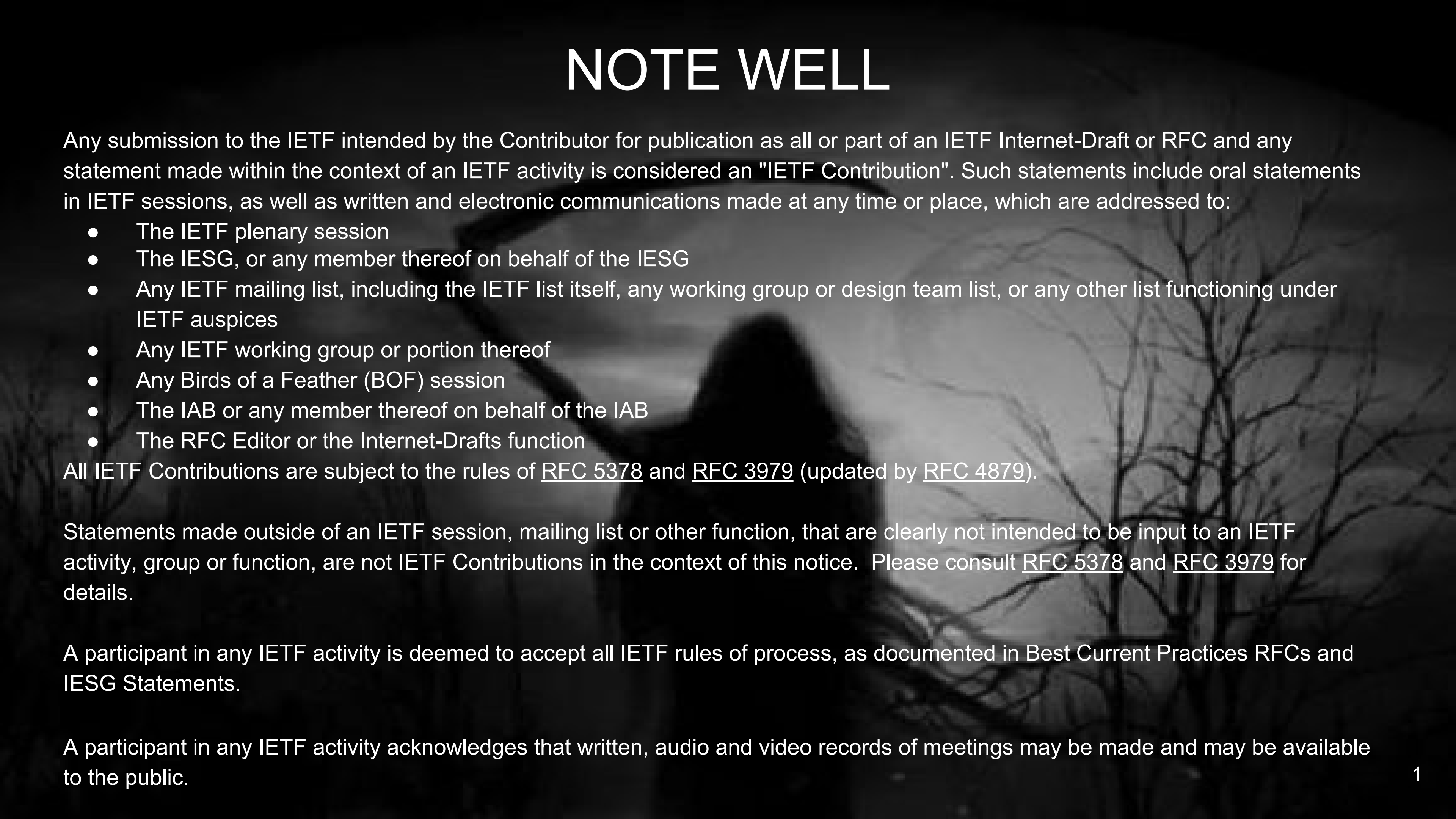

NOTE WELL

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-96
Tuesday, July 19, 2016

WG Chairs: David Black, Kyle Rose

Since Buenos Aires...

Adopted API document

- Need to decide on approach

Assignment of TCP option ExID

- Using ExID 0x454E
- All use of TCP option number 69 has been prohibited in both drafts, and that option is no longer supported by the reference implementation

New versions of both ENO (-03) and tcpcrypt (-02) drafts:

- Incorporated feedback from prior reviews
- Several technical reviews of each new draft already

Mirja stepped down as chair

- Now Transport AD (congratulations!)
- Many thanks to Mirja for her contributions as a chair!

Milestones

Aug 2016 (likely delayed)	Submit extended API to IESG as Informational
Jul 2016 (likely delayed)	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

- Document restructured to separate normative protocol description from design discussion
- No major recent protocol changes
- Close to 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

Finalize TCP-ENO document

- Document restructured to improve clarity
- Resolve remaining issues
  - ‘a’ and ‘m’ bits
  - Terminology (“spec”)
- Additional reviews expected and encouraged

Related placeholder draft:

- TCPINC BCP: 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 of normative protocol spec

Agenda

TCP-ENO: Encryption Negotiation Option

- David Mazières
- 40 minutes

tcpcrypt: Cryptographic protection of TCP Streams

- Andrea Bittau
- 40 minutes

TLS privacy negotiation using TCP-ENO

- Dave Plonka
- 20 minutes

Open mic