Mid-term Exam for IERG4130 2022 Fall

Instructions:

(1) The exam will start at 9:30am Oct 20, 2022 and end at 11:15am Oct 20, 2022

(2) You need to answer all of the twelve questions, and put all your answers in a separate PDF file

(3) You need to upload your PDF file to blackboard system before or on 11:20am Oct 20, 2022.

(4) All submissions after 11:20 am will be regarded as late submissions, and every 5 minutes of late will lead to a 10% deduction of your mid-term score.

(5) If you have any questions about the questions, you can ask us via the Zoom with Meeting ID: 994 5664 0851, and Passcode: lasr

---

1. When we set up a Web server, normally we will create a dedicated account to run that Web server instead of running it directly under the root/administrator's account. Could you explain why and which security principle has been used here? (5'+5'=10')

2. After Bob had visited a web site called www.sample.com , he found he could not open and view the contents of his documents (like word and PDF files) any more. According to what you have learned in this course, what had happened to his computer? If you were Bob, what could you do to prevent this happening to your computer? (5'+5'=10')

3. In a stream cipher, the random number generator plays an important role in terms of security, and in general we would expect the generated random numbers to be unpredictable as much as possible. So Charlie suggest to use a true random number generator in stream ciphers. Is it a good idea or not? Why? (1'+4'=5')

4. A computer worm is a piece of malicious software that will propagate through networks. Could you name one possible reason (i.e., vulnerability) which could be exploited by worms? Please also explain how it works. (3'+7'=10')

5. Between authentication and authorization, which one do you think should be done first? Why? (2'+3')

6. It is important for a program to validate and/or sanitize inputs from users. What is the difference between input validation and input sanitization? If you are the developer, which one do you think is better? Why? (3'+2'+5'=10')

7. What is the Initial Vector in the CBC mode of AES? What is the common thing between the Initial Vector and the Counter value in the CTR mode? (2'+3'=5')

8. Between CBC mode and OFB mode, which one will you choose for a noisy communication channel? Why? (2'+3')

9. Between OFB and CTR mode, which one will you choose to achieve best performance? Why? (2'+3')

10. What attacking the Vigenere Cipher, what is the purpose to calculate the index of coincidence (IC) and compare it with that value of normal English text? Shall we calculate a single IC out of all cipher text, or shall we divide the cipher text into groups and calculate IC for each group? (5'+5')

11. What is the value of: $\mathbf{3^{1024} \bmod 7}$? Please use what you have learned in this course and give intermediate steps (correct result without intermediate steps will get a zero mark) (10')

12. Why symmetric key encryption algorithms cannot provide the guarantee of non-repudiation? (5')

==================================== THE END ===================================