STUNbis

Marc Petit-Huguenin
Gonzalo Salgueiro
2017-03-28

Since IETF 96 in Berlin

We did a protocol analysis of the Long-Term Credentials Mechanism (LTCM) in RFC 5389 and found a bunch of issues that were then fixed in STUNbis, with assistance from Jonathan Lennox:

- Packets discarded in a reliable or unreliable transaction triggers an attack error instead of a timeout error. An attack error on a reliable transport is signaled immediately instead of waiting for the timeout.
- Explicitly state that a received 400 response without authentication will be dropped until timeout.
- Clarify the SHOULD omit/include rules in LTCM.
- If the nonce and the hmac are both invalid, then a 401 is sent instead of a 438.
- The 401 and 438 error response to subsequent requests may use the previous NONCE/password to authenticate, if they are still available.
- Change "401 Unauthorized" to "401 Unauthenticated"
- Makes clear that in some cases it impossible to add a MI or MI2 even if the text says SHOULD NOT.

More changes

With LTCM fixed, we could then restart doing the editing on what was decided in Berlin:

- Removed the reserved value in the security registry, as it does not make sense in a bitset.
- Updated the minimum truncation size for M-I-256 to 16 bytes.
- Changed the truncation order to match RFC 7518.
- Stated that STUN Usages have to explicitly state that they can use truncation.
- Removed truncation from the MESSAGE-INTEGRITY attribute.
- Add reference to C code in RFC 1952 (Jonathan
- Replaced RFC 2818 reference with RFC 6125 reference and aligned the TLS verification (Olle and Martin discussion).

And even more changes

And one final cleaning of LTCM:

- Made clear that the same HMAC than received in response of short term credential must be used for subsequent transactions.
- The "nonce cookie" is now mandatory to signal that SHA256 must be used in the next transaction.

Hash Agility

- The end (of SHA-1) is upon us!
- Should we revisit hash agility?
- Bid down attack protection is really under-specified at the IETF (and elsewhere).

Happy Stunballs

Olle Johansson invited us to consider the interactions of Happy Eyeballs with STUN. We did not yet came to a conclusion, but we did some analysis of the problem:

- Happy Eyeballs would be specific to each STUN Usages. E.g. it does not make sense with Connectivity Checking (RFC 5245), Media Keep-Alive (RFC 5245), SIP Keep-Alive (RFC 5626) and Consent Freshness (RFC 7675), although both candidates and c= lines in ICE could carry a domain name.
- For NAT Discovery (RFC 5389) and NAT Behavior Discovery (RFC 5780), Binding is idempotent, so it is not an issue to send both IPv6 and IPv4 at the same time. But the network element probably already knows what protocol it wants to use.
- The situation for TURN is different, as Allocate transactions are not idempotent. But that's an issue better left to turnbis.