An Origin Attribute for the STUN Protocol

draft-ietf-tram-stun-origin-06

Alan Johnston <alan.b.johnston@gmail.com>
Justin Uberti <justin@uberti.name>
John Yoakum <yoakum@avaya.com>
Kundan Singh <kundan10@gmail.com>

Recent Changes

- List discussion after IETF-93
- Version -06 changes
  - Only share ORIGIN when STUN/TURN URI domain matches ORIGIN domain (Details on next slide)
    - No new meta-data is generated
    - Still covers many use cases (details on slide after next)
  - Removed text on sending empty ORIGIN attribute - just don’t send
  - Removed different handling based on usage (web, SIP, XMPP, etc) - just handle all the same
  - Should clear DISCUSSes

New Origin Matching Rules

- An ORIGIN attribute MUST NOT be included in a STUN or TURN request if the fully qualified domain name (FQDN) of the Origin does not match the FQDN of the STUN or TURN URI which was used to reach the STUN or TURN server.
- The FQDN comparison does not include ports or URI schemes.
- Examples:
  - A web origin of http://foo.example.com:8080 matches a TURN URI of turn:foo.example.com
  - A SIP origin of sips:bar.example.org:5061 matches a STUN URI of stun:bar.example.org:999

Use Cases Supported

- Single tenanted STUN/TURN server
  - Allows operator to only respond to STUN/TURN requests from own domain
- Multi tenanted STUN/TURN server
  - Allows for realm selection for challenge
  - Allows for logging/policy of usage based on domain
- Potentially firewall traversal
  - e.g. draft-jennings-behave-rtcweb-firewall

Way Forward

- Is WG OK with these changes?
- If so, authors will work to get DISCUSSes cleared and this work finished!