tcpcrypt

July 19, 2016

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

Seems like we’re getting close…

Draft changes

- Use TCP experimental EXID (2 extra bytes)
    - Session resumption on OS X uses all 40 bytes of option space. Makes dedicated option important.
- Session resumption signaled by using original cipher spec and setting the “v” bit instead of a generic “resume” cipher spec.
- Separated the “how” and “why” in draft.
- Many other nits. Thanks Jana, Kyle, David & everyone.

Implementation status

- Effort shift: no longer chasing draft changes but instead making the implementation production quality.

- Compatible with new versions of OpenSSL’s libcrypto.

- (Need to) fix Session ID leaks, and more generally, get/setsockopt authentication.

- Kernel implementation would avoid many of these problems.

- Many thanks to Daniel Gillmor for continued work on Debian packaging, bug hunting and useful suggestions.

Recent discussions

- Does ignoring unauthenticated FIN/URG require special language about updating RFC793?
- Encrypt frame lengths?
- Should tcpcrypt have its own API document?
- Post RFC: Interactions with other protocols (e.g., TFO).

What’s next for tcpcrypt?

- Last call for draft changes? (Are we “done”?)
- Kernel implementation.
- Harden and polish user-space implementation.