Transport Layer Security (TLS)
IETF-82

Chairs:

Joe Salowey

Eric Rescorla

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **The IAB or any member thereof on behalf of the IAB**
- **The RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

TLS Agenda

1. Administrivia (5 min)
Note takes, blue sheets, Note Well, Agenda

2. Document Status (20 Min)

3. TLS Origin-Bound Certificates (20 min) - Wan-Teh Chang
http://tools.ietf.org/html/draft-agl-tls-encryptedclientcerts
http://tools.ietf.org/html/draft-balfanz-tls-obc

4. Next Protocol Negotiation (20 min) - Wan-Teh Chang
http://tools.ietf.org/html/draft-agl-tls-nextprotoneg
(also http://technotes.googlecode.com/git/nextprotoneg.html)
http://tools.ietf.org/html/draft-agl-tls-nextproto

5. TLS out-of-band public key validation (10 min)
http://tools.ietf.org/html/draft-wouters-tls-oob-pubkey

6. PWD Key Exchange (20 min) - Harkins
http://tools.ietf.org/html/draft-harkins-tls-pwd

Active Document Status

- DTLS Heartbeat

  Discuss: Are the request and response messages too similar leading to an attack vector in some TLS cipher suites?

- DTLS 1.2

  Auth48 waiting for author response

Queued Documents

- AES-CCM ciphers
  - Used by Zigbee
  - Standards track for RSA and ECC (new IPR statement)
  - Will ask list if there are any objections to this
- Extensions
  - TLS-OBC
  - TLS-Next Protocol Negotiation
  - TLS Out-of-band public key validation
  - Multiple OCSP Response

Process for Extensions (cont'd)

RFC 5246 defines an extensibility mechanism for TLS based on extensions signaled in the ClientHello and ServerHello. With TLS 1.2 and DTLS 1.2 being relatively stable, we are starting to see more proposed extensions, some of which, if used, represent significant changes to the TLS processing model or state machine. RFC 5246 requires IETF consensus for any extension, either through individual submission to an Area Director or to the TLS Working Group (for as long as the WG exists).

Any proposed extension can be brought to the Security Area Director as an individual submission for IETF consensus; it can also be brought directly to the TLS WG. In the former case, the Area Director will decide whether he/she believes the extension needs to be

Process for Extensions

processed through the TLS WG or just to process it through IETF Last Call. This decision will be made based on the level of impact the extension would have on TLS. Specifically, any extension which would cause a significant change to the TLS processing model or state machine will be referred to the TLS WG. The Security Area Director may also ask the WG chairs and other active TLS participants ahead of time about whether or not a particular proposal should be processed (if at all) in the TLS WG. The AD may decide not to allow an extension to progress based on feedback from the working group and other sources.

In the case of drafts going through IETF Last Call, the TLS WG mailing list will be informed of the IETF Last Call ahead of or concurrently with the Last Call.