Matt Forbes

Assignment 6

March 11, 2011

6.2

All peers might act like both the server and the client at the same time. After obtaining some list of seeders, a client might try and make connections with all/some of those addresses. When a connection is established, the client could request different parts of the file it needs to download. While all of this is happening, the client will also be acting like a server by listening for connections. This time, other peers connect to it and request parts of the file, and are uploaded when found.

6.19

Assuming the book means the process ID given to an program by the OS, that would be a pretty bad way of identifying services. It would completely defeat the purpose of "well-known" ports as process IDs not only differ from host to host, but also change when a program is restarted. To get around this, all connections would need to first be filtered through some auxilary service like inetd that can forward a request along to the correct service.

7.3

DNS servers map domain and subdomain names to actual IP addresses. Losing that ability would cripple the net for most individuals, seeing as not many people know the exact IP address for any of the web sites or email addresses they use. It would render most of the world internet-less until the DNS servers were put back online (assuming their data is all backed up and locked away).

7.6

If a DNS server in charge of returning the IP address for such a machine, it may be updating dynamically based on server load. Another way this could be achieved is if multiple IPs point to a machine but the domain name is just associated with one of them.

7.11

Every 24 bits are split in to four groups of 6 bits. Each individual group is then encoded in to an ASCII character. 4 ASCII characters is 32 bits, so we gain 8 bits for every 24. 4560 bytes is 36480 bits, or 1520 24-bit groups. Each 24-bit group is transformed in to a 32-bit group and thus the file size grows to 48640 bits, or 6080 bytes. Adding a CR+LF (2 bytes) after 110 consecutive bytes means an extra 110 bytes for a grand total of 6190 bytes.

7.13

The MP3 file being sent could be split in to four pieces of 1MB each (the limit his friend's ISP set). He could then send each of these four parts in order, using the content-id of the email header to specify the order. Once his friend has recieved the four parts, he could rig them back together and have his file.

7.15

White space generally means the "space" character, but whether that's just one or multiple isn't necessarily defined. The space character isn't the only thing that statisfies "blank space." In html the string *nbsp*; is rendered as white space. New line's are rendered as space. Sometimes non-printables can be rendered as spaces.

7.18

Of course not. The IMAP interface must be the same across all implementations so that a single client can make the same request to any and recieve the same response. An actual implementation should be free to design the actual mailbox structure however they want, granted they know how to respond to client IMAP requests.

7.23

With just the information given in the question, I don't really know why a domain name shouldn't end with a digit. Any browser or program that uses URLs should be able to determine whether or not it's working with an IP or a DNS name. Subdomains can end in digits, I'm not sure if the question is asking specifically about the last character of the TLD or something else.

7.44

Assuming equal distribution across the month, one tenth of their customers will watch a movie at some time on any given day (3 movies per 30 days, $\frac{3}{30} = \frac{1}{10}$). One tenth of their customers is 5,000, and two thirds of those will be watched at 9pm. Rounding up, that's

556 movies each requiring 6Mbps for a total of 3333Mbps served. OC-12 lines have up to 622Mbps capability. The video server will need is 5-6 such connections.

7.47

I don't want to look up 25 random websites that are most likely all domain-squatting spam. My estimate is that at least 80% of the sites I might type in from those categories would be a spam page.

8.1

WILL YOU WALK A LITTLE FASTER SAID A WHITING TO A SNAIL THERES A PORPOISE CLOSE BEHIND US AND HES TREADING ON MY TAIL SEE HOW EAGERLY THE LOBSTERS AND THE TURTLES ALL ADVANCE THEY ARE WAITING ON THE SHINGLE WILL YOU COME AND JOIN THE DANCE WILL YOU WONT YOU WILL YOU WONT YOU ILL YOU JOIN THE DANCE WILL YOU WONT YOU WILL YOU WONT YOU WONT YOU JOIN THE DANCE

8.3

a digital computer is a machine that can solve problems for people by carrying out instructions given to it x

8.30

If Jim and Mary are on the same VPN, they should be able to send direct email to each other without having to encrypt it. This is because the email message will never leave the internal network. On the other hand, if they use some external service to communicate like Skype, they might be accessing a server out on the net. This connection would not be secure.

8.41

Based on the way PGP was described here, a PGP-encrypted message is designed for only one recipient to be able to open it. Building such a message requires the recipients public key, and most be known ahead of time. So no, only one person could read the message, sending it to an arbitrary IP address wouldn't work at all.

Private Key Crypto Systems

A private key system uses symmetric-key algorithms. This just means that the encryption method and decryption method use the same key. Both the sender and receiver should both know this secret key and use it for securing/sending data. The problem with using a symmetric-key algorithm is that if an intruder is able to steal the key, the system is completely shot.

Public Key Crypto Systems

As discussed above, securing a private key is huge deal and kind of a deal-breaker when it comes to security. All persons needing to encrypt or decrypt messages need access to this key, so it gets harder and harder to keep it hidden. A public key system bypasses this by using two separate keys, one for encrypting and one for decrypting. A "public key" can be given out freely, and the "private key" is kept safe and given to no one. For this idea to work, a few requirements need to be met: It should be completely infeasible to produce the private key given any message and public key, and the encryption method needs to be too strong to be broken by a plaintext attack. It really boils down to a private key being intractable to solve in any way given the public key.