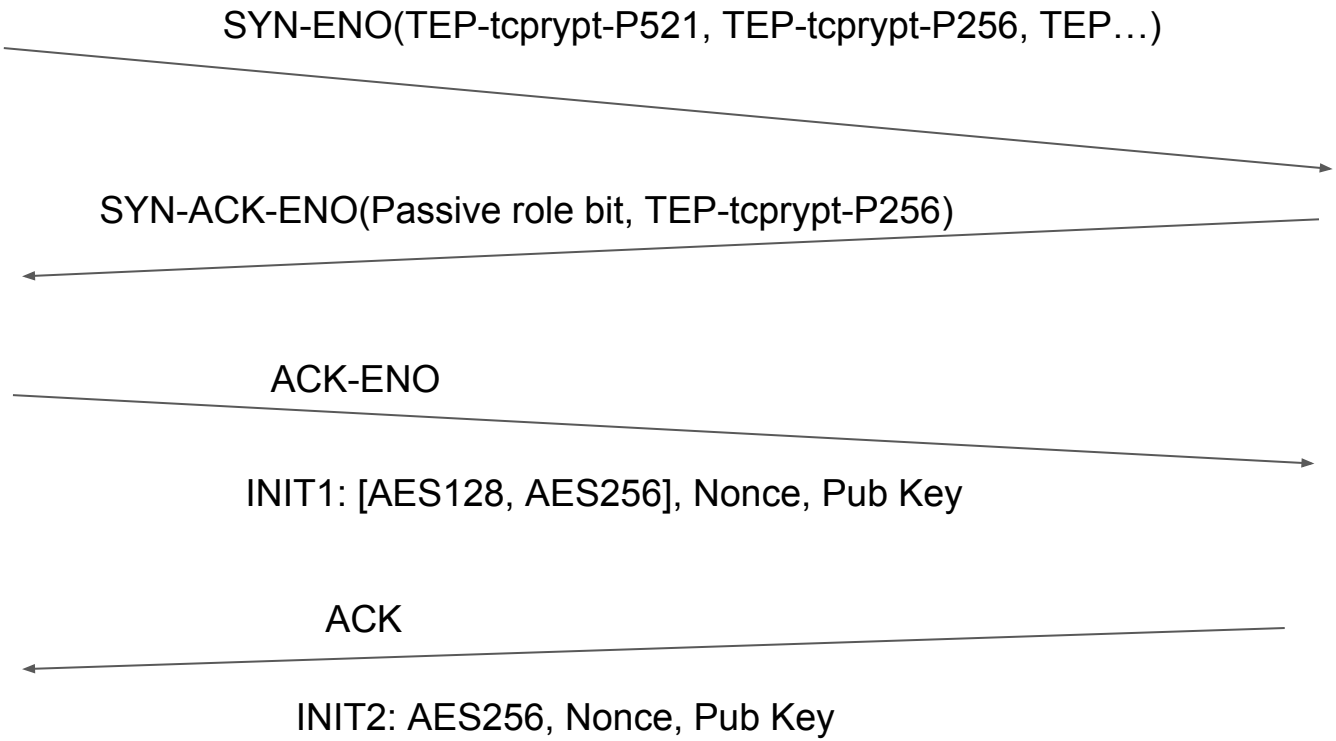
tcpcrypt

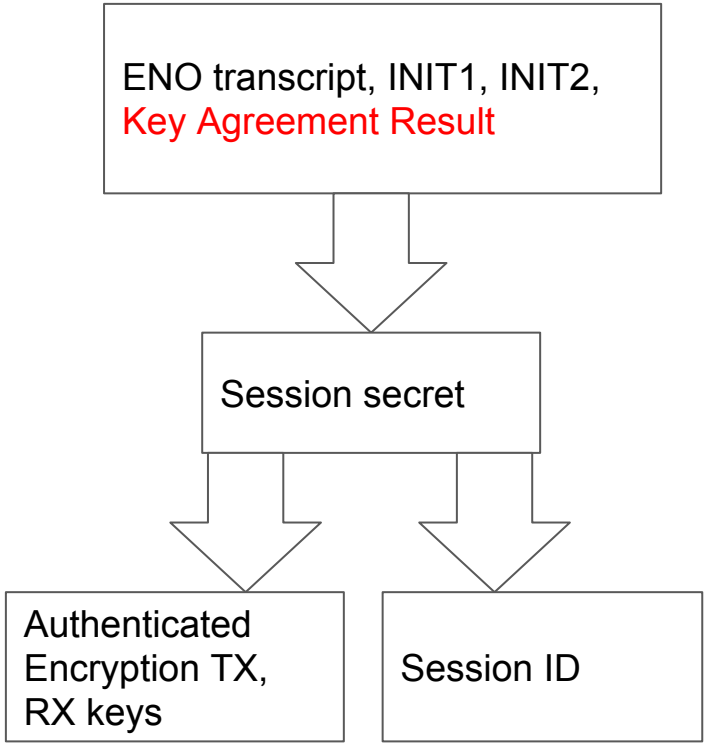
November 18, 2016

Andrea Bittau, Dan Boneh, Daniel Giffin, Mike Hamburg, Mark Handley, David Mazières, Quinn Slack, and Eric Smith

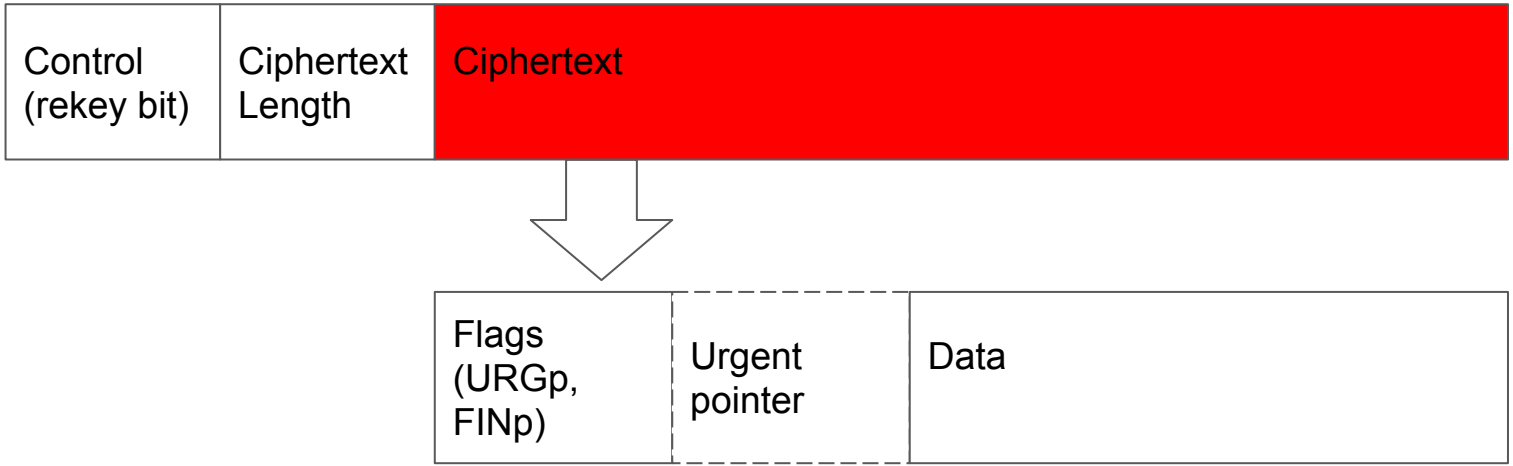
Review: tcpcrypt 4-way handshake



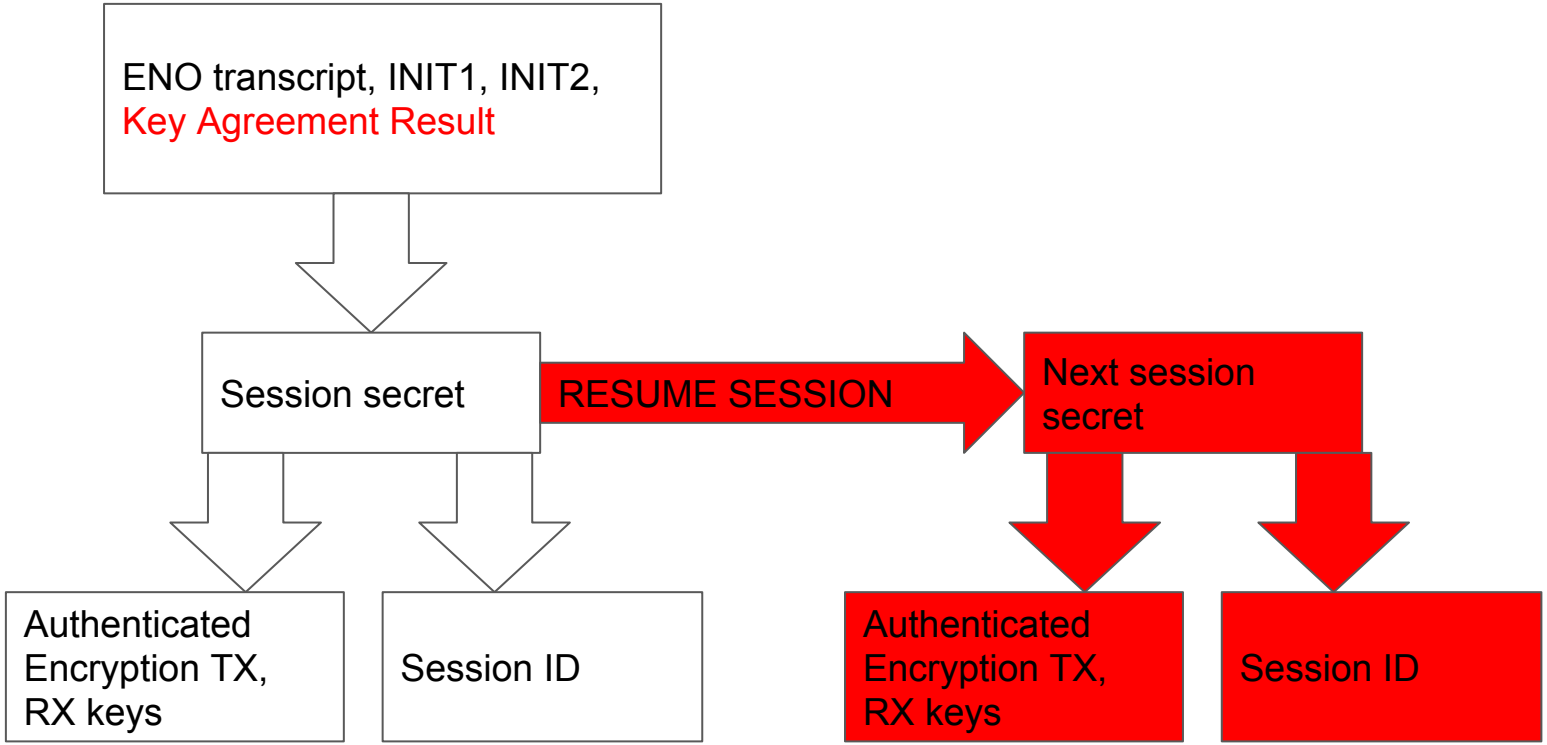
Review: key scheduling



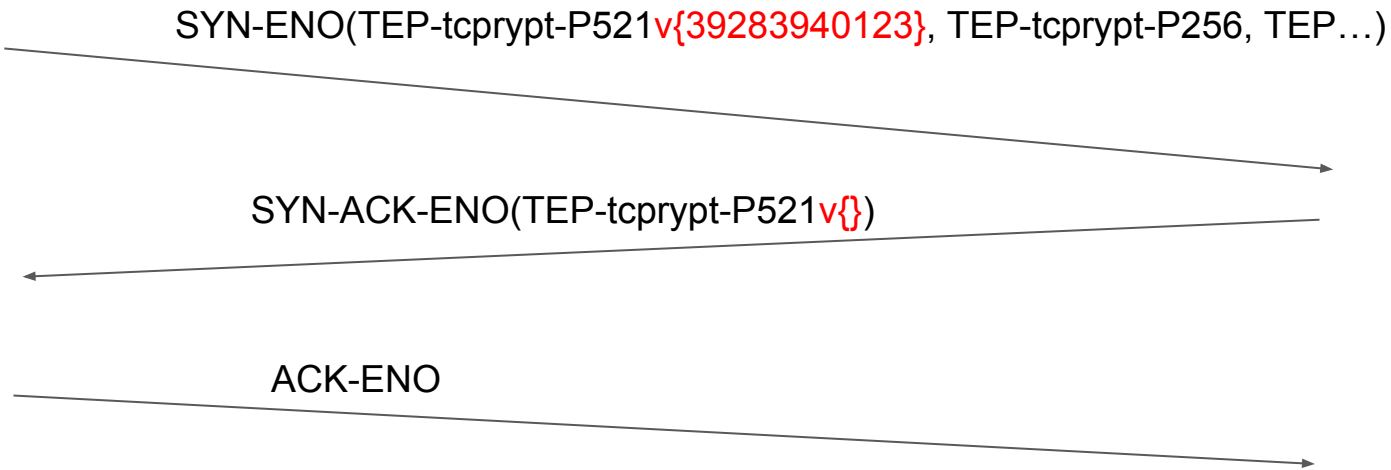
Review: payload authenticated encryption



Review: key scheduling - session resumption



Review: cached session 3-way handshake



v{...} is ENO's variable length suboption, used by tcpcrypt to indicate session resumption

New: cleaned up session caching.

- Signalling resumption for TEP X also implies willingness to start fresh negotiation with TEP X.
- Forbid signalling multiple session resumptions for the same TEP.
- IETF96 - Use TEP-id with some metadata (e.g., the Session ID) to signal session resumption instead of having a generic “session resume” TEP.
  - Better interplay with APIs. E.g., TCP_ENO_NEGSPEC returns the public key algorithm originally used to establish the connection. Previously, a generic “session resumed” algorithm would be returned.
  - Allows to implicitly signal the willingness to start fresh negotiation with the given TEP. Saves bytes in SYN.

New: other changes

- tcpcrypt does not specify how to use data in SYNs. Implementations must not send data in SYNs. (ENO, and tcpcrypt, are incompatible with TFO.)
- Moved APIs to the separate API document.

What’s next?

- Draft - is it complete?
- Implementation - need a kernel one.
- Seeking for independent implementations.

http://tcpcrypt.org