CYBR 8410 – Distributed System Security

Midterm Exam (100 points)

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NUID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Design a scheme/protocol that fulfills the following requirements when entity A sends a message to entity B. (30 points)

* The message must be confidential during its transmission from A to B;
* B can detect any modification on the message during its transmission;
* B cannot claim any his forged message was sent from A;
* B can detect any replayed message from A (hint: timestamp or challenge).

1. It was stated that the inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Although those two characters are known to the attacker and need not be guessed, the salt still increases security. (20 points)
   1. Assuming there are at most N accounts on the password file, how many bits do we need for the salt? (10 points)
   2. Assuming that you have successfully answered 2.1 and understand the significance of the salt, here is another question. Wouldn’t it be possible to thwart completely all password crackers by dramatically increasing the salt size to, say, 24 or 48 bits? (10 points)
2. Supposing we are designing an authentication system. Please discuss what aspects we need to consider in this design. These aspects may include but are not limited to the risk assessment / assurance level / impact level, authentication method (such as password, biometric, and even the multi-factor authentication), protocol, potential attacks and defenses, etc. (30 points)
3. Please describe what the DoS attack is? You may answer this question from aspects including but not limited to what type of resources are required, what types of resources are targeted, and what techniques can be used and how they are used, etc. (10 points)
4. What defenses are possible against various types of DoS / DDoS attacks that we have learned. You may answer this question from aspects including but not limited to the detection, prevention, source tracing, and recovery, etc. (10 points)