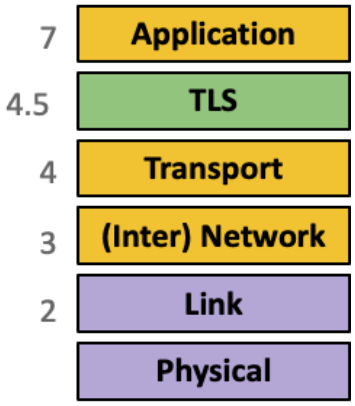
Week 11: Transport Layer and Network Layer Security

Transport Layer Security: TLS



- TLS is a protocol for creating a secure communication channel over the Internet.
- It is built on top of TCP and **relies** on TCP's byte-stream abstraction.

Goals of TLS:

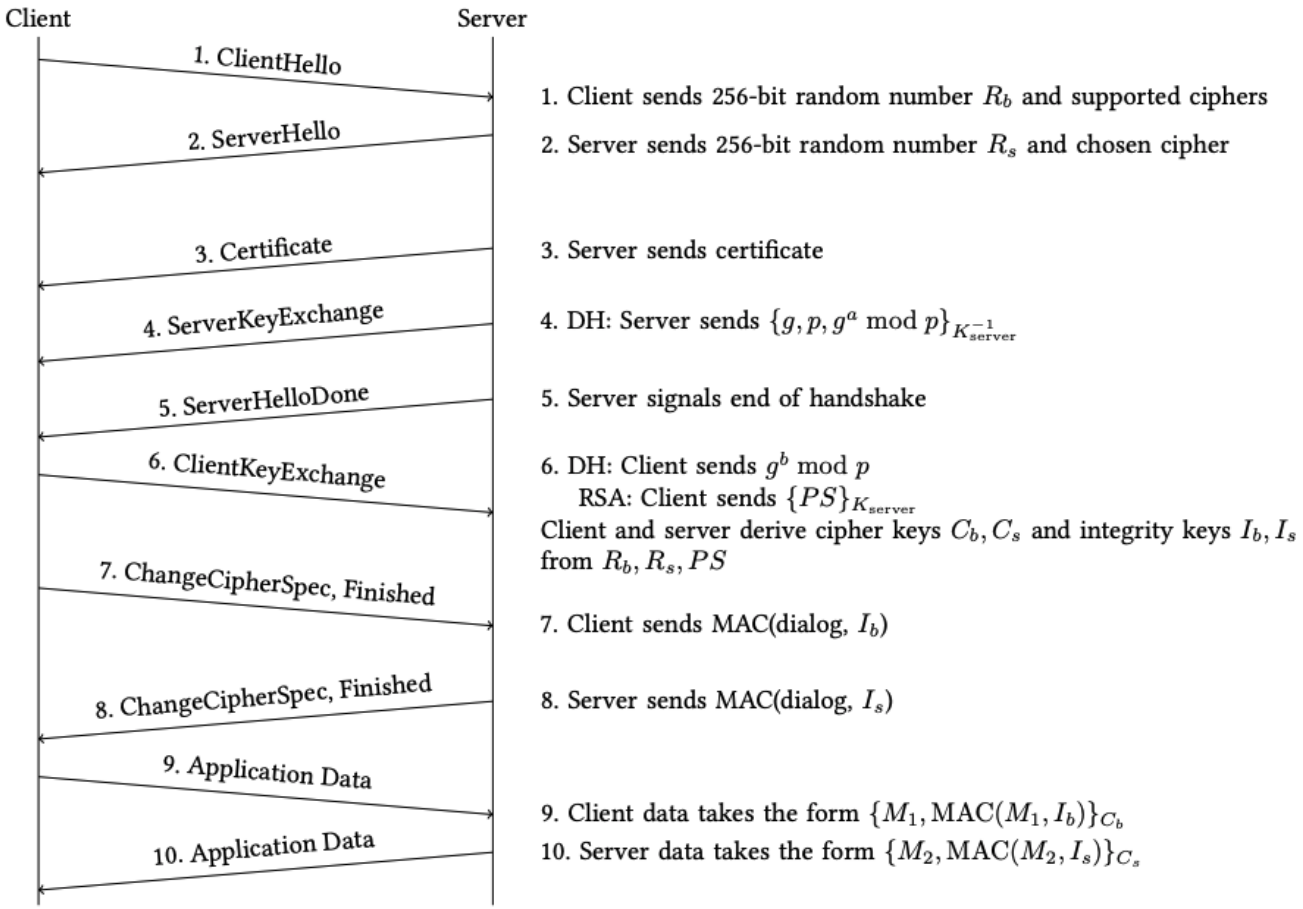
A. **Confidentiality**: Ensure that attackers cannot read your traffic
B. **Integrity**: Ensure that attackers cannot tamper with your traffic
    a. Prevent **replay attacks**
C. **Authenticity**: Make sure you're talking to the legitimate server
    a. Defend against an attacker impersonating the server

Q1. How can we be sure we are talking to the legitimate server? (select all that apply)

A. Server sent their Diffie-Helman Exchange
B. Server sent its public key
C. Server proved that it owns the private key

Q2. What is the purpose of the client random and server random fields?

A. No purpose
B. They act as nonces to prevent replay attacks
C. They ensure validation of the two endpoints.



Q3. ClientHello and ServerHello are not encrypted or authenticated. Explain why a man-in-the-middle cannot exploit this. (Consider both the Diffie-Hellman and RSA case.)

Q3 Part B. Assume that the PRNG generating the Client and Server Hello is compromised. I.e., the internal state of the PRNG is known, and the attacker can predict the next PRN generated. Can a MiTM attack succeed?

A. Yes
B. No

Q4. Does TLS provide anonymity? Anonymity is hiding the client and server's identities from an attacker.

A. Yes
B. No

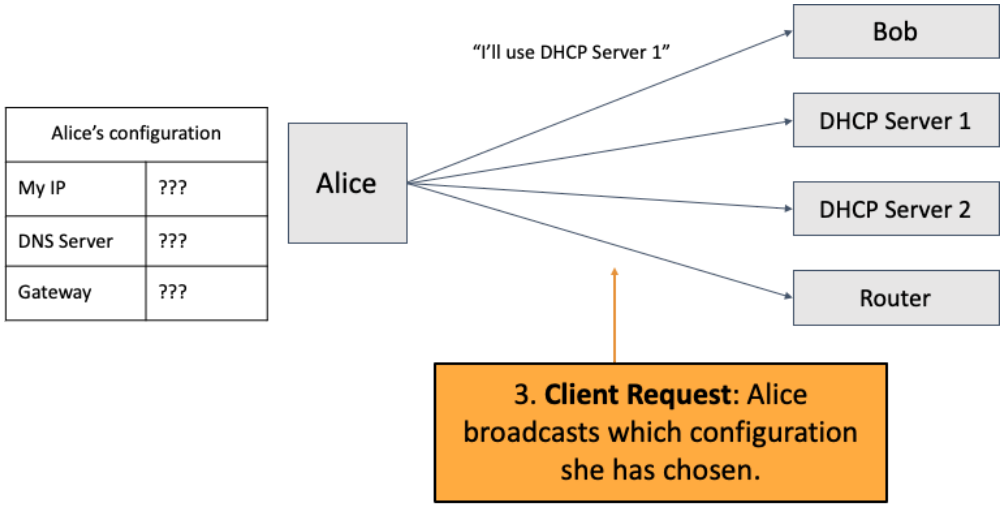
Q5. Does TLS guarantee our three security goals: Confidentiality, Integrity and Availability?

A. Yes
B. No

Q6. Does TLS defend against the following? (Choose yes/no for each)

A. SQL Injection
B. XSS, CSRF
C. Buffer Overflows
D. Does TLS prevent

DHCP



Q1. Alice usually expects only one DHCP server to respond, so she will accept the first response. What does the attacker need to do to trick Alice into using their server?

A. Race with a DHCP response from their server + on-path attacker
B. Race with a DHCP response from their server + off-path attacker (different subnet)
C. Provide a DHCP response, does not have to race the correct server

Q2. What damage can the attacker above do?

A. Become a MiTM (modify, corrupt packet contents)
B. Claim to have a legitimate DNS local resolver
C. Masquerade as Bob (the person Alice is communicating with).

Q3. What are possible defenses to DHCP?

A. Use cryptography in some manner
B. There are no defenses at this layer
C. Use other protocols at the network layer (like ICMP, routing protocols)