INST 346 Final Exam Solutions
Spring 2018

1. This question called for the use of Wireshark.
   a) If you provide a relative sequence number, the sequence number for the SYN packet would be 0. If you provide an absolute sequence number, the sequence number for the SYN packet would be randomly chosen (and shown by Wireshark in hexadecimal).
   b) Regardless of whether you provide a relative or an absolute sequence number, the sequence number of the HTTP request would be 1 more than the sequence number you provided in answer to (a)
   c) 3,525 bytes
   d) The Web page was sent using http, not https, and thus was not encrypted. Note that (c) could not have been answered if the HTTP message was encrypted.
   e) This number needs to be well over one hundred because (even if you provide a relative sequence number) it is acknowledging at least the first packet of the Web page, which will contain hundreds of bytes.

2. The client python program:

```
from socket import *
serverName = 'localhost'
serverPort = 8150
clientSocket = socket(AF_INET, SOCK_DGRAM)
message = input('Input a string to reverse:')
clientSocket.sendto(message.encode(),(serverName, serverPort))
modifiedMessage, serverAddress = clientSocket.recvfrom(2048)
print (modifiedMessage.decode())
clientSocket.close()
```

   The server python program:

```
from socket import *
serverPort = 8150
serverSocket = socket(AF_INET, SOCK_DGRAM)
serverSocket.bind(('', serverPort))
print ("The server is ready")
print ("Enter a string to reverse")
while 1:
  list = []
  message, clientAddress = serverSocket.recvfrom(2048)
  modifiedMessage = message.decode()
  modifiedMessage = modifiedMessage[::-1]
  serverSocket.sendto(modifiedMessage.encode(), clientAddress)
```

3. The types of costs include at least (type / annual cost / change direction for cloud / reason) [the numbers here are my personal estimates; yours may differ]:
   a) Computer / $1,000 / lower / virtualization and availability contracts
   b) Software / $500 / same / licensed
   c) Network / $50 / lower / economies of scale
   d) Facility / $50 / lower / economies of scale

e) Energy (power & cooling) / $200 / lower / purpose-built cooling design
f) Staff / $60,000 / lower / amortized over more computers
g) Backups / $200 / same / media costs
h) Insurance / $100 / higher / business risk

4. This question is about ransomware
   a) One type of attack would be spear phishing to gain credentials that could then be used to compromise access control. Once logged in, the ransomware could then be installed. Many other approaches are also possible.
   b) A network intrusion detection system could detect many types of attacks. It might detect the specific attack described above in (a) based on a combination of the attacker's (unfamiliar) IP address, and known payloads of the ransomware during the file transfer. A host-based intrusion detection system might detect the action of the ransomware (e.g., encrypting the file system).
   c) Symmetric key encryption is much faster than public key encryption.

5. This question asks about wearable devices.
   a) Video will take up the most disk space. The answer to (b) makes that clear.
   b) 1 year =31,540,000 seconds (this averages between 365 and 366 day yaars; you could have used either). For video, we'll multiply 1920x1080 (the number of pixels per frame for some reasonable resolution; you might have selected lower resolution) by 3 (for RGB color), by 30 (assuming 30 frames per second) = 186624000 bits per second of video. This number * the 31,540,000 seconds in a year gives us a total of 5.886121 times 10 to the 15^{th} power bits, or nearly 736 Terabytes of video before compression. We'll assume 100:1 compression for video (you might have assumed more or less than that). This leaves us with a 7.36 TB video file at the end of a year. High quality audio is recorded as a wav file at 320 kilobits/s 320 * 31,540,000 = 10092800000 kilobits, which is about 1.26 Terabytes worth of audio. Heart rate is simply a numeric value, which HW1 said we can imagine would be stored in four bytes (although you could store typical heart rates in a single byte if you wanted to). Let's assume that your heart rate will be added to a log every minute (you might have assumed something more frequent), as it is measured in beats per minute. There are 525,600 minutes in a year, so 525600*4 bytes gives us 2102400 bytes, or about 2.1 Megabytes.
   c) If we were to add up the sizes of all the stored data for a year, we'd get a little over 8.6 Terabytes. This number divided by the number of seconds in a year is 300kB/s, or 2.4 Mbits/s, so that's the minimum transmission rate needed to send your data to the cloud in real time.

6. This question is about IPv6
   a) The principal concern was that IPv4 was running out of addresses, but new devices were still being connected to the Internet. A larger address space was therefore needed.
   b) IPv6 packets can be sent through IPv4 networks using tunneling. This is done by encapsulating the IPv6 packet inside an IPv4 packet, and sending that through IPv4 to a router that can extract the IPv6 packet and forward it on an IPv6 network.
   c) Among the factors affecting adoption of innovation, relative advantage best explains the very slow adoption of IPv6. IPv6 simply does not have a

sufficiently large relative advantage over IPv4 to adequately incentivize adoption of IPv6.

7. This question is about WiFi
   a) One difference between a MAC address and an IP address is that the MAC address is assigned to the hardware, and its structure indicates who manufactured that hardware, whereas the IP address is assigned by Internet Service Provider and and its structure indicates where in the network that IP address is located (said another way, IP addresses are “routable”).
   b) If a node has the IP address of another device on the same subnet, it can discover the MAC address of that device by using the Address Resolution Protocol (ARP).
   c) If a packet is lost because two hosts transmit at the same time, the host sending the packet will not receive an acknowledgement. The sending host will then wait a random delay time and retransmit the packet.

8. This question is about jurisdiction.
   a) The Internet Corporation for Assigned Names and Numbers manages DNS.
   b) No, national governments do not have jurisdiction over the domain name system because that system includes servers in many countries, and the country in which the domain name server is located may not be the same as the country in which the server that has a domain name is located. Only ICANN can direct the removal of a domain name.
   c) Yes, national governments can employ or direct the employment of firewalls that filter packets that are sent to or from specific IP addresses.
   d) No, national governments can not prevent packets from traveling between other countries. National governments can prevent packets from being routed through their country, but the Border Gateway Protocol permits packets to be routed around specific Autonomous Systems (AS) and thus makes it possible to avoid sending packets through any specific network.