Transport Layer Security (TLS)

IETF-72, Dublin
July 27, 2008
Chairs:

Eric Rescorla <ekr@networkresonance.com>
Joseph Salowey <jsalowey@cisco.com>

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

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) 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 3978 (and RFC 4748) 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.

Agenda

- Administrative (5 Min)
  Blue Sheets, agenda
- TLS 1.2 Status (10 min)
  draft-ietf-tls-rfc4346-bis-10.txt
- Extension Definition Status (15 min)
  draft-ietf-tls-rfc4366-bis-02.txt
- Cipher suite Status (10 min)
  draft-ietf-tls-ecc-new-mac-07.txt
  draft-ietf-tls-rsa-aes-gcm-03.txt
  draft-ietf-tls-des-idea-02.txt
  draft-ietf-tls-psk-new-mac-aes-gcm-01.txt
  draft-ietf-tls-ecdhe-psk-01.txt
- DLTS Update (15 min)
  draft-ietf-tls-rfc4347-bis-00.txt
- Keying infrastructure based on TLS (15 min)
  draft-urien-tls-keygen-00.txt
- Camellia Cipher Suite (15 min)

TLS 1.2

- Auth-48 Issue
  - Handling of version mismatch in pre-master secret to avoid side-channel attacks
  - Resolution to keep document as is

Extension Definition Status (4366-bis)

- Mandatory Hash in Client Certificate URL
  - Change current definition vs. Create new extension
  - Add hash agility
- Truncated HMAC
  - MUST (instead of MAY) discard packets that are too long?

Cipher Suite Drafts

- Waiting on completion of TLS 1.2
  - draft-ietf-tls-ecc-new-mac-07
  - draft-ietf-tls-rsa-aes-gcm-03
- Others waiting on progress of extensions and extractor
  - draft-ietf-tls-des-idea-02.txt
  - draft-ietf-tls-psk-new-mac-aes-gcm-01.txt
  - draft-ietf-tls-ecdhe-psk-01.txt

DTLS 1.2

- Mainly clarification
- New PMTU text
- Other issues raised
  - What to do with invalid cookies
  - Header alignment

TLS Key Generation
(draft-urien-tls-keygen-00)

- Pascal Urien

Camellia Cipher Suites

- Satoru Kanno