-and-paste attack to the destination

We define a special PASSporT to track retargets
  – With its own “ppt” – “**div**” for “divert”

Different from History-Info and Diversion?
  – Yes, as it is signed by the original destination domain
  – Moreover, it only captures “major” changes
    • Thanks to our canonicalization procedures
What’s New in -04?

• Now nesting is a MUST
  – For in-bound and OOB
  – Note that there still can be multiple Identity headers for in-band, but “div” no longer will lead a new one
    • Just a longer one...

• Made “opt” independent of “div”
  – Just in case we want to nest PASSporTs for some other extension

• One more thing...
Pre-div in SHAKEN

• Signing the R-URI instead of the To
  – Why? To capture retargeting, as in the freephone case, where the original called number is in the To but the geographical number is in the R-URI
  – Would this change STIR? Yes, STIR expects you to sign the To
    • A gap opens where an attack could choose any original called number, effectively, and the destination would trust that redirection had occurred

• Is this a fix we should make? Alternatives?
Issues

• This is pretty close
  – ATIS has kicked the tires on this one, hard
  – Also see Mary’s H-I call flows doc

• Need some more editorial reviews?
  – Thanks Eric

• Last call time, methinks
draft-ietf-stir-oob

Out of Band

• STIR WG IETF 103 (กรุงเทพฯ)
• July 2018
Basic STIR Out of Band

Authentication and Verification Services are not just end-user devices
Next Steps

• In WGLC
• Need some editorial/content review, though
• Someone read it?