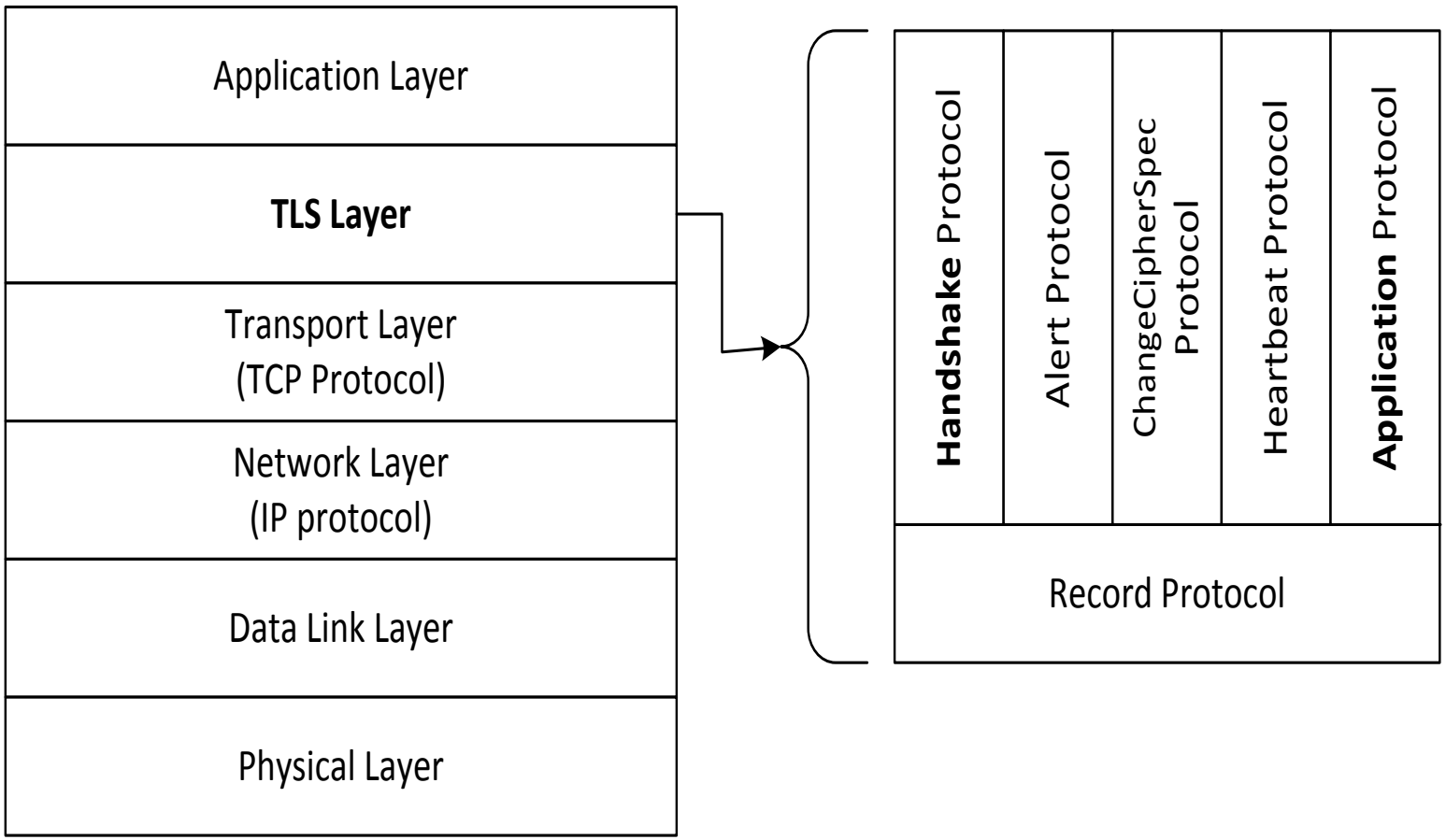
Agenda

- Transport Layer Security (TLS)

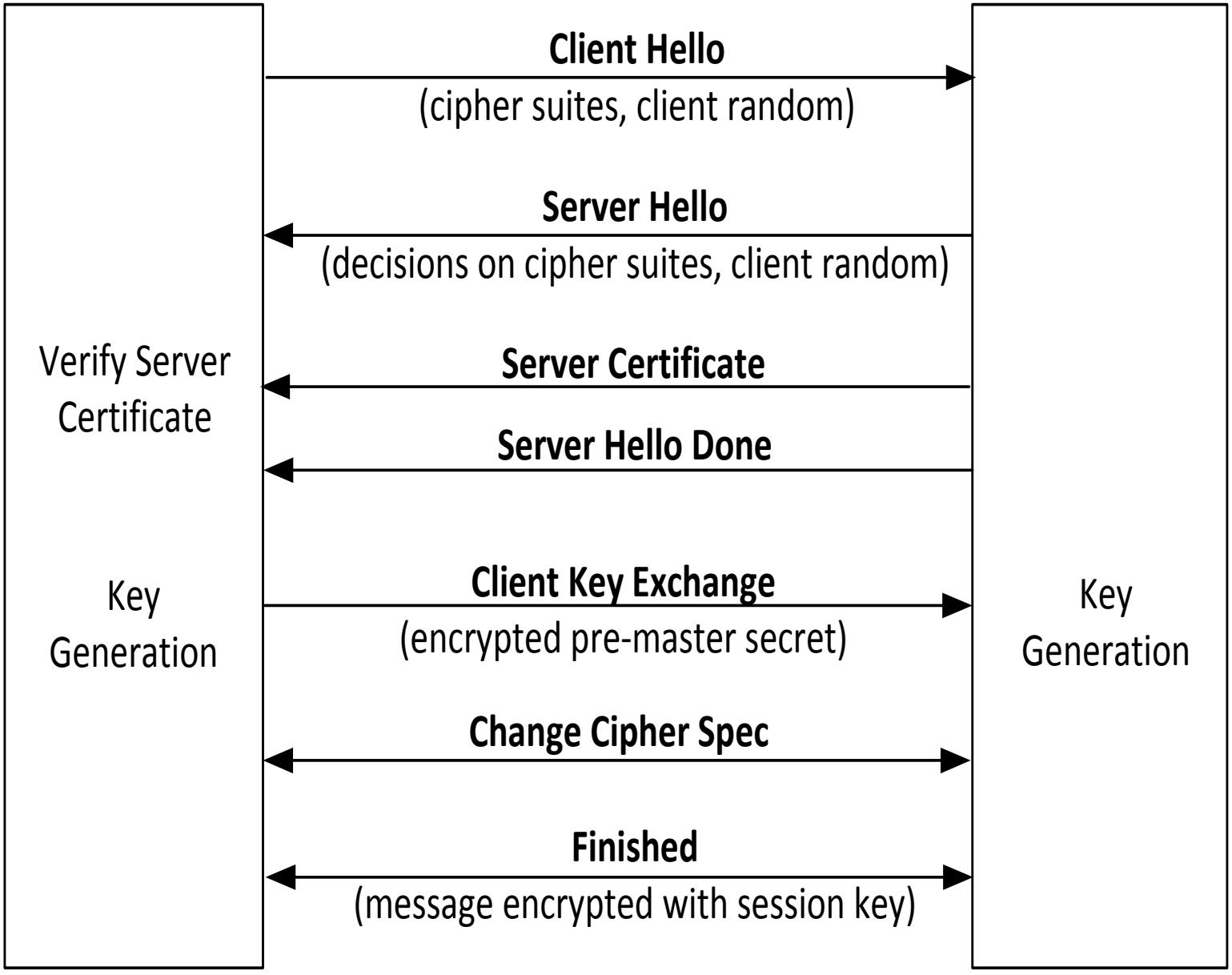
Transport Layer Security

- formerly known as Secure Socket Layer (SSL), later renamed to TLS; SSL, TLS, SSL/TLS are used interchangeably.
- sits between the Application Layer and the Transport Layer.
- Application layer passes unprotected data to TLS, TLS do encryption; After encryption, protected data will be given to the Transport Layer for transmission.

TCP/IP network stack with the TLS layer



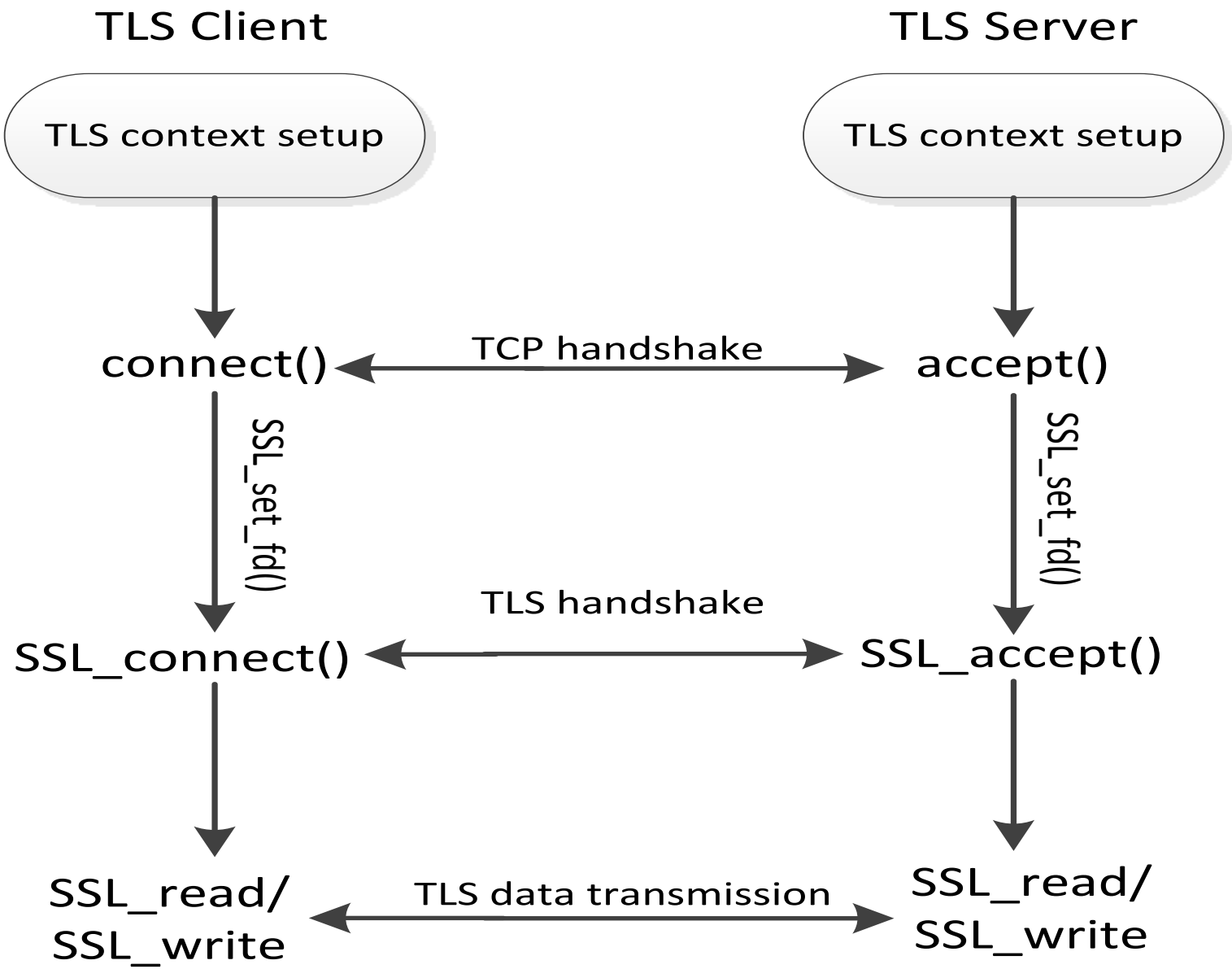
TLS Handshake Protocol



TLS Programming - Four major steps

- Initialization (allocate and initialize data structures, setup the location of trusted CA certificates)
- TCP handshake (TLS is built on top of TCP, so the client and server need to establish a TCP connection first)
- TLS handshake (Establish TLS session)
- Data transmission

TLS Programming Overview



References

A large portion of the material is adapted from:

- Computer Security - A Hands-on Approach by Wenliang Du