Opportunistic TCP-AO with TLS

Maxime Piraux, Olivier Bonaventure, Thomas Wirtgen

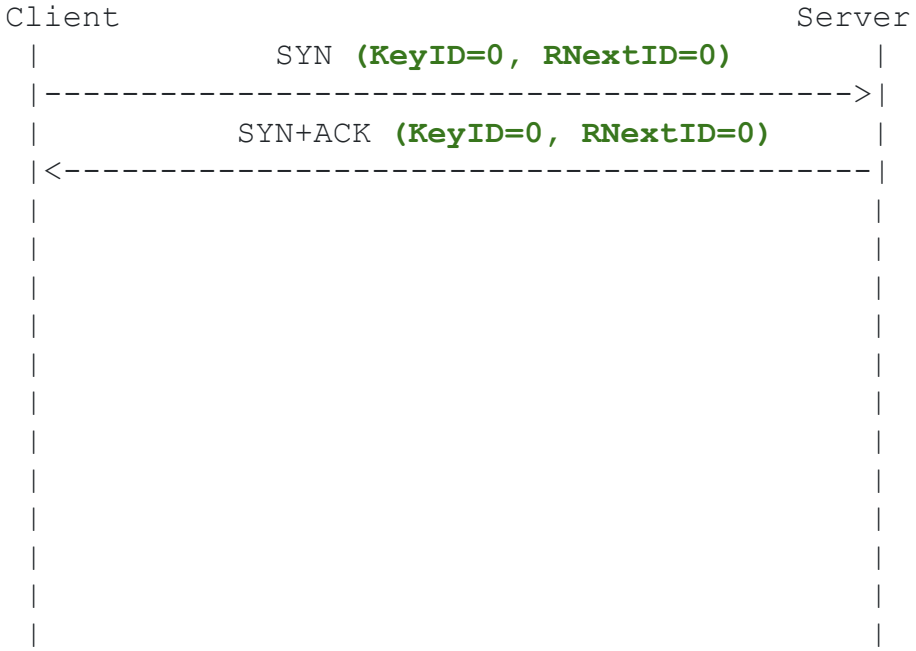
IETF 118 Prague, TCPM wg

Context

- TCP-AO [RFC5925] provides integrity protection and authenticity to TCP packets.
- Cryptographic keys (MKTs) are set up out of band.
- When a TLS session is established over a TCP connection, there is an opportunity to derive secure TCP-AO keys from the TLS handshake.
- The draft proposes a way to achieve it.

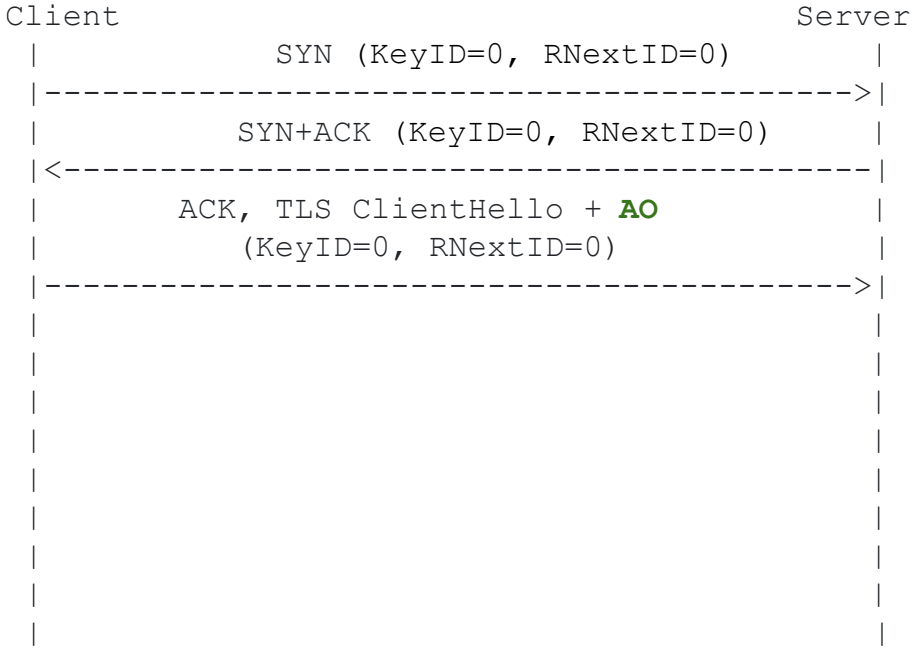
Example of use

- The TCP connection is started with **a default MKT** specified in the I-D.



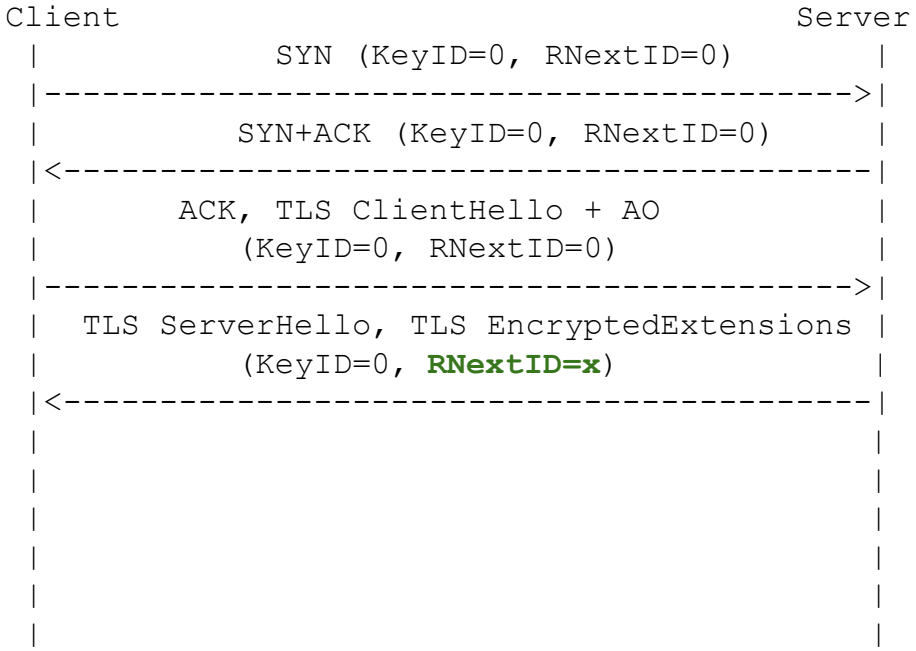
Example of use

- The TCP connection is started with a default MKT specified in the I-D.
- The client includes the **AO** TLS extension to negotiate the authentication algorithm and KDF.



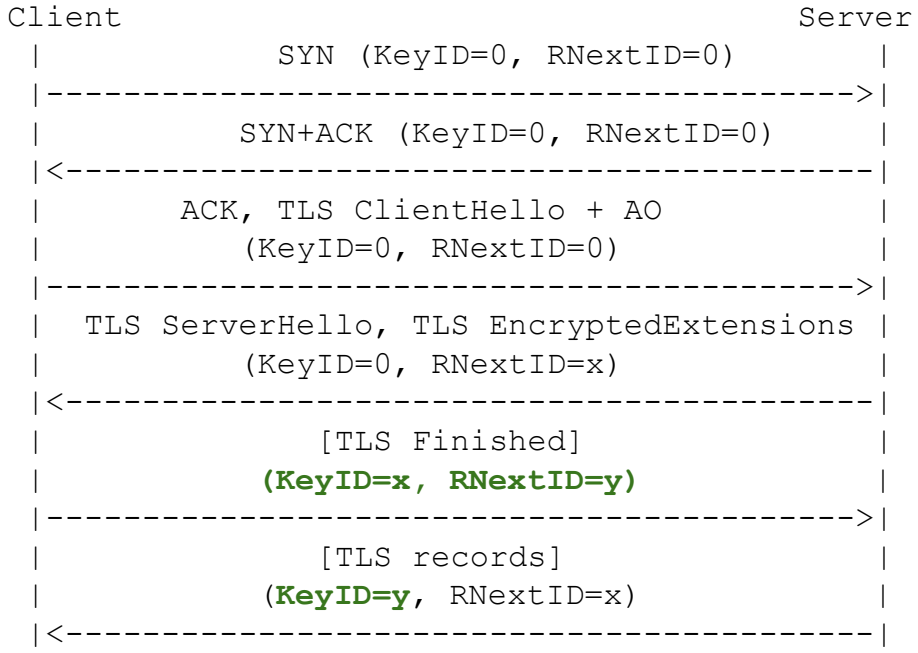
Example of use

- The TCP connection is started with a default MKT specified in the I-D.
- The client includes the AO TLS extension to negotiate the authentication algorithm and KDF.
- The server **prepares the MKT** for subsequent client packets.



Example of use

- The TCP connection is started with a default MKT specified in the I-D.
- The client includes the AO TLS extension to negotiate the authentication algorithm and KDF.
- The server prepares the MKT for subsequent client packets.
- The client can **protect** its packets and **verify** server packets.



Use-cases

- BGP sessions was one original use-case of TCP-AO [RFC5925]
  - BGP can benefit form this opportunistic mode as well, see draft-wirtgen-bgp-tls.
- Any long-lived TCP connections using TLS can benefit from this mode
  - HTTPS
  - DoT

Future document updates

- Discuss interactions with other TCP extensions:
  - TCP Fast Open
- Discuss interactions with other TLS mechanisms:
  - 0-RTT and pre-shared keys
- Define a way to renew the MKT on long-lived connections.