INST346 Final Exam Spring 2018

You have 120 minutes to complete this exam. Time begins promptly at 1:30 PM and ends promptly at 3:30 PM. You may not read the exam questions before 1:30 PM.

Please record your answers in a Word file, in a text file, or on a piece of paper (which could be this printed exam or any other paper). You can answer some questions one way (e.g., as Word) and others the other way (e.g., by writing on paper). At the top of every piece of paper or every file in which you write an answer, write your name and the date. If you answer any questions using Word or a text file, submit that file on ELMS and also email it to both oard@umd.edu and mwalker1380@gmail.com. If you answer any questions on paper, turn in that paper. Make sure your name is on everything that you turn in! And if you use both paper and a file, make a note on each about what can be found in the other so that we don't miss any of your answers.

You may use any information and software that existed before the start of this exam. This means (among other things) that you may search the Web.

You may NOT communicate with any other person other than the professor or the teaching assistant (Mike) for any purpose during the exam period, either in person or in any other way, and you may not post anything to any location other than ELMS (to submit your exam) for any purpose during the exam period. Note that this means you may not have skype, email or any instant messaging application active on any device that you use during the exam, and that that even if you leave the exam room early you may not talk with anyone about anything, you may not send or receive any email, etc. until the exam period ends at 3:30 PM.

You may not use headphones during this exam except when listening to a class video (if you choose to do so during the exam).

Hand type – no cut and paste – the honor pledge followed by your name as your signature on this exam. (For reference, the honor pledge as stated at http://osc.umd.edu/Uploads/OSC/Honor%20Pledge.pdf, is: "I pledge on my honor that I have not given or received any unauthorized assistance on this exam.")

As strategies for completing the exam, keep the following in mind:

- If you find a question to be ambiguous, you may come to the front of the room to ask about it, but please do so in a way that other students can't hear. If you don't get an answer that resolves your question, then please explain your confusion and any reasonable assumptions that you have made in order to answer the question and include those with your answer so that they can be considered during grading.
- You are more likely to get partial credit for an incorrect answer if you show your work.
- **Be careful not to spend too much time on any one question.** The total available credit on this exam is 25 points. Plan ahead, and don't devote more time to a question than it is worth.

***** WRITE YOUR NAME! *****

Answer **either** question 1 or 2. If you answer both, only question 1 will be graded.

1. [5 points] Use Wireshark to observe the packets that are exchanged between your computer and the Web server that serves the page http://legacydirs.umiacs.umd.edu/~oard/apollo/moontalkers2.txt to you. Based on what you see in Wireshark, answer the following questions:
    a) What sequence number was sent in the HTTP SYN message that set up the TCP connection over which the Web page was sent to you?
    b) What sequence number was sent in the TCP packet that contained the HTTP request message that your Web browser sent to request the Web page?
    c) According to the HTTP response message that actually sent the Web page to you, what is the length of that page (in bytes)?
    d) Was the page encrypted using either SSL or TLS when it was being sent to you? If so, what type of encryption was used?
    e) What acknowledgement number was included in the TCP packet that your client sent to acknowledge receipt of the Web page?

2. [5 points] Create two python programs that both run on your computer (i.e., on localhost), one of which is a UDP server that listens on port 8150 and the other of which is a UDP client. The client should accept a character string input by the user, then send that string to the server using UDP, then receive a different character string back from the server, and then display that received character strong to the user. The server should receive a character string by UDP from the client, then reverse the characters in that sting (e.g., the string "Doug Oard" should become "draO guoD"), and then send the reversed string back to the client. You should test your programs, because to receive full credit it must work correctly. The answer to this question must be submitted online (so that we can run your programs).

Answer **four** of the remaining six questions (i.e., four questions from the six questions numbered 3 through 8). If you answer more than four, only the first four will be graded.

3. [5 points] Describe every type of cost involved in purchasing, managing, operating and maintaining a Web server, and include estimates (expressed as dollars) for the amount that would be spent in a typical year for each type of cost. Then explain how cloud computing using centralized data centers can provide similar service at lower cost. Do this by explaining, for each type of cost you have identified, whether the cost would be lower (per Web server) when using a data center. For those costs that would be lower, explain why they would be lower.

4. [5 points] Answer **all** of the following parts of this question about ransomware attacks:
   a) How can an adversary install ransomware on your computer? A complete answer to this question would be a specific description of a plausible process that an actual adversary could use against your computer with a reasonable chance of success. Simply naming one type of attack would not receive full credit; you will need to explain how the attack actually works.
   b) Explain whether an Intrusion Detection System (IDS) would have been able to detect the attack you have described. If you believe an IDS could detect the attack, your answer should explain how the IDS could do so. If you believe an IDS could not detect the attack, your answer should explain what limitations that apply to all Intrusion Detection Systems would prevent the attack from being detected.
   c) One common form of ransomware encrypts the contents of your hard drive using symmetric key encryption. Explain why symmetric key encryption is a better choice for this task than public key encryption would be.

5. [5 points] Wearable devices can generate very large amounts of information, including (among other things) video of what the wearer sees, audio of what the wearer hears, and biometric data such as heart rate that characterizes the wearer's activity. Answer **all** of the following parts of this question about this information:
   a) Which of the three types of information (video, audio, heart rate) would require the largest amount of disk space if all of that information is stored?
   b) How much disk space would be needed to store one year of those three types of lifelogging data. You can express your answer in bytes, kilobytes, megabytes, gigabytes, or terabytes. For full credit, you must explain how you calculated this number.
   c) What is the minimum transmission rate that would be needed for a network connection that is used by your wearable device to transfer all of your lifelogging data to cloud storage as it is acquired? You can express your answer in bytes per second, kilobytes per second, megabytes per second, gigabytes per second, or terabytes per second. For full credit, you must explain how you calculated this number.

6. [5 points] Answer **all** of the following parts of this question about the Internet Protocol (IP):
   a) Explain why IPv6 was developed. Do this by identifying the needs that IPv4 can not meet and then describing what IPv6 does to meet those needs.
   b) IPv6 devices are able to communicate using IPv4 networks. Explain how that happens.
   c) IPv6 was first proposed 20 years ago, but IPv4 continues to be widely used. Use the framework for adoption of innovation that we discussed in class to explain why. For full credit, you must draw on the adoption of innovation framework to answer this question.

7. [5 points] Answer **all** of the following parts of this question about wireless (WiFi) connections.
   a) What is the difference between a MAC address and an IP address?
   b) If a node on a WiFi network knows the IP address of another node on the same Ethernet subnet, how can it discover the MAC address of that node?
   c) If a packet is lost on a WiFi connection because two hosts transmit at the same time and interfere with each other, what happens?

8. [5 points] The Internet connects people in many different national jurisdictions. For example, a server in Croatia owned by a company in The Netherlands might send a Web page to the Web browser of a user that is located in China. Answer **all** of the following parts of this question:
   a) What organization is responsible for managing the worldwide Domain Name System?
   b) Can national governments delete domain names that are associated with servers located within their borders from the Domain Name System? If so, explain how they would do this
   c) Can national governments prevent computers within their borders from sending or receiving packets to or from specific Internet Protocol (IP) addresses? If so, explain how they would do this.
   d) Can national governments prevent computers outside their borders from sending or receiving packets to or from specific IP addresses that are also located outside their borders? If so, explain how they would do this.

*** WRITE AND SIGN THE HONOR PLEDGE ***