Service Provider OOB

IETF 108

STIR WG

Jon - @home – Apr 2020
A new draft about using OOB in a more constrained environment
  – Could you do security differently if you assume the CPS is not a third-party service?
    • Instead something operated by (or for) the originating or terminating domain?
  – i.e., what if the entity operating the CPS would already see call signaling?
    • And hence learn the called/calling party numbers

Descriptive of emerging efforts in the deployment of STIR
  – Not a science project, aiming for PS
Solution Components

• Currently focused on the CPS being operated by the terminating service provider
  – Use OOB REST interface to store PASSporTs at destination
• Thus, no need to encrypt PASSporTs
  – They go directly from the originating to terminating provider
    • Gateways? Maybe, but only if they have a trust relationship with the originating or terminating provider
• “CPS Advertisement”
  – Some means of making available the CPS discoverable to calling service providers
    • Propose a signed JSON object
Service Provider OOB

CPS is part of the terminating administrative domain, maybe composed with VS.
Terminating Side CPS

• May be composed with the OOB-VS
  – Or may be a push interface to the VS
  – Still allows CPS to be run by a third party on behalf of the terminating SP
    • Multiple CPS instances may be housed in the same deployment, each pointing to a particular terminating SP

• Verification process otherwise follows OOB
  – Correlate PASSporT with call signaling

• No need to worry over attackers querying the CPS to learn call state data
  – CPS is effectively a one-way street
Next Steps

• Review
  – Do we need this draft?
  – There is a parallel effort at ATIS, aiming in particular at the SHAKEN IPNNI space
    • I think the considerations here are more generic

• Adoption?
BACK UP