TCP Use TLS Option

Eric Rescorla

ekr@rtfm.com

Background: TLS over TCP

- TLS over TCP is ubiquitous
  - Probably the most deployed Internet security protocol
  - Widely implemented
  - Heavily analyzed and reasonably well understood
- Hard to coordinate
  - Servers which are expecting application data choke on TLS `ClientHello`

Some Existing Coordination techniques

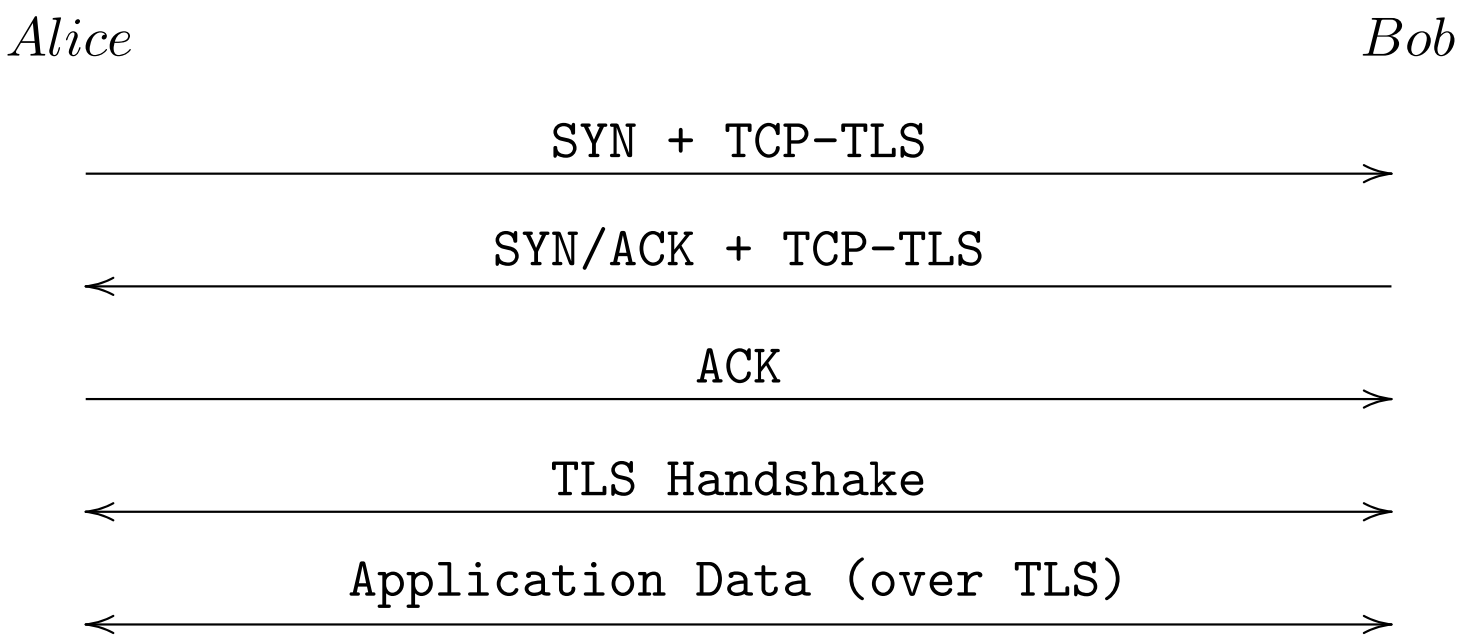
- External signal to the client (e.g., `https:`)
- Separate ports
- Manual config
- DNS signaling
- Extend the application layer protocol (`STARTTLS`)

- None of these lend themselves to opportunistic deployment

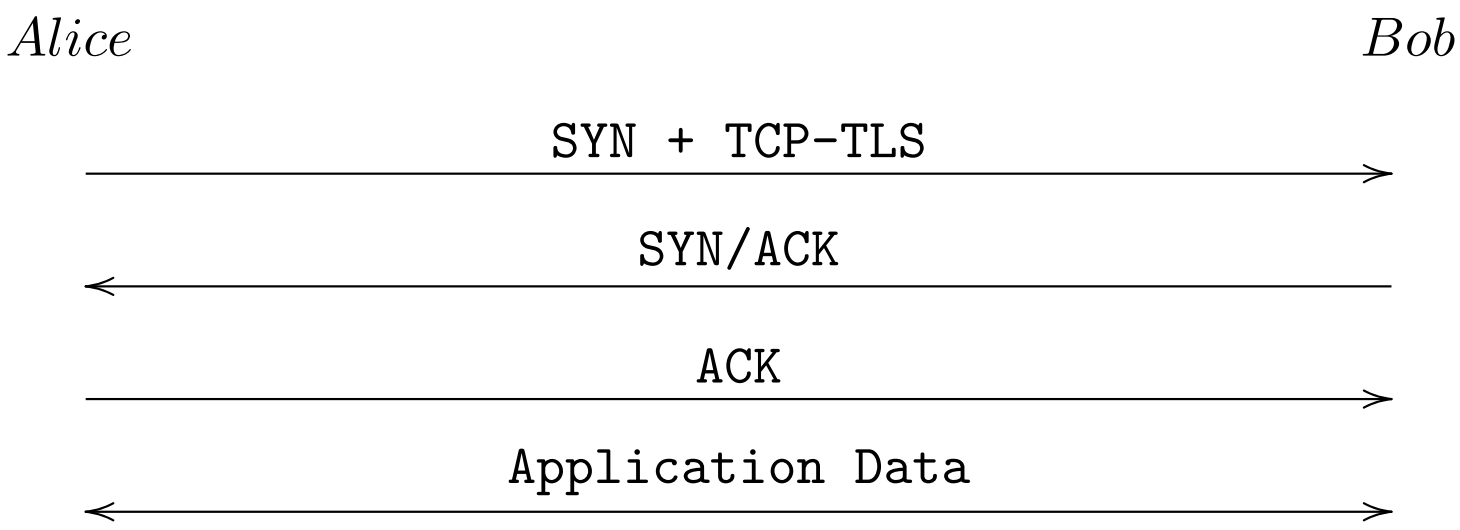
Problem Statement

- Add the minimum necessary machinery to TCP to let it opportunistically negotiate TLS when both sides want to.

TLS TCP Option



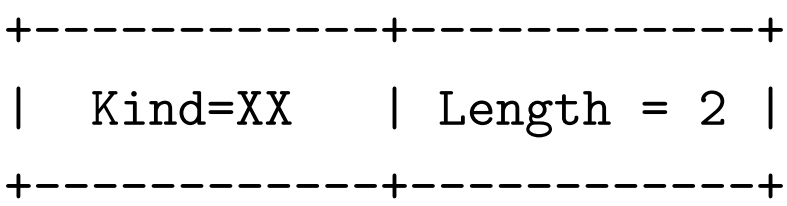
Bob doesn't support TLS



What do we need to signal?

- That I want to do TLS
  - Signaled by option present
- TLS roles (client vs. server)
  - Obvious for non simultaneous open case
  - Do we need to do simultaneous open?
- Thanks to Michael Scharf for help here

Minimal Option (client/server)



- Note: this is not what is in the draft

What about DoS?

- TLS provides security for the content
  - But not for the headers
  - This leaves a DoS vector (e.g., RST injection) against TCP connections
- Not clear how important this is
  - Primary issue here is pervasive monitoring
  - But might be nice to solve
- RST is still a difficult problem

Strawman Proposal

- Use TCP-AO
  - Use TLS Exporter [RFC5705] to make TCP-AO key
- Issue: what about packets from before the TLS handshake
  - Touch argues that a connection can't start AO mid-way through
  - Potential Solution: dummy non-matching MKT (Section 7.3 says these can be ignored)

Comparison to Integrated Designs (e.g. tcpcrypt)

- Advantages
  - Easy to specify and implement
  - Leverage the work that has alredy gone into TLS
  - Looks like existing TLS over TCP on the wire
- Disadvantages
  - Imports TLS history; may want to profile
  - Less optimized, especially when you want to do anti-DoS
  - TLS records can span segment boundaries
    * Easy to manage with attention to MTU

Questions?

Handling Simultaneous open

- Use a random tiebreaker value in option
  - This takes up SYN space so should require application layer setting
  - Can't use sequence number because gateways may resequence
  - Is 32-bits enough
- Edge case?
  - There are probably other options here