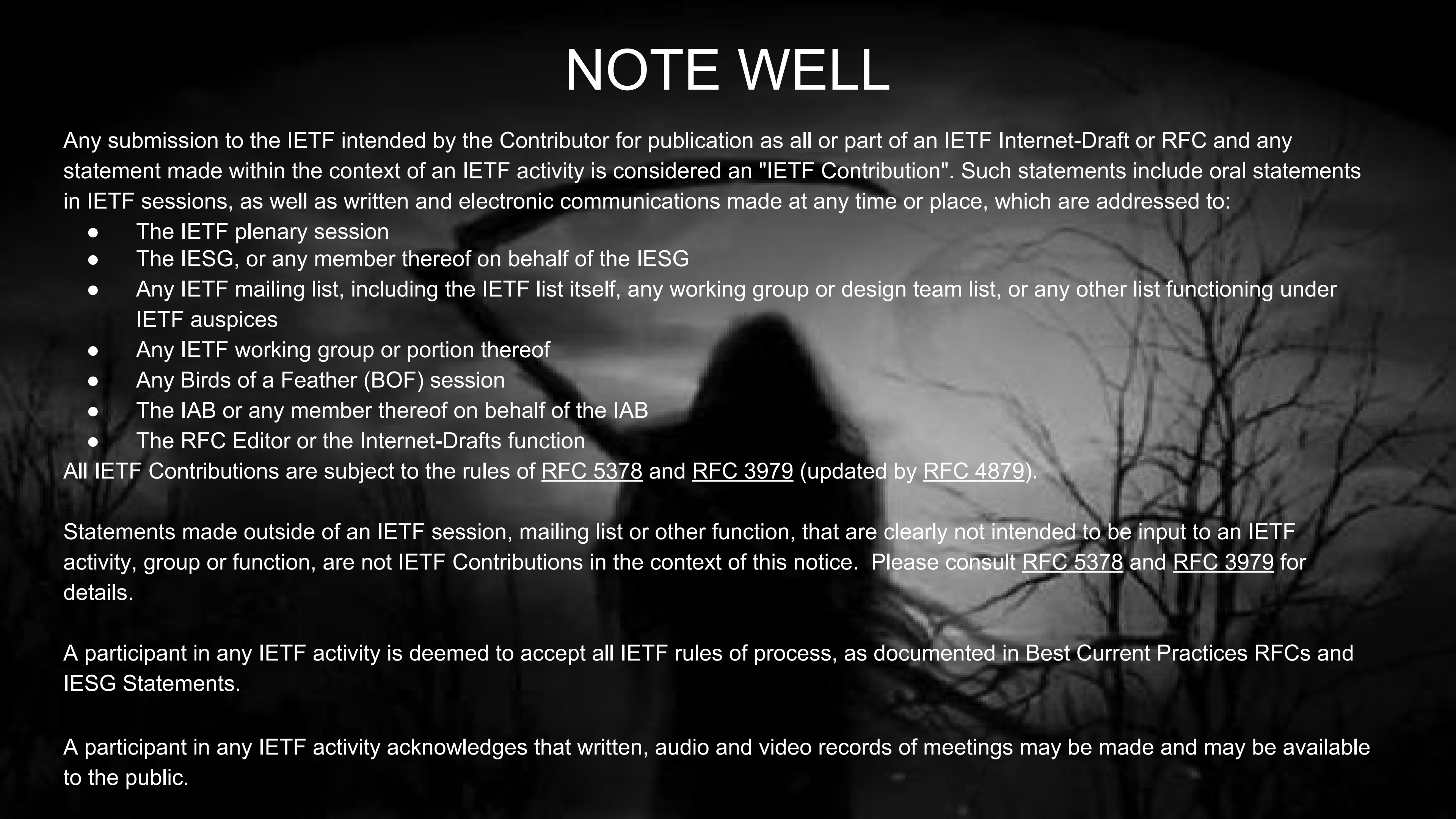

NOTE WELL

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-95
Thursday, April 7, 2016

WG Chairs: David Black, Mirja Kühlewind, Kyle Rose

Since Yokohama...

Rough consensus on approach to simultaneous open:

- There is no requirement for tcpinc to support all possible TCP-SO cases in all circumstances; but
- tcpinc should support TCP-SO when it can do so cheaply; and
- tcpinc setup failures for TCP-SO should result in proceeding unencrypted.

Rough consensus on a path to meet the WG's milestones:

- Move forward on a path to standardization of tcpcrypt and TCP-ENO
- Allocate code points for TLS and ensure TCP-ENO can support negotiating the use of TLS when that profile is ready for standardization

Since Yokohama...

Expert reviews of tcpcrypt are complete, and have been posted to the list:

- Yoav Nir
- Jana Iyengar

The chairs thank them for their efforts!

Updated drafts:

- tcpcrypt
- TCP-ENO
- Interface Extensions for TCP-ENO

Placeholder related draft:

- TCPINC BCP: seeking co-authors with middlebox experience

Milestones

Aug 2016	Submit extended API to IESG as Informational
Jul 2016	Submit unauthenticated key exchange mechanism and extensions to current TCP to IESG for publication as Experimental
Mar 2016 (Overdue)	Adopt first WG document on extended API draft-bittau-tcpinc-api
November 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

Call for Implementors

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

Agenda

TCP-ENO: Encryption Negotiation Option

- David Mazières
- 30 minutes

Interface Extensions for TCP-ENO

- David Mazières
- 20 minutes

Negotiation of Userspace TLS using TCP-ENO

- Eric Rescorla
- 10 minutes

tcpcrypt: Cryptographic protection of TCP Streams

- Andrea Bittau
- 40 minutes

Open mic

TCPINC-use-TLS Status

- TLS WG hard at work finalizing TLS 1.3
- Completion of TLS 1.3 a prerequisite for TCPINC profile
- TLS 1.3 is the first priority at this time for TLS experts

Conclusions:

- Proceed toward standardization of tcpcrypt and TCP-ENO
- Make sure ENO can be used to negotiate TLS later

Next Steps: Using TCP-ENO to support app-layer TLS

- Need a short draft showing either:
  - that TCP-ENO and the API suffice to negotiate either user-mode TLS or a TCPINC profile; or
  - that enumerates the changes required to allow for such support
- Allocate code points for TLS
  - IANA registry?