

An Origin Attribute for the STUN Protocol

draft-ietf-tram-stun-origin-05

Alan Johnston <alan.b.johnston@gmail.com>

Justin Uberti <justin@uberti.name>

John Yoakum <yoakum@avaya.com>

Kundan Singh <kundan10@gmail.com>

Recent Changes

- Completed IETF LC in May 2015
- IESG Telechat in May 2015
 - Three DISCUSSEs (next slides)
 - Details at
 - <https://datatracker.ietf.org/doc/draft-ietf-tram-stun-origin/ballot/>
- No consensus among authors on path forward

Barry's DISCUSS

- Questioned MUST/SHOULD and empty ORIGINS
- Questioned SHOULD NOT for ICE and other usages
- Question about Multiple ORIGINS
- We resolved these issues on mail

Stephen's DISCUSS

- Draft runs “counter to e.g. RFC 7258 or to the general trend towards data minimisation”
- In telechat and other conversations, argued the benefits (REALM selection for multi-tenanted TURN server 401 challenge) wasn't worth the increased meta data generated
 - Turns out that WebRTC doesn't need this anyway, REALM is essentially ignored
- My personal opinion: He's right

Alissa's DISCUSS

- Supports Stephen's DISCUSS
- Concerned about clients lying about ORIGIN
 - Not really a problem
- Logging is not sufficient justification
- My personal opinion: She's also right

Way Forward

- Lots of discussion among authors and ideas, but no consensus
- Ideas discussed:
 - Only share ORIGIN when STUN/TURN URI domain matches ORIGIN domain
 - Make ORIGIN opt-in only
 - Make ORIGIN an extension to RETURN (draft-ietf-rtcweb-return)
 - Only shared with a Border TURN Proxy not any Application TURN server or STUN server
 - Useful for policy decisions and some logging

Feedback and Other Ideas

- Most welcome...