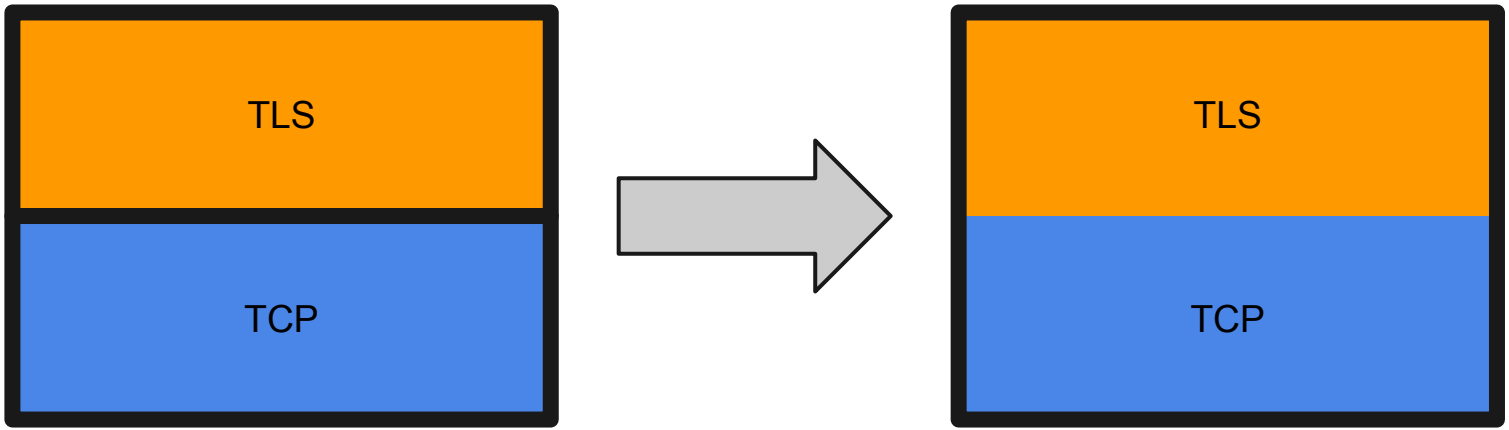
Securing TCP

Opportunistically

Neat layering is for chumps

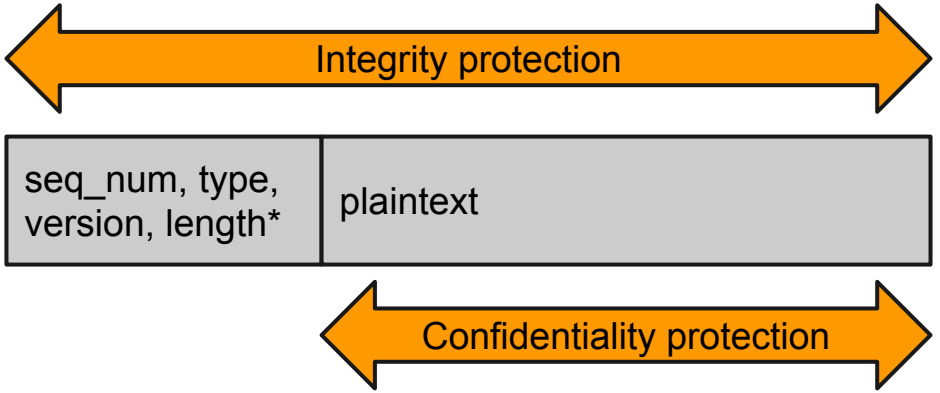


Innovation

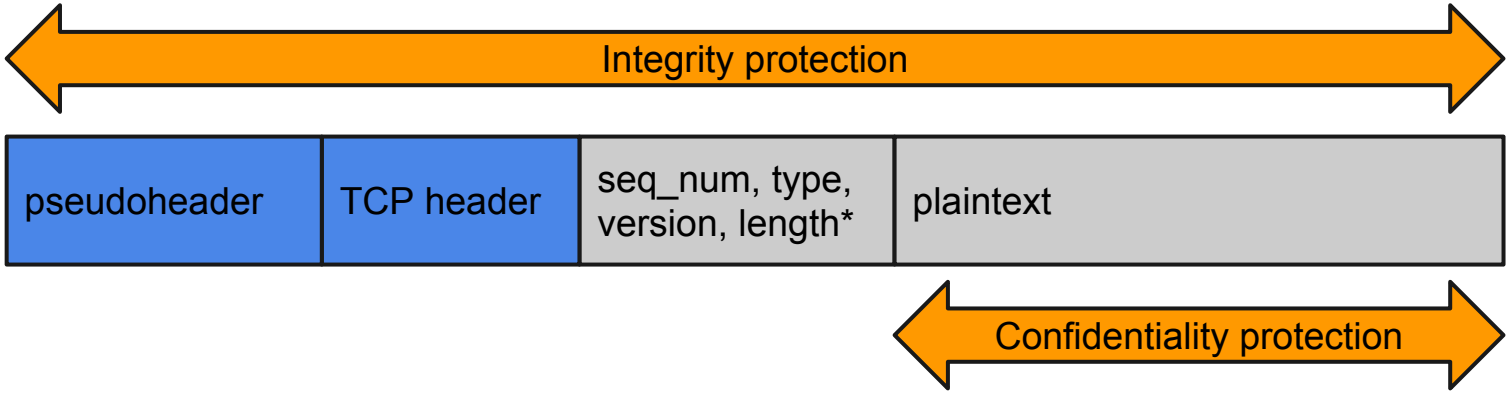
Innovation in security protocols is hard

Don’t do that

AEAD in TLS


Integrity protection
seq_num, type,
version, length*
plaintext
Confidentiality protection

AEAD in TCP


Integrity protection
pseudoheader
TCP header
seq_num, type, version, length*
plaintext
Confidentiality protection

What about the ‘D’?

The draft uses DTLS

That is largely unnecessary

Something like Minion’s COBS would be needed to make this a meaningful choice

What to protect

This matters a lot

I’ve chosen to avoid protection of ACK

Addressing is optionally protected

All options are optionally protected

Profiling TLS

Not doing this would be nuts

You don’t want TLS baggage

I didn’t do this

Good argument-fodder

...go

draft-thomson-tcpinc-dtls-00