TCP Increased Security (tcpinc)

Chairs:
David Black <david.black@emc.com>
Mirja Kühlewind <mirja.kuehlewind@tik.ee.ethz.ch>

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.

Administrativa

Today's slides

http://datatracker.ietf.org/meeting/94/materials.html#tsv

Remote participation

Audio: http://ietf94streaming.dnsalias.net/ietf/ietf947.m3u

Meetecho: http://www.meetecho.com/ietf94/tcpinc

Jabber chat

xmpp:tcpinc@jabber.ietf.org?join

Mailing list

tcpinc@ietf.org

What happened so far…

- First WG meeting in Jul'14 with two candidate solution proposals: TCP-TLS vs. tcpcrypt

- WG was not able to make a decision for one proposal so far

- Sep'15: Adopt of TCP-ENO as wg item (TCP Encryption Negotiation Option)

- Nov'15: Adoption of tcpcrypt and TCP-TLS

3 possible ways forward

1. Both approaches (naturally) converge into one approach.

2. We work on both approaches to get them into a (similar) state where the wg is able to make a decision (and withdraw the other doc).

3. We publish both approaches as different 'versions' of tcpinc that can be negotiated in the TCP-ENO handshake, where at least one of them is mandatory to support/implement.

Next step(s)

- Assign shepherds to all current wg items: tcp-eno, tcpcrypt, TCP-TLS

- Additional editor needed for TCP-TLS

- Intent to ask for expert reviews for both docs (tcpcrypt and TCP-TLS) by **mid/end of Feb’16**

Implementation Status

- tcpcrypt: https://github.com/sorbo/tcpcrypt
  - userspace implementation for Linux, Windows and Mac
  - kernel implementation will be updated
- TCP-TLS: work-in-progress userspace implementation using divert sockets and based on NSS/libssl (hopefully Nov or early Dec)

- Anybody working on further implementations?

- Plans for kernel implementations?

Milestones

Nov 2015 Adopt first WG document on unauthenticated key exchange mechanism and extensions to current TCP

Mar 2016 Adopt first WG document on extended API

Jul 2016 Submit unauthenticated key exchange mechanism and extensions to current TCP to IESG for publication as Experimental

Aug 2016 Submit extended API to IESG as Informational

Agenda

13:00 WG Status & Agenda Bashing (*Chairs*)

13:15 TCP-ENO: Encryption Negotiation Option (*Andrea Bittau*)
draft-ietf-tcpinc-tcpeno-00

13:45 Interface Extensions for TCPINC (*David Mazieres)*
draft-bittau-tcpinc-api-00

14:30 Cryptographic protection of TCP Streams (tcpcrypt) *(Andrea Bittau)*
draft-ietf-tcpinc-tcpcrypt-00

15:00 TCP Use TLS Option Encryption (*Eric Rescorla*)
draft-ietf-tcpinc-use-tls-00