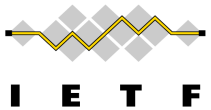
Session Traversal Utilities for NAT (STUN)

draft-ietf-tram-stunbis

Marc Petit-Huguenin, Gonzalo Salgueiro

IETF-92

Dallas, March 26, 2015

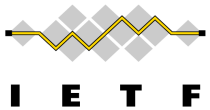


Changes Since -00

- Addressed reported Errata
- Move the Acknowledgments and Contributor sections to the end of the document, in accordance with RFC 7322 section 4.
- Make clear that the cache RTO is discarded only if there is no new transactions for 10 minutes
- Added more C snippets to Appendix A

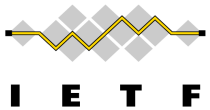
Changes Since -00

- Merge of STUN URI (RFC 7064)
  - DNS discovery is done from the URI.
  - Reorganized the text about default ports.



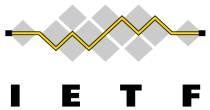
Changes Since -00

- Merge of STUN over DTLS (RFC 7350)
  - Split the "Sending over..." sections in 3.
  - Add DTLS-over-UDP as transport.
  - Update the cipher suites & cipher/compression restrictions.
  - A stuns URI with an IP address is rejected.
  - Update the STUN Usages list with transport applicability.



Changes Since -00

- The RTP delay between transactions applies only to parallel transactions, not to serial transactions. That prevents a 3 RTT delay between the first transaction and the second transaction with long term authentication.

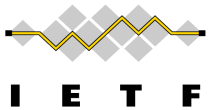


Changes Since -00

- Add a new attribute ALTERNATE-DOMAIN to verify the certificate of the ALTERNATE-SERVER after a 300 over (D)TLS.
- Added support for DANE in resolution algorithm
- Prevent the server from allocating the same NONCE to clients with different IP address and/or different port. This prevents sharing the nonce between TURN allocations in TURN.

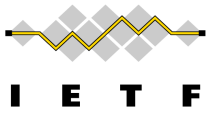
Changes Since -00

- Describe the MESSAGE-INTEGRITY/MESSAGE-INTEGRITY2 protocol.
  - As simple as possible
  - MI2 is only SHA256
  - First transaction you must put MI/MI2
  - Subsequent transaction you use either
  - MI2 comes after MI so it can be comprehension mandatory



Changes Since -00

- Add negotiation mechanism for new password hash algorithms.
  - Server proposes a list of algorithms, client chooses one.
  - Magic prefix in NONCE and repeated algorithm list in subsequent authenticated transaction protect against bid down attacks.
  - What hash algorithm do we want? (aligned with HTTP/SIP?)



Changes Since -00

- Add text saying ORIGIN can increase a request size beyond the MTU and thus require an SCTPoUDP transport.
- Add support for SCTP to solve the fragmentation problem.
  - Selected SCTPoDTLS in order to match WebRTC
  - Changed prefix to use 8 bits instead of 2
- Simpler solution would be STUN PMTUD (draft-petithuguenin-tram-stun-pmtud-00)

Next Steps

- Do we need to integrate RFC 5769 (stun vectors) as additional examples in STUNbis?
- Update of Security Considerations pending
- Update of IANA Considerations section
  - Remove text making initial registrations
  - Update STUN Methods registry from RFC 5764 demux update draft-petithuguenin-avtcore-rfc5764-mux-fixes
- Additional reviews requested