

CS138 Homework Assignment 2

Spring 2009

1. 24.248.56.68 is an IP address.

a. What DNS name has this as at least one of its associated addresses? (Hint: use the `nslookup` command on Linux — do a “`man nslookup`” to discover how to use it. In particular, you’ll want to run it interactively and use the “`set query=ptr`” command to look for `ptr` records.)

wsip-24-248-56-68.ri.ri.cox.net

b. To determine the answer to part a, you used `nslookup`. What name servers were contacted to do this lookup? Assume the query was iterative (and thus starts at the root). (Hint, consider the “`set query=ns`” command.)

Among the possible name servers that might have been used are:

A.ROOT-SERVERS.NET. (root nameserver)

chia.arin.net (nameserver for 24.in-addr.arpa)

ns.west.cox.net (nameserver for 248.24.in-addr.arpa)

ns1.coxmail.com (nameserver for 56.248.24.in-addr.arpa)

2. In class we wondered how reverse lookups are done when one is in one part of the world, looking up an IP address in another.

a. 203.125.49.10 is an IP address in Singapore. What outfit appears to have assigned the address? (Hint: after using `nslookup`, use google.)

Asia Pacific Network Information Centre.

b. Note that there is no reverse lookup available for this address, perhaps because its owners don’t want you to know what it is (it’s actually `extdns.dns3.gov.sg`: for really minimal extra credit, how did I figure this out?). 137.132.21.117 is another IP address in Singapore. What DNS name has this as at least one of its associated addresses?

(I started with `extdns.dns3.gov.sg`, then obtained its IP address.)

`www.nus.edu.sg`.

c. What name servers were contacted to give you the answer to the previous question?

`x.arin.net`.

`ns1.nus.edu.sg`.

`id4.nus.edu.sg`.

`www.nus.edu.sg`.

d. How do you reconcile the answer to part a with those of b and c?

Asia Pacific Network Information Centre was not involved in b and c, instead, ARIN was, despite the fact that it’s nominally in charge of just North America and the Caribbean. Apparently its servers backup (or at least cache) the database maintained by APNIC.

3. *The Needham-Schroeder protocol is discussed in lecture 7. In slide VII-10 we mention that the third message could be replayed by Mallory so as to make Bob think he's talking to Alice, when it's really Mallory. Show how this can be done and explain why the version of the protocol given in slide VII-11 prevents it from happening.*

If Mallory has somehow learned K_{AB} , and has "sniffed" the message $K_{AB}(R_{A2})$, $K_{B,KDC}(A,K_{AB})$ sent by Alice to Bob earlier, she can replay this message to Bob. Bob would then respond $K_{AB}(R_{A2},R_B)$ as he did previously. With her knowledge of K_{AB} , Mallory would be able to decrypt Bob's response and then send $K_{AB}(R_B)$ to Bob, as required by the protocol. Thus Bob would now believe that he is communicating with Alice.

In the version of the protocol given in slide VII-11, Bob passes $K_{B,KDC}(R_{B1})$ to Alice. She then sends $R_{A1}, A, B, K_{B,KDC}(R_{B1})$ to the KDC, and gets back $K_{A,KDC}(R_{A1},B,K_{AB}, K_{B,KDC}(A,K_{AB},R_{B1}))$, which can be decrypted only by Alice (and not by Mallory). Alice then sends $K_{AB}(R_{A2})$, $K_{B,KDC}(A,K_{AB},R_{B1})$ to Bob.

Suppose now that Mallory has sniffed this last message, and that she later learns K_{AB} . She can't simply replay the message, because it's the second message that Bob receives in the protocol, not the first. So she would have to run the protocol from the beginning and send the required first message to Bob, to which Bob would respond with $K_{B,KDC}(R_{B1})$. But this value of R_{B1} would be different from the one in the message she sniffed, and Bob could determine that the replayed message is not correct.

4. *The concept of hierarchical trust is discussed in slide VII-24. Assuming each realm has its own privilege server (consisting of a Kerberos KDC and additional functionality), explain how a client at `/.../acme.com/east_coast` would obtain a ticket that authenticates it at `/.../college.edu/CS`. Be sure to indicate where the restrictions imposed by hierarchical trust (as opposed to transitive trust) are enforced.*

The client obtains from its local KDC a ticket for the KDC at `/.../college.edu`. This takes advantage of the cross-hierarchy link between the two KDCs. The client would then, using this ticket, contact the KDC at `/.../college.edu` and obtain a ticket for `/.../college.edu/CS`. The KDC at `/.../college.edu` would allow this since the request is for a ticket to a KDC lower in the hierarchy.

5. *We discussed the concepts of strict consistency, sequential consistency, and entry consistency in lecture 9.*

- a. *Which form of consistency do clients of GFS see? Explain.*

Strict consistency. Clients aren't notified that writes complete until the data is safely replicated on all participating chunk servers, and all chunk servers store data in the same order.

- b. *NFS's file protocol is weakly consistent. If all its clients use its lock protocol, do they then see entry consistency? Explain. (Hint: be careful.)*

No. The problem is that the lock protocol is independent of the file protocol. Thus one might lock a file, modify it, then unlock it, but there's no guarantee that the modified data has been sent to the server. To ensure entry consistency, one must explicitly flush the file's data after locking a file and before unlocking it.