A TLS Flags Extension

Yoav Nir – IETF 105

TLS Extensions

- TLS 1.3 currently has 28 extensionTypes defined.
  - TLS 1.2 had 46.
  - Many more are proposed.
- Some of them carry data, but some (like post_handshake_auth) carry no data at all, while others (such as early_data) do not carry data in some contexts (CH & EE in the case of early_data).
- They carry 1 bit of information: their presence indicates something.
- We'll call them "flag extensions".
- Each such extension takes 4 bytes: two for type; two for length.
- Which makes my inner engineer sad.

TLS Flags Extension

- It is proposed to create a single extension for these flags.
- This extension will carry a bunch of 1-bit indications in a more efficient way.
- The actual format is to be decided in the future by the group.
- This really short slot is for deciding if the group wants to get into this.
- Of course I couldn’t help myself and added a few proposed formats in the following slides.
- But the big question is: Do we want to do this?

Proposal #1: 32-bits

- The extension will have an extension_data field that is 4 octets long.
  - A total of 8 octets with the extension header.
- It will be present in all ClientHello / EE messages.
- Up to 32 flags can be supported.
  - A zero bit in the appropriate place says the flag is not set
  - A one bit says that it is.
- If we ever define a 33rd flag, we'll need a new extension.
  - We can hope it won't come to that.
  - But TLS 1.2 has 46 extension (not all flags, but still…)

Proposal #2: As many bits as needed

- One extension.
- Flags are numbered from zero to as many as we want to define.
- Extension_data field is as long as needed to include the last octet that has a set flag.
  - For example, if we want to set flags 1,2, 9, and 23 we need three bytes.
  - All flags whose bits are zero or not present are unset.
- Hopefully we can allocate the values in a smart enough way that all flags that are often set will have a low number.