Spring 2024
CS-352 Authentication Protocols Name: ______________________________

Please note: handouts *will not* be collected and graded. However, *you are expected to complete them.* The material on the handouts is a fair game for exams, quizzes, and assignments. It is in your best interest to use handouts during lectures. The instructor will be happy to assist you if you do not understand something.

1. What are the main issues in authentication?

2. Explain the different types of replay attacks.

3. At what layer of the TCP/IP model does SSL protocol reside?

4. Explain the Needham-Shroder public key protocol. How does it differ from the Needham Schroder Symmetric protocol and the Needham-Shroder Public Key Protocol.

5. Explain the process of obtaining an SSL certificate.

6. Describe the functions of the following components of the SSL protocol:

- HTTP Protocol

- HTTP Alert Protocol
- SSL ChangeCipherSpec Protocol
- SSL Handshake Protocol
- SSL Record Protocol

7. Describe the messages exchanged between server and client during the handshake phase of the SSL protocol.

8. Describe how SSL Record protocol processes text blocks.

9. SSL protocol allows compression of text blocks. How can compression actually increase the size of the compressed block of text?

10. What is SSL heartbeat? How does it relate to the Heartbleed vulnerability?

11. What is password salting? How can it help protect passwords?

12. Explain how password salting is implemented in Linux.

13. Many researchers think biometrics should replace passwords. Unlike passwords, people do not need to be remember their physical and behavioral characteristcs such as faces. This creates the need to protect biometric data stored by the systems. How can we protect biometric data without resorting to encryption?

14. Explain how Linux stores, manages, and protects passwords. Be sure to mention the roles of the `/etc/passwd`, /etc/shadow, hashing, and salting.

15. Consider the following approach to performing biometric-based authentication. Capture a biometric image, e.g. a face photo. Let I represent the captured image. Store H(I), the SHA-512 hash of I, on the system. In the biometrics lingo, this stage is called enrollment; entering user's biometric data into the system, to be used for future authentication. When the user wants to log in, he provides image I'. The system then computes H(I'). If H(I') == H(I), then grant access. If H(I') $\neq$ H(I), then deny access. Is there a problem with this approach? If so, then explain what it is. If not, explain why the approach will work.

16. Can Linux password salting scheme be used for protecting user's biometric data stored on the system? Explain.