Midterm Exam
CS 136
Spring, 2018

84/100

[redacted]

[redacted]

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 these issues enables both the Cold Boot attack and the Rowhammer attack?
   - a. Poor programming practices
   - b. Improper choice of operating system security policy
   - [✓ c.] Inadequate models of hardware behavior
   - d. Fundamental aspects of Internet design

✓

2. What is the purpose of an *own* right for an access control list?
   - a. It gives the possessor all access rights to the controlled object
   - [✓ b.] It allows the possessor to change the list
   - c. It stands for Other Write Null, and allows truncation of a file
   - d. It allows the possessor to create a new group with a subset of the access permissions he possesses for the object

X

3. What is the difference between masquerading and delegation access requests?
   - [✓ a.] Delegation requests explicitly indicate the party being delegated to
   - [✓ b.] Masquerading requests are commonly used to provide role based access control
   - c. Delegation requests cannot be performed across a network
   - d. Masquerading requests can be detected with ingress filtering

✓

4. What does the principle of attenuation of privilege mean?
   - a. Over time, privilege in a system grows progressively more limited
   - b. The finer the granularity of data that access control can be applied to, the harder the access control system is to set properly
   - c. Security is best if one limits the access privileges of all subjects to the minimum required for them to perform proper actions
   - [✓ d.] Subjects cannot increase their rights to access an object nor grant rights they do not possess to someone else

5. What is write-down? ✓
   - [✓ a.] Intentional reclassification of sensitive information to allow less privileged subjects to work with it
   - b. Saving passwords in a password vault
   - c. Removal of a subject from an access control list
   - d. Tagging an object for special care in performing access control

6. What party controls access to a piece of information in originator controlled access control systems? ✓
   - a. The party that owns the object that contains the information
   - b. A party specified by name in an associated access control list
   - [✓ c.] The party that first created the information
   - d. The party owning the system that implements the policy

7. What is the purpose of the Kerberos system? ✓
   - a. To prevent DDoS attacks
   - b. To detect attempts at buffer overflows
   - [✓ c.] To distribute authenticated keys in a distributed system
   - d. To prevent booting of a false version of an operating system

8. What does crossover error rate indicate? ✓
   - a. The probability that a bit flip of an encrypted message will corrupt future blocks of encrypted data, given use of a particular mode
   - [✓ b.] The point at which the false positive and false negative curves for a biometric intersect
   - c. The speed with which a heap-based buffer overflow attack will successfully compromise an application
   - d. The likelihood that a bug in a program will allow a remote user to compromise the system

9. Which of the following is NOT an advantage of providing full disk encryption in hardware vs. in the operating system? ✓
   - [✓ a.] Hardware full disk encryption will protect the disk even if it is stolen and examined on another machine
   - b. Hardware full disk encryption is faster
   - c. Hardware full disk encryption have less performance impact on user processes
   - d. Hardware full disk encryption does not require the operating system to protect the key

10. What is the purpose of a proactive password checker? ✓
   - a. To assist hackers in dictionary attacks
   - b. To rapidly check passwords provided by users trying to log in
   - c. To salt passwords
   - [✓ d.] To ensure users do not choose weak passwords

11. Which of the following is an advantage a DDoS attacker gains by using IP spoofing? ✓

- a. The attacker can more easily generate a large quantity of traffic
- b. It's harder for a defensive system to add capacity to meet the size of the attack
- [✓ c. It's harder for the defender to filter packets]
- d. The attacker can more easily perform a SYN flood attack

12. Which of the following is an advantage of Diffie Hellman key exchange? ✓

- [✓ a. Participants can share a symmetric key using only an unencrypted channel]
- b. It can be used to share a key among an arbitrary number of users
- c. It authenticates the participants in the key exchange
- d. It does not require pre-agreement on anything to exchange a key

13. For which of the following types of cipher is cryptanalysis by index of coincidence likely to be helpful? X

- [✓ a. A pure transposition cipher]
- [✓ b. A pure substitution cipher]
- c. A one-time pad
- d. An elliptic curve cipher

14. In the Needham Schroeder key exchange protocol, why does Alice believe she is not being subjected to a replay attack? ✓

- a. A message she receives from Trent contains the encrypted identity of Bob
- b. A message she received from Bob contains a nonce encrypted with the new session key
- c. A message she received from Bob contains information encrypted by Trent that includes the session key
- [✓ d. A message she receives from Trent contains the encrypted nonce she chose]

15. If an attacker obtains a site's salted and encrypted password file, what attack is he likely to perform? ✓

- a. A brute force attack
- [✓ b. An off-line dictionary attack]
- c. A social engineering attack
- d. A SQL injection attack

16. What type of attack does address space layout randomization (known in Windows as ASLR) address? ✓

- [✓ a. Buffer overflows]
- b. Dictionary attacks on passwords
- c. SQL injection attacks
- d. DDoS attacks

17. What is the purpose of padding in network defense? ✓

- [✓ a. To conceal characteristics of users' traffic]
- b. To provide greater integrity for messages
- c. To prevent IP spoofing
- d. To combat DDoS attacks

18. Why is DES no longer recommended for serious use?

a. The details of its implementation have become publicly known

[✓ b.] There is a known method of quickly cracking the cipher

c. Evidence shows the NSA has a back door allowing simple breaking of the cipher

✗ not wrong → [✓ d.] The key is too short

19. Which characteristic must a third party site (i.e., non-compromised site) have to be useful in performing a reflection attack?

✓ [✓ a.] It must accept requests from anywhere on the Internet

b. It must be a DNS server

c. It must not have ingress and egressing filtering enabled at its ISP

d. It must provide services based on TCP

20. If my firewall uses source address filtering to drop some packets going from my edge network to the Internet, which of the following packets can't it safely drop?

✗ [✓ a.] Packets using possibly spoofed addresses of my own edge network

b. Packets using unallocated addresses

[✓ c.] Packets using possibly spoofed addresses of some remote autonomous system

d. Packets using private network addresses

21. What issue causes users of RSA to keep increasing key length as time goes by?

a. Newly discovered vulnerabilities in the algorithm

b. Increased ease of brute force attacks on the key due to increased processing power

✓ [✓ c.] Increased ease of factoring large numbers due to increased processing power

d. Tendency of long-used keys to be divulged

22. What is the main purpose of multifactor authentication?

a. To slow down attackers trying to compromise a system

b. To provide authentication in key exchange protocols

c. To ensure complete mediation in a computer system

✓ [✓ d.] To compensate for security vulnerabilities in each of the factors

23. What security benefit is made possible by gathering entropy in a computer system?

✓ [✓ a.] Selection of better cryptographic keys

b. Detection of buffer overflows

c. Defense against DDoS attacks

d. Prevention of cold boot attacks

24. What does use of a Linear Feedback Shift Register (LFSR) to generate a key try to simulate?

✓

[✓ a.] Use of a one time pad
b. Diffie Hellman key exchange
c. Generation of an elliptic curve public/private key pair
d. Performing a known-plaintext attack on a cipher

25. What is the purpose of including a clock value in computation of a SYN cookie?

✓

a. To ensure authentication of the SYN message
[✓ b.] To prevent replay of ACK messages
c. To prevent use of spoofed source IP addresses
d. To prevent replay of SYN messages