DTLS 1.1

Eric Rescorla
Network Resonance
ekr@networkresonance.com

Overview

- Update to match TLS 1.2
  - Mostly `s/TLS 1.1/TLS 1.2/`
- Clarify confusing points in the spec
- No other changes

TLS 1.2 Upgrade

- DTLS 1.0 is a delta off TLS 1.1
  - This is intentional
  - Not clear you can just pick a random version (cf. TLS 1.0)
- But now TLS 1.2 is out
  - Need to upgrade
- Proposal: Rev DTLS version to 1.1 and have it matched to TLS 1.2
  - Question: would it be better to go to 1.2 to match versions?

Known Issue 1: HelloVerifyRequest and CertificateVerify

- S 4.1.2. specifies that the first ClientHello and HelloVerifyRequest are not included in Finished
- Nothing is said about CertificateVerify
- Proposal: it's not included there either

Handshake Headers and Hashes

- DTLS handshake messages are:

```
struct {
  HandshakeType msg_type;
  uint24 length;
  uint16 message_seq;                              // New field
  uint24 fragment_offset;                          // New field
  uint24 fragment_length;                          // New field
  ...
}
```

- How are handshake hashes computed with fragmentation
  - Reassemble and then hash
  - Include the headers?
    - This isn't clear in the spec (answer is "yes" in TLS)
- Proposal: change the text to make this clear

Planned Timeline

- Gather other issues
  - Call on the mailing list
  - Have them by 31-April-08
- Discusss contentious issued on mailing list
- New draft by 31-May-08
- Resolve final contentious issues in Dublin