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.

TCPINC

IETF-97
Friday, November 18, 2016

WG Chairs: David Black, Kyle Rose

Agenda

Chair update

- 10 minutes

TCP-ENO: Encryption Negotiation Option

- David Mazières
- 40 minutes

tcpcrypt: Cryptographic protection of TCP Streams

- Andrea Bittau
- 40 minutes

CFRG Questions

- Kyle Rose
- 20 minutes

Open mic

Since Berlin...

New versions of ENO (-06), tcpcrypt (-03), and API (-01) drafts:

- Incorporated feedback from prior reviews
- Clarified language around SYN data and URG/FIN bits
- Altered terminology based on discussions in Berlin session
- Moved tcpcrypt API into shared TCPINC API document

Chairs requested feedback from CFRG on some crypto issues

Milestones

Jan 2017	Submit extended API to IESG as Informational
Dec 2016	Submit unauthenticated key exchange mechanism and extensions to current TCP to IESG for publication as Experimental
Apr 2016 (Done)	Adopted first WG document on extended API draft-ietf-tcpinc-api
Nov 2015 (Done)	Adopt first WG document on unauthenticated key exchange mechanism and extensions to current TCP draft-ietf-tcpinc-tcpcrypt draft-ietf-tcpinc-tcpeno draft-ietf-tcpinc-use-tls

TBD...

Finalize tcpcrypt document

- Ready for WGLC?

Finalize TCP-ENO document

- Ready for WGLC?

Work on API document

- Most discussion so far debating socket API vs. abstract API
- Need to decide on approach and then complete the document

Related placeholder draft:

- TCPINC middlebox probing: still looking for co-authors with middlebox experience (“NAT traversal scars”)

Call for Implementors

TCP-ENO and tcpcrypt need independent implementations developed from the specifications in the documents

Doesn’t have to be a kernel-level implementation: even one based on modifications to a userspace TCP stack would help demonstrate completeness and usability of protocol spec