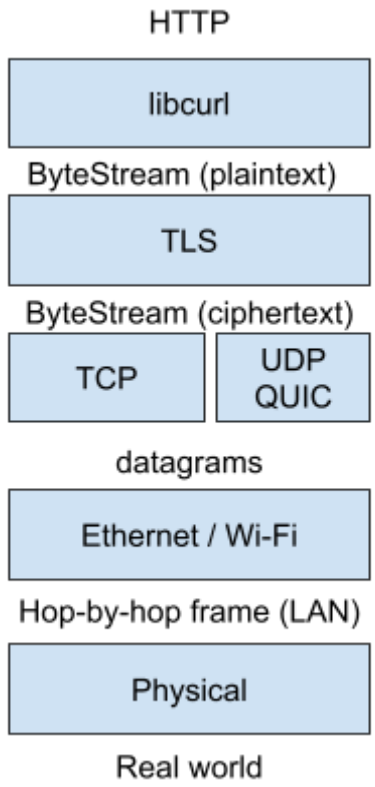
Last Time:

- Security Properties: Integrity, Confidentiality, Authenticity
    - ,and authenticity is necessary for confidentiality
- Certificate provides authenticity
    - (Opportunistic encryption: even if you are not sure who you are talking to, still do encryption. This kind of confidentiality makes it harder for third parties (e.g. governments) to learn the content of the traffic, though it does not require authenticity.)



- Does this layer of TLS solve everything?
- **Issue 1:** Certificate authorities may be corrupted / intentionally issued not correct certificates. The transparency log helps to mitigate this, but it is not a 100% solution.
    - Big companies would monitor the transparency log
    - Browsers may require the certificate to also contain a proof that the certificate is from the transparency log
- **Issue 2:** Even if the payload of Internet datagrams is encrypted, you could still tell who is talking with who by the src/dst in the IP header. **“Metadata privacy”**.
    - VPN or through one relay server: governments can’t tell who is talking with whom, but they can still get the info by threatening the relay server
    - How about more than one relay server? Essentially, any single relay server cannot see the full picture of the connection.
        - Onion routing: layers of encryption and each relay server can only take out one layer of the encryption. **The Onion Router (TOR).**
        - Each relay server only knows the hop before itself and the hop after itself
    - But: the timing still reveals something

- **Threats:** eavesdropper timing attack correlation
    - Something is being sent from TOR to Netflix at 1:33 a.m.
    - And if there is a short list of people that were using TOR at that time
    - It may not be that difficult to tell who is actually sending to Netflix
    - Q: How do third parties (say governments) tell people that are using TOR?
      A: TOR relay servers are public and TOR traffic may look different. Governments could figure out TOR relay servers IP addresses and block them. (To fight against this, TOR relay servers IP addresses are released slowly, and they are trying to make TOR traffic look as innocent as normal traffic).
- **Threats**: Sybil attack
    - TOR works only if the relay servers are not colluding. If a certain entity has a huge number of TOR relay servers, then there is a high probability that a whole sequence of relay servers belong to this entity, then the entity can learn about the connection.
- TOR hidden service
    - Allow publishers and users of services to hide their identity.
    - Normally contains 6 hops of relay, 3 picked by the publisher, 3 picked by the client.
    - By exploiting security holes, governments can still reveal who was visiting/posting on TOR web servers. (Put the security hole exploit on the web servers of these hidden services, then whoever downloads the content would also download the security hole exploit).