CS 3710: Introduction to Cybersecurity Midterm, fall 2024

Name

Be sure to write your name and e-mail ID on top of this page.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded. So please do that first. Sorry to have to be strict on this!

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

Free public WiFi

Is it really safe to use?

Ask Man in Middle

Page 2: Security mindset, terminology, & ethics

1. [3 points] *Briefly* define the security mindset.

2. [3 points] Write a rabbit program. You may use (reasonable) pseudo-code for this.

3. [3 points] List an abuse of each of the four ethical frameworks discussed in lecture.

4. [3 points] List three different activities that botnet owners might realistically use their botnet for.

Page 3: Encryption

5. [3 points] List the three different mathematical principles that various types of encryption are based on? Which one(s) does RSA use?

6. [3 points] *Briefly*, why is entropy needed for random numbers? List two good sources of entropy that a computer can use.

7. [3 points] *Briefly* explain how an RSA in-the-middle attack works. No long winded answers here!

8. [3 points] Give an example of *one* of the operations that AES performs to encrypt data.

Page 4: Networks and web security

9. [3 points] The presentation and session layers are in the OSI network model, but not the TCP/IP network model. *Briefly*, why not?

10. [3 points] For each of the layers in the TCP/IP network model, list one of the types of encryption used at that level. We are looking for a list here, not descriptions.

11. [3 points] Imagine you are Alice, and you are communicating with Bob to determine a shared private key using Diffie-Hellman key exchange. *Briefly* list the algorithm steps Alice uses to perform her side of the algorithm. You may assume that Bob sends value β over to Alice during his part of the algorithm.

12. [3 points] Of the DOS (Denial of Service) attacks discussed in lecture, which one is the most effective? *Briefly*, why?

Page 5: More web security

13. [3 points] *Briefly* what are the two main differences, as discussed in lecture, between TLS 1.2 and TLS 1.3? The version we studied in detail in lecture was version 1.2; version 1.3 was discussed after version 1.2 was presented.

14. [3 points] *Briefly* explain how the Heartbleed attack worked.

15. [3 points] How can an HTML <canvas> element be used to track you online?

16. [3 points] List five fields that are in a typical server certificate.

Page 6: No questions here

This page unintentionally left unblank.



xkcd #2966