Communication Networks – HW5

Oz Cabiri & Guy Harem

Question 1 – HTTP:

a) d
   i) Persistent Connection: Instead of opening and closing a TCP connection to the server for each image, we can utilize a single TCP connection that stays open. This eliminates the need of additional handshakes, reducing the number of RTT necessary.
   ii) Pipelining: Instead of sending a request for an image and waiting for a response to send the next request, we can send all request sequentially, without waiting for a response. The server will then answer with our requests in order. This saves the RTT while waiting for a response.
   iii) Multiplexing: Pipelines can cause application-level HOL blocking in case of a delayed response. With multiplexing we can open several streams on the same TCP connection which will take turns in utilizing it, preventing application-level HOL blocking, which of course reduces the time needed to load the full page.

b) CDN and/or local caching. While it will **not reduce the number of RTT** needed to load the page it will **reduce the waiting time** by reducing the RTT itself.

Question 2 – HTTP Versions:

a) Multiplexing, header compression, server push.
b) UDP based, independent streams, integrated security in a single handshake, no transport-layer HOL blocking.

Question 3 – DNS:

a) `www.TauNetworksCourse.com: type **CNAME (CN)**, class IN, CompNets.ABB.com`
   `CompNets.ABB.com: type **A**, class IN, 150.37.1.122`

   CN – Canonical Name: This means that the requested name was an alias, and the host needs to ask for the IP of it's matched value instead. (www is a nickname)

   A – Address: The actual IPv4 address needed to connect to the requested destination.

b) `www.TauNetworksCourse.com: type **CN/NS**, class IN, CompNets.ABB.com`
   `CompNets.ABB.com: type **A**, class IN, 150.37.1.122`

   In the case `www.TauNetworksCourse.com` is a host name – CN + A: same as before.

   In the case it's a delegated sub-zone – NS + A:
   NS – Name Server: the DNS doesn't know where `www.TauNetworksCourse.com` is, so it references the resolver to the appropriate name server `CompNets.ABB.com`, which is the authoritative for that zone, where it can find an answer.

   A – Address: a glue record. the address of the name server specified in the previous record to which `www.TauNetworksCourse.com` is delegated, so the resolver can request the information from there.

Question 4 – DNS Cache Poisoning:

a) An attacker can get the RR to resolve a name they'd like to take over. Then they can flood spoofed responses with R, R+1, R+2,…, in order to "intercept" a future request, just as was shown in class.

b)

i) Randomize the source port and require it to be returned in the response.

ii) Use DNS-0x20. Since
DNS labels are case insensitive, randomize letter capitalization in the request and require the same capitalization to be returned in the response.