TLS 1.3

`draft-ietf-tls-tls13-21`

Eric Rescorla

Mozilla

`ekr@rtfm.com`

Status

- Now in draft-21
- WGLC#2 ended yesterday

Changes Since -19

- Shorten HKDF labels (20)
- Make post-handshake auth implementation option (and controlled by an extension) (20)
- Add a per-ticket nonce so each ticket is associated with a new PSK (21)
- Extensive new section on 0-RTT and anti-replay

Mandatory Anti-Replay?

- We currently require the you do bounded anti-replay at SHOULD level
- Ben Kaduk on-list suggests that we should make this mandatory
  - Probably not a specific technique but require some bounded mechanism
- This didn't seem to have consensus, but...

PR #1053: Hashes that aren't hashes (1)

```
HKDF-Expand-Label(Secret, Label, HashValue, Length) =
     HKDF-Expand(Secret, HkdfLabel, Length)

Where HkdfLabel is specified as:

struct {
    uint16 length = Length;
    opaque label<7..255> = "tls13 " + Label;
    opaque hash_value<0..255> = HashValue;
} HkdfLabel;
```

- This isn't a hash in some cases
- Proposal change the name to "context"
- Additional proposal: Derive-Secret often called with Label = `""`
  - Special case this so we don't have to compute `Hash("")`

Placeholder: NAT/Middleboxes

- TLS 1.3 shows increased connection failure rates in the field
  - Hard to get clear measurements, but probably the 1-10% range
  - Problem seems to be middleboxes
- Currently studying various approaches
  - Make connection look less like TLS 1.2 (PR#1051)
  - Make flight look more like TLS 1.2 (maybe like resumption?)
  - Fallback paired with middlebox fixing
  - More data needed.
- More soon (next few months)

Other issues?