

Computer and Network Security
Fall Semester 2002

Quiz No. 1

July 30, 2002

Time Allowed: 20 Minutes

Total: 20 Points

Multiple choice questions carry one point each and short questions carry two points each

Name: _____

1. The requirement that only authorized parties can modify the computer system assets is called:
a. *Integrity* b. *Availability* c. *Secrecy* d. *Authenticity*
2. Interruption is an attack on the:
a. *Integrity* b. *Availability* c. *Secrecy* d. *Authenticity*
3. Attacks which are difficult to detect because there is no modification of data are called:
a. *Replay* b. *Dictionary Attacks* c. *Active Attacks* d. *Passive Attacks*
4. Which of the following is a passive attack:
a. *Interruption* b. *Traffic Analysis* c. *Modification* d. *Fabrication*
5. Encryption can protect from Traffic Analysis.
a. *True* b. *False*
6. Data padding and filler sequences can protect from Traffic Analysis.
a. *True* b. *False*
7. DES is a security mechanism.
a. *True* b. *False*
8. SSL is a security protocol.
a. *True* b. *False*
9. Computer security is constrained by societal factors.
a. *True* b. *False*
10. The type of attack in which an entity pretends to be another entity is called:
a. *Masquerade* b. *Replay* c. *Modification of* d. *Denial of service*
Messages

11. Differentiate between two types of authentication.

12. Differentiate between an adjudicated protocol and an arbitrated protocol with the help of a figure?

13. Differentiate between encryption and steganography in one sentence.

14. What is the job of each of the following characters in a security protocol?

(1) **Alice:**

(2) **Mallory:**

(3) **Trent:**

(4) **Eve:**

(5) **Dave:**

15. Label the parts of the figure given below:

