Review: tcpcrypt 4-way handshake

SYN-ENO(TEP-tcprypt-P521, TEP-tcprypt-P256, TEP…)

SYN-ACK-ENO(Passive role bit, TEP-tcprypt-P256)

ACK-ENO

INIT1: [AES128, AES256], Nonce, Pub Key

ACK

INIT2: AES256, Nonce, Pub Key
Review: key scheduling

ENO transcript, INIT1, INIT2, Key Agreement Result

Session secret

Authenticated Encryption TX, RX keys
Session ID
Review: payload authenticated encryption

<table>
<thead>
<tr>
<th>Control (rekey bit)</th>
<th>Ciphertext Length</th>
<th>Ciphertext</th>
</tr>
</thead>
</table>

Flags (URGp, FINp) | Urgent pointer | Data |

Diagram:
- Control (rekey bit)
- Ciphertext Length
- Ciphertext
- Flags (URGp, FINp)
- Urgent pointer
- Data
Review: key scheduling - session resumption

ENO transcript, INIT1, INIT2, Key Agreement Result

Session secret

RESUME SESSION

Authenticated Encryption TX, RX keys
Session ID

Next session secret
Authenticated Encryption TX, RX keys
Session ID
Review: cached session 3-way handshake

SYN-ENO(TEP-tcprypt-P521v{39283940123}, TEP-tcprypt-P256, TEP…)

SYN-ACK-ENO(TEP-tcprypt-P521v{})

ACK-ENO

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