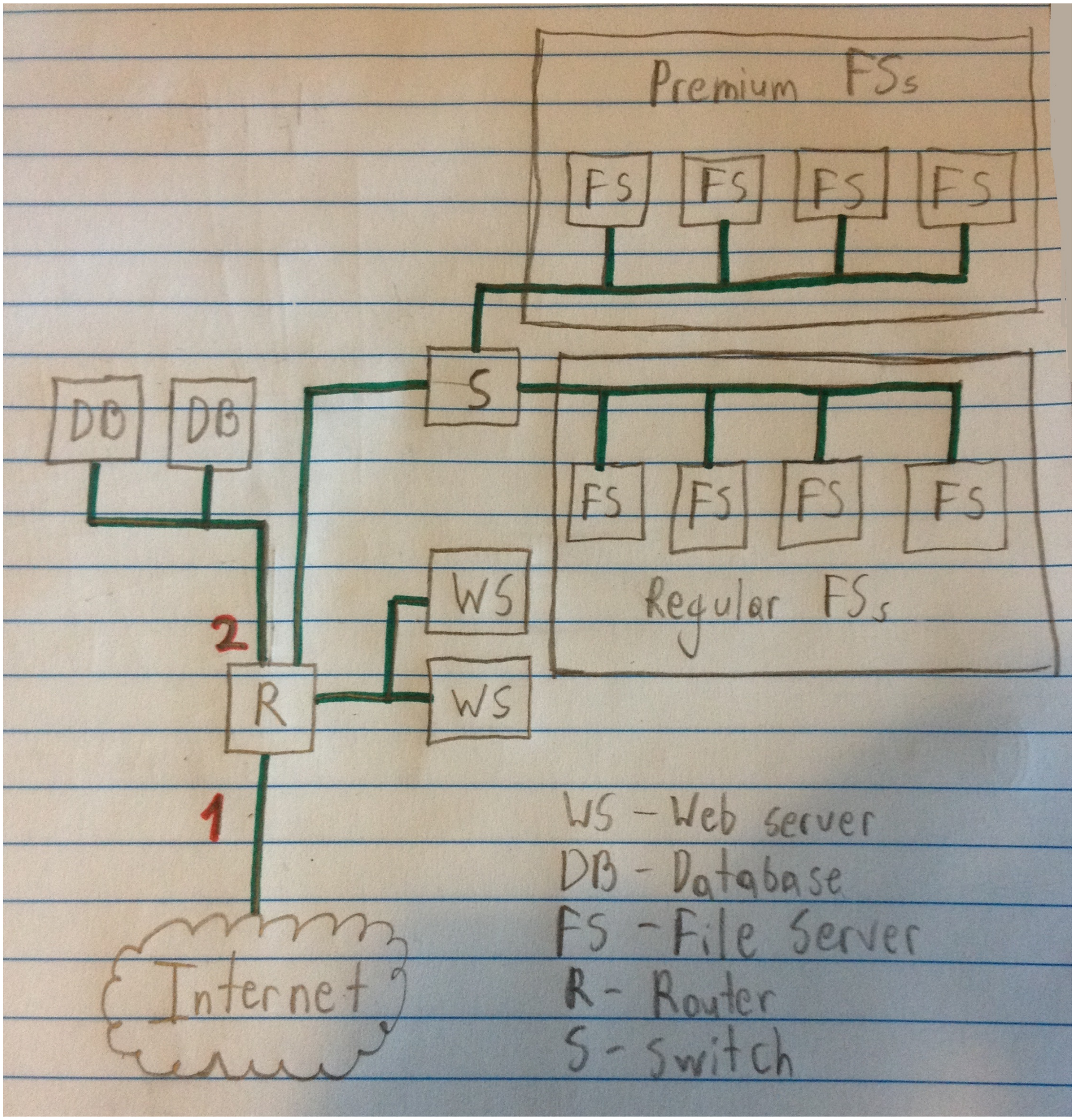
Michael Prelich
mprelich
20424478

Written Response Questions

1) a)



The router decides where to route each packet. The client will talk to the web server when browsing the site to login, chose a movie, etc. There are two web servers to deal with times of increased traffic. The web server sends requests to the database for logging in users and getting their information such as if they have a premium or regular account. There is a backup database which contains the same information, should the first database go offline. When the user selects a movie, the web server sends a request to file servers. The file servers are split into 2 zones, regular file servers and premium file servers. The regular file servers contain all of the regular movies, while the premium file servers contain the premium movies. Only premium customers can send requests to the premium file servers. The premium file servers each contain the same movies as each other, as do the regular file servers. Their only differences are their geographic locations. Once a movie is chosen, it is streamed and directed to the proper user via the router.

1) b)
If we could only use one firewall, it would be placed just before the router at the red 1. It would be an application proxy. With an application proxy, the user would first have to talk to the proxy, and the proxy would talk to the servers. This proxy could make sure that only certain database queries are made, so that users could not modify their own, or other users', entries. It could also perform strong user authentication. Though this application proxy may have high overhead, it comes with the added security we desire.

1) c)
If we could place more than one firewall, they would be placed on either side of the router, at red 1 and 2. This would turn the web server zone into a demilitarized zone (DMZ). We could use stateful inspection firewalls to lower the overhead of the firewalls compared to the application proxy method. The internal firewall acts between each geographic location of the file servers. The firewalls could also remember which packets are going where, speeding up the streaming process while still keeping the security we need.

2) a)
We see that each of our queries must return between N/4 and 3N/4 records.
I am assuming that in the database, around half (or 0.4N to be more specific) of the players will be in PvP servers. This assumption is based on the World of Warcraft server statistics retrieved from: https://realmpop.com/us.html. Our tracker will then be T = (Server = PvP). Our three queries will be:

A) SELECT SUM(GOLD) FROM PLAYERS WHERE (NAME="XdarksephirothX" OR SERVER="PvP")
B) SELECT SUM(GOLD) FROM PLAYERS WHERE (NAME="XdarksephirothX" OR NOT(SERVER="PvP"))
C) SELECT SUM(GOLD) FROM PLAYERS

Then XdarksephirothX's gold = A + B – C

2) b)
We would first need to use count queries to identify an additional attribute about doomlaser that returns an appropriate amount of records. We will once again use the server attribute and assumption from part a. We first use the following queries:

A) SELECT COUNT(*) FROM PLAYERS WHERE SERVER="PvP"
B) SELECT COUNT(*) FROM PLAYERS WHERE (SERVER="PvP" AND NOT(NAME="doomlaser"))

We then do A - B. If this returns 1 then we know that doomlaser is in a PvP server. If it return 0, then they are in a PvE server. From the example database provided in the assignment: A – B = 5 – 4 – 1, so doomlaser is in a PvP server. Using this information, we construct the following queries:

```
C)  SELECT COUNT(*) FROM PLAYERS
     WHERE (SERVER=”PvP” AND NOT(NAME=”doomlaser”))
                 OR (SERVER=”PvP” AND NOT(GOLD>X))
D)  SELECT COUNT(*) FROM PLAYERS WHERE SERVER=”PvP”
```

We then take C – D. If this equals 1, we know that doomlaser has more than X gold. If it equals 0, then he has less than or equal to X gold. We know that gold is bound between 0 and 20 billion, so we start at X = 10 billion, and continually query C – D, while changing X, to narrow in on doomlaser’s gold.

3) a)
The issues intended to be solved include having to go to the judge whose district is involved in the crime being investigated, as well as having to obtain multiple warrants to search multiple devices. With Rule 41, investigators can go to any judge to obtain the warrant they need, and they will only need to obtain one warrant in order to search multiple computers.

3) b)
Peter Carr is likely talking about TOR networks, used to conceal the IP address of the person committing the questionable activity. Without knowing the IP address, it is very difficult to pinpoint where the crime was being committed from. Under existing law, a warrant can only be issued for the district that the judge is in charge of. Without the IP address of the criminal, it is difficult to say which district that could be, and which judge needs to be involved.

3) c)
Smartphone users will be affected, as investigators could not only search an unnumbered amount of computers, but phones as well. Users who use social media could have their personal information compromised, if their devices are searched because of a warrant. Finally, anyone using email on their device could have their personal information compromised as well, as investigators would be able to search through these emails for suspicions content.

3) d)
Negative consequences involved with passing the proposed changes to Rule 41 include wrongfully accessing computers in mass searches, like those in identifying botnets, as well as accessing computers abroad, not in the jurisdiction of the judge issuing the warrant. Both of these consequences could affect Canadians, as the idea of jurisdiction is completely erased, and investigators are free to search any amount of computers in any part of the world.

3) e)
Judge shopping is the act of filing numerous lawsuits asserting the same claim, hoping that eventually a favorable judge is assigned the case and is more likely to gran the warrant without fully understanding the power that warrant possesses. Another example of judge shopping occurred in 2015 in the Freddie Gray case were prosecutors were accused of judge shopping to obtain a warrant to search the defendants phone.

https://ballotpedia.org/Judge_shopping

Programming Questions

1)
We have to make at least one call to the oracle, up to 256 calls (max), for every byte in a block in order to find valid padding. On average, we will have to make 256 / 2 = 128 calls per byte.
N = number of blocks
b = block length in bytes
W = number of possible words (256 [0 up to 0xFF])

Worst case = N x b x W = N x 16 x 256 = 4096N
Average case = N x b x W / 2 = N x 16 x 256 / 2 = 2048N

2)
We could use a MAC to help fix this vulnerability. It provides integrity, we know if the message has been modified, and authenticity, we know if the message is coming from who we expect. We must make sure that we encrypt, then MAC, otherwise the message needs to be decrypted before the MAC can be checked which negates its purpose. The MAC makes sure we only read messages that have been authenticated. If an attacker tries to change the message, the MAC will be altered and we will know the message has been forged. The server will still return different responses for valid and invalid padding, however it will also return a negative response for a wrong MAC, but the attacker will have no way of knowing if the response they got was for an incorrect padding, or an incorrect MAC.

3)
In 3.1 we would change line 5. In part b, we would instead of XORing with n, have to XOR with our padding scheme. In this case, the last byte would be XORed with whatever iteration we are on (the number of bytes of padding). We would then iterate backwards over the bytes, XORing them with whatever iteration we are on (byte 15 XORed with 1, byte 14 XORed with 2, byte 13 XORed with 3, etc.)

In 3.2 we would have to change line 1, and 5, once again to fit our padding scheme. Instead of XORing with (b-j+2) we would as above, have to iterate backwards over the bytes and XOR with the correct value, as in the correction above.