Sample Midterm Exam
CS 136

Name: _____

Student ID number: _____

Answer all questions. There are 100 points total. The test is closed book, closed notes.

Each multiple choice question is worth 4 points. There is one best answer for each multiple choice question.

1. Which of the following best describes how a process' authentication is most commonly performed in a typical operating system?
    a. Processes are not authenticated unless their application software requires it
    b. Processes must provide a password upon creation
    c. The process inherits the identity of the parent process
    d. Processes receive an identity associated with the executable they are running
2. Nonces, initialization vectors, and password salts, at a high conceptual level, provide the same characteristic benefit to a security system. Which of the below best describes that benefit?
    a. They simplify the problem of key distribution
    b. They ensure that the encrypted versions of two pieces of information are different
    c. They permit multi-factor authentication
    d. They improve diffusion in cryptography
3. Why are asymmetric ciphers more useful for authentication than symmetric ciphers?
    a. They are harder to break
    b. They provide faster authentication
    c. They allow parties to create cryptographic proof of identity that can be easily checked
    d. They provide both secrecy and authentication in a single cryptographic operation
4. Which of the following is typically an example of link level encryption?
    a. IPSec
    b. WPA2
    c. SSL
    d. VPNs

5. Which of the following best describes the relationship between security policies and security mechanisms?
    a. Security policies implement security mechanisms
    b. Security mechanisms implement security policies
    c. Security policies are a type of security mechanism
    d. Security mechanisms are a type of security policy
6. Which should change more frequently, a session key or an interchange key?
    a. A session key
    b. An interchange key
    c. Both should change at the same rate
    d. Neither should change
7. Which of the following is a disadvantage of the volume encryptor approach to encrypted file systems?
    a. It requires hashing a possibly weak password to obtain the encryption key
    b. It is not transparent to the user during ordinary operation
    c. Its cryptography is performed in a possibly untrusted user level process
    d. It does not offer fine-grained encryption at the file or directory level
8. Which of the following is a passive threat?
    a. A man-in-the-middle attack on an Internet connection
    b. A SQL injection attack
    c. A phishing attack
    d. Eavesdropping on an unencrypted wireless network
9. Which of the following is a disadvantage of the Bell LaPadula security model?
    a. It does not provably achieve its stated purpose
    b. It does not allow mandatory access control
    c. It does not address secrecy of information
    d. It makes it difficult to share necessary information among subjects with different security clearances
10. The Linux file access control model is a form of what access control method?
    a. An ACL
    b. Role based access control
    c. Capabilities
    d. An access control matrix
11. What is the confinement problem?
    a. Preventing a server from leaking confidential information
    b. Dividing a network into disjoint segments for security purposes
    c. Preventing details of key generation from becoming known to attackers
    d. Ensuring that all data that should pass through a VPN does so
12. Which of the following is a direct benefit of using a password vault?
    a. It reduces the risk of single sign-on
    b. It allows the user to select longer and more complex passwords
    c. It makes the user immune to a dictionary attack
    d. It prevents phishing attacks from succeeding

13. Which of the following kinds of cryptanalytic attacks is most likely to require physical access to the device performing the cryptography?
    a. A known plaintext attack
    b. Differential cryptanalysis
    c. A timing attack
    d. A chosen plaintext attack
14. Which of the following problems do we need to worry about most if we use a certificate hierarchy for authentication?
    a. IP spoofing
    b. Covert channels
    c. Transitive trust
    d. Replay attacks
15. Which of the following security mechanisms has trouble with revocation?
    a. Firewalls
    b. Data execution prevention
    c. Capabilities
    d. Honeypots
16. What kind of cryptographic algorithm is a one time pad, of the form described in class?
    a. A monoalphabetic substitution cipher
    b. A polyalphabetic substitution cipher
    c. A single permutation cipher
    d. A multiple permutation cipher
17. Which of the following is not an element of a cryptographic mode?
    a. A key
    b. Feedback
    c. Authentication
    d. A cipher
18. If a secure communication system exhibits the property of perfect forward secrecy, what benefit does it gain?
    a. Decrypting one packet encrypted with a particular key will not help an attack decrypt other packets encrypted with that key
    b. Proper use of entropy in the system is ensured
    c. Authentication of communicating parties is provided
    d. Divulging one session key will not help an attacker learn other session keys
19. What is cross-over error rate?
    a. The speed at which a DDoS defense system discovers which packets should be dropped to mitigate the attack
    b. A description of the effectiveness of a biometric authentication mechanism
    c. The rate at which a covert channel can transmit data
    d. A description of how far an error propagates in an encrypted data stream using a particular mode

20. Which of the following is true of password salts?
    a. They can be stored in plaintext form without reducing their benefit
    b. They need to be changed frequently to remain effective
    c. Users must take special care to choose their password salts
    d. The password salt should be derived from the password via a one-way cryptographic hashing function
21. Which of the following is true of authentication devices based on cryptographic challenge/response?
    a. The challenge is chosen from a small set of pre-defined personal questions
    b. Only asymmetric cryptography can be used
    c. Such devices ensure proper authentication even if they are stolen, without any further authentication required
    d. The cryptography should be performed on the device, rather than a computer the device is plugged into
22. Which of the following security guarantees does a typical paged virtual memory system attempt to provide to a process?
    a. No other process can read the data in its pages
    b. The page frames used by the process cannot be taken away by another process
    c. No covert channel can be used to transmit data in the process' pages to another process
    d. Buffer overflows cannot corrupt memory outside of the page frame where they occur
23. Which form of cryptography is likely to have the most problems preventing repudiation?
    a. A symmetric cipher
    b. An asymmetric cipher
    c. A block cipher
    d. A stream cipher
24. When is it easiest to perform source address filtering?
    a. As traffic enters a tier 1 autonomous system
    b. On arrival at scrubbing sites where traffic is diverted from its usual path
    c. On arrival at the destination machine
    d. As traffic leaves a local network and enters the Internet
25. Which of the following is an example of failing to provide complete mediation?
    a. Single sign on
    b. Use of DES
    c. Failure to salt passwords
    d. Lack of true randomness in key generation