This survey will be administered the first day of class and again toward the end of the semester. The purpose of this survey is to assess a student’s understanding of fundamental cybersecurity and network security concepts. When your survey responses are graded, the instructor will ask you to write your name at the top of page 1.

# Instructions

* Please complete as many question as you can in the time allotted.
* Unless otherwise stated, please circle the one choice that best answers the question.

# Cybersecurity Fundamentals

1. With respect to cybersecurity, what does CIA stand for?
   1. Central intelligence agency.
   2. Confidential internal audit.
   3. **Confidentiality, integrity, and availability.**
   4. Cyber information asset.
2. The security concept of anonymity is the property that certain transactions are:
   1. **Not attributable to any individual.**
   2. Not authenticated to any individual.
   3. Kept confidential to only those who have proper access.
   4. None of the above.
3. Which of the following statements is true about the security concept of assurance?
   1. Assurance is associated with how trust is provided and managed in computer systems.
   2. Assurance involves the interaction of policies, permissions, and protections.
   3. **All of the above.**
   4. None of the above.
4. **True** or false? The concept of authenticity in a network is the ability to determine if a message sent by a person or system is genuine.
5. Why is it hard to design a software system that satisfies both the security goal of non-repudiation and the fundamental security concept of anonymity?
   1. Because non-repudiation requires that transactions not be attributable to any individual while anonymity requires that transactions be identified back to a user.
   2. **Because non-repudiation requires that transactions be identified back to a user while anonymity requires that transactions not be attributable to any individual.**
   3. All of the above.
   4. None of the above.

*Please flip this sheet over for more questions …*

1. True or false? Keeping the existence of a software vulnerability a secret is always better than publicly revealing that the vulnerability exists.
   1. True.
   2. **False.**
2. True or false? It is possible to create a software system that has perfect (100%) security (i.e., has no vulnerabilities).
   1. True.
   2. **False.**
3. **True** or false? An open design is likely to lead to more secure software than a design that is proprietary. (An open design is a design that is publicly available for review while a proprietary design is kept a secret.)

# Network Security Concepts

1. Why do most of the network layers ***not*** have security features built into them?
   1. **Because the network layers were developed under the assumption that users are not malicious.**
   2. Because the network layers were developed to be as fast as possible; the researchers thought that security would slow these layers down too much.
   3. All of the above.
   4. None of the above.
2. True or **false**? The network layers have been designed to prevent distributed denial-of-service (DDOS) attacks.
3. Which of the following is true about cryptography?
   1. Symmetric cryptography is when the same key is used to encrypt and decrypt a message.
   2. Asymmetric cryptography is when a public key is used to encrypt a message and a private key is used to decrypt a message.
   3. **All of the above.**
   4. None of the above.
4. Why is the design of an application layer protocol so critical to the security of a distributed application?
   1. Because the application layer gives developers the opportunity to design for security.
   2. Because the application layer has the potential to satisfy many of the security goals and fundamental security concepts.
   3. **All of the above.**
   4. None of the above.