TLS Working Group
IETF-88

Chairs

Eric Recorla

Joe Salowey

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**
- **Any Birds of a Feather (BOF) session**
- **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.

Agenda

1. Administrvia (5 min) - Blue Sheets, Note Takers, etc.
2. Document Status and TLS related work (10 Min)
   DICE, HTTPbis & ALPN, Apps Area TLS BCP
3. ALPN (15 Min) - draft-ietf-tls-applayerprotoneg
4. TLS BCP (15 min) - draft-sheffer-tls-bcp
5. Updating Cipher Model (20 min)
   draft-gutmann-tls-encrypt-then-mac and AEAD
6. Stream Ciphers (20 min)
   ChaCHa - draft-agl-tls-chacha20poly1305
7. Hardware Considerations for TLS Key Generation (5 Min)
8. TLS 1.3 (60 min)

TLS Related Work

- DICE – DTLS in constrained environments
- HTTPbis – ALPN
- Apps Area – BCP on TLS use in Apps

Draft Status

- draft-ietf-tls-applayerprotoneg – WGLC done, HTTPbis OK
- draft-ietf-tls-oob-pubkey – Waiting for proto write-up
- draft-ietf-tls-cached-info – New rev, ready? DICE have a look?
- draft-ietf-tls-pwd – Start working group last call this week

ALPN

TLS-BCP

Updating Cipher Model

- Encrypt-then-MAC for TLS and DTLS
  - draft-gutmann-tls-encrypt-then-mac
- Use AEAD approach
  - draft-mcgrew-aead-aes-cbc-hmac-sha2-02

Encrypt-then-MAC Extension

- TLS extension to signal change from MAC-then-Encrypt to Encrypt-then-MAC
- Any TLS version that handles extensions could take advantage of this approach (not for SSLv3)

- Q: Insecure version fallback issue
- Q: Clarify MAC length for computation

AEAD Approach

- Define new TLS AEAD ciphers for Encrypt-then-MAC

  for example, AEAD_AES_128_CBC_HMAC_SHA1
- TLS 1.2 already supports AEAD

Q: Previous version support - define AEAD for earlier TLS versions as necessary

Q: Need to resolve plaintext length for MAC computation

ChaCha20

TLS PRF Issues

TLS 1.3