Jakub Szpunar
CS4480
HA 2

P7) The time to get the IP address from DNS is(assuming n > k): $D_1k + D_2(n-k)$

The time to get each object involves first connecting to the server, then requesting the object.

The time to get the objects is: $2mRTT_0$

The total time is $D_1k + D_2(n-k) + 2mRTT_0$

P8) Time to get the IP: $2D_1 + D_2$

a) Time to get the objects: $10RTT_0$
   Total time: $2D_1 + D_2 + 10RTT_0$
b) Time to get the objects: $2RTT_0$
   Total time: $2D_1 + D_2 + 2RTT_0$
c) Time to get the objects: $RTT_0 + 5RTT_0$ (Here only one TCP connection needs to be made.)
   Total time: $2D_1 + D_2 + 6RTT_0$

P15) MTA stands for "Mail Transfer Agents."

The malicious host that generated the spam email looks to be 58.88.21.177. The headers are set in reverse chronological order. The IP address given is of the oldest host. The IP address the email originated from is also the IP address of this host. Perhaps the host is simply churning out emails?

P18)

a) A whois database allows everyone to see the information of the person who registered a domain name.
b) Doing a whois on google-public-dns-a.google.com has the IP of 8.8.8.8
   OpenDNS has a DNS server at 208.67.222.222
c) Looking up www.utah.edu. My ISP local server shows the address to be 155.97.137.55 for type A. The type ns shows the server to be ns.utah.edu. The type mx shows mail servers of smtp.cc.utah.edu and ipo.cc.utah.edu. The Google free DNS server returns the same answers. Using OpenDNS, the type A and MX results are the same. However OpenDNS says "No name server (NS) records available for www.utah.edu). All of the DNS servers say that they are not authoritative.
d) Cnn.com has four addresses. 157.168.255.X where X=19,25,26,18 www.utah.edu has only a single IP address.
e) The U has an IP address range of 155.97.0.0 to 155.97.255.255
f) An attacker now has all the possible IP addresses of computers belonging to an organization. He/she can now focus attacks on these. Additionally, an attacker now knows exactly what computer provides what tasks. A DNS attack, or a DoS attack on a webserver/mailserver/etc now has a target.

g) By being publicly available, a person can see who a domain/IP address/site belongs to. They can help judge if a location on the internet is safe or malicious by looking at this information.

P19)

a) Starts at d.root-servers.net, next to a.edu-servers.net, next to ns.utah.edu. ns.utah.edu returns the type A record of 155.98.64.249/.250 for cs.utah.edu

b) Looking up anandtech.com. Starts at a.root-servers.net, next is a.gtld-servers.net, next is ns67.worldnic.com which returns the type A record of 199.19.80.10
Looking up google.com. Starts with a.root-servers.net, next is a.gtld-servers.net, next is ns1.google.com which returns ip addresses 74.125.255.168 and more.

P24)

a) Here we assume the server upload speed is <= average upload speed of all peers. If the server sends chunks of the file round robin style between the peers, the file will be out there in F/u_s time. Because the average upload speed of all peers is >= the server upload speed, these chunks will propagate between peers at least as quickly as the server sends out chunks.

b) Since the server's upload speed is >= average upload speed. The server can send out chunks to the first clients. Next, these clients propagate the chunks through peers. Because the server is faster than the average peer, the server will have sent out at least a full copy of the file before all of the peers can get the file themselves. It is bound by $NF/(U_s + u_1 + \dots u_n)$.

c) The minimal distribution time must account for both the time it takes the server to send out a full file, and the time it takes for that file to propagate through the peers. Whichever takes longer will be the minimal distribution time.

P28) Peer 6 will ask peer 15 for its successor, and then it will continue asking until it reaches the point where it passes from a peer with an index less than it, to a peer with an index more than it. In this case, it stops on peer 8. It sets peer 8 as its successor, then asks peer 8 for its successor and sets this as its second successor. It remembers that before peer 8, it spoke to peer 5. It asks peer 5 to update it to be peer 5s successor, and peer 8 to be peer 5s second successor. It also tells peer 4 that it is now its second successor.