7 61/100

Sam Rubenacker
504295581

Midterm Exam
CS 136
Winter, 2017

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

Multiple Choice questions. Each multiple choice question is worth 3 points. There is one best answer for each multiple choice question.

54/75

1. Chip and Pin is one form of two-factor authentication. What types of factors does it use? ✓
   a. Something you have and something you are
   b. Something you are and something you know
   c. Two different types of something you have
   [✓ d.] Something you know and something you have
2. Assuming random choices of passwords in each case, which of the following will be most resistant to brute force attacks? X A
   [✓ a.] 8 character passwords, upper and lower case alpha characters only ~~[illegible]~~ 52^8
   [✓ b.] 10 character passwords, lower case alpha characters only 26^{10}
   ~~c.~~ 8 character passwords, lower case and numeric characters only 36^8
   ~~d.~~ 6 character passwords, upper case, lower case, numeric characters only 62^6
3. What is the purpose of a shadow password file? X
   [✓ a.] To prevent non-privileged users from accessing some password-related information
   [✓ b.] To permit storage of passwords in encrypted forms
   ~~c.~~ To deceive attackers into trying to crack fake passwords
   ~~d.~~ To allow the system to send users plaintext versions of passwords they have forgotten
4. What is the confinement problem as defined by Lampson? X
   [✓ a.] Ensuring that untrusted code cannot access confidential information
   [✓ ~~b.~~] Preventing a server from leaking confidential information
   ~~c.~~ Ensuring that a cipher has proper quantities of confusion
   d. Ensuring that malicious code cannot propagate from one node to another

5. What is a covert channel?

✓

a. A type of VPN
b. A method of securely distributing a cryptographic key
[✓ c.] A channel that uses shared resources as a path of communication
d. A channel that uses one time pads to protect communications

6. Which of the following is an example of applying the principle of separation of privilege?

✗

[✓ a.] Running newly downloaded code in a sandbox that does not have access permission to most system resources
b. In a setuid root program, relinquishing superuser status as soon as possible
c. Prohibiting single sign-on to a sensitive system
d d. In a system using the Bell-La Padula model, requiring more than one user to approve write-down

7. Which of the following operations could not be performed by a filtering firewall?

✗

a. Preventing HTTP traffic from being delivered to a local machine that does not run a web server
[✓ b.] Stopping ping floods
c. Ensuring that all packets delivered to a VPN server have the address of a known partner VPN server
d d. Dropping email messages sent by unknown parties

8. Which of the following messages should not be put into a log?

✓

a. A message indicating that a program used OS features to escalate its privileges
b. A message indicating that a packet was delivered to a closed port on the receiving machine
[✓ c.] A message indicating the user ID and password for failed login attempts
d. A message indicating that a program attempted to open a file for which it did not have proper access permissions

9. Which of the following is true of the Biba security policy?

✓

a. Subjects cannot write objects with lower clearance levels
[✓ b.] Subjects cannot read objects with lower integrity levels
c. Subjects cannot write objects with lower integrity levels
d. Subject cannot read objects with higher clearance levels

10. What is mandatory about mandatory access control policies?

✓

a. The system requires the policy to be followed based on the choices of the owners of data items
b. The system does not allow individual users to prevent access to their data
[✓ c.] The system requires the policy to be followed regardless of the wishes of users
d. The policy must be applied to all data items in the system

11. Which of the following operations is easy to perform in a capability-based access control system?

✓

a. Taking access permissions away from a user
b. Determining the entire set of subjects that can access an object
[✓ c.] Determining the entire set of objects a subject can access
d. Ensuring proper access control when subjects and objects are located in different nodes of a network

12. Which desirable security property is most closely related to the use of a reference monitor?

✓

[✓ a.] Complete mediation
b. Least privilege
c. Fail-safe defaults
d. Economy

13. Which of the following is a strong mixing function?

✓

[✓ a.] SHA-1
b. A one-time pad using XOR to encrypt
~~c.~~ A polyalphabetic substitution cipher
~~d.~~ A triple columnar transposition cipher

14. Which of the following is the best example of an interchange key?

✓

[✓ a.] A public key contained in a X.509 certificate
b. The key established by a Diffie-Hellman key exchange
c. The key used to perform full disk encryption
d. A session key set up by the Needham-Schroeder protocol

15. What security problem is addressed by certificate pinning?

✓

[✓ a.] Creation of false certificates by legitimate certificate authorities
b. Certificate revocation
c. Handling updates to expired certificates
d. Improper copying of certificates

16. What type of attack does data execution prevention (known in Windows as DEP) address?

X

~~a.~~ SYN floods
~~b.~~ Brute force password guessing
[✓ c.] Return oriented programming attacks
[✓ d.] Buffer overflows

17. Which of the following statements is true of key use for different styles of network encryption applied to applications like web browsing?

X

[✓ a.] It can only use end-to-end encryption
b. It can use either end-to-end encryption or link level encryption, but not both
[✓ c.] It may use both end-to-end and link level encryption
~~d.~~ It can only use link level encryption

18. Which of the following is true of IPSec?

✓

~~a.~~ It only works with IPv4
[✓ b.] It can be used to ensure message integrity
~~c.~~ It includes procedures for key distribution
~~d.~~ Its transport mode encrypts an entire IP packet

19. What is a reflection attack? ✓

- a. A method of attack-back, in which a defender sends attack packets to the site that attacked him
- [✓ b.] A DDoS attack in which the attacker sends spoofed packets to legitimate sites, which respond to the target site
- c. An attack that results in the duplication of a virtual machine, allowing the attacker to replay its behavior
- d. An attack on a pseudo-random number generator that causes it to reuse old seeds

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

- a. Packets using spoofed addresses of my own edge network
- b. Packets using loopback addresses
- [✓ c.] Packets using spoofed addresses of some remote autonomous system
- d. Packets using private network addresses

21. What is a reverse firewall? ✓

- a. A firewall configured to specify only the packets that should be let through, rather than those that should be dropped
- b. A firewall used to control access to a secondary network connection
- c. A firewall used to trace attackers rather than filter their packets
- [✓ d.] A firewall that filters outgoing packets

22. Which of the following is not an element of a cryptographic mode? ✓

- a. A cipher
- b. A key
- [✓ c.] A key distribution mechanism
- d. A form of feedback

23. In the field of computer security, what is meant by non-repudiation? ✓

- a. An inability to revoke a capability or certificate
- b. An inability to change a system's trust in another system
- c. An inability to distinguish false positives from false negatives
- [✓ d.] An inability to deny one's past actions

24. What important security property does Diffie-Hellman key exchange provide? ✓

- a. Authentication of participating parties
- [✓ b.] Secrecy when using an insecure channel
- c. Immunity from man-in-the-middle attacks
- d. Immunity from replay attacks

25. Which of the following is a reasonable concern about security properties of data in a page frame on a modern general purpose operating system?

✓

a. Will an arbitrary process be able to read the data in a page frame allocated to my process?

b. Will a malicious process be able to prevent me from accessing data in my page frame?

[✓ c.] Will the data in the page frame be cleared before the page frame is given to another process?

d. Will a malicious process be able to prevent me from swapping the data in my page frame to disk?

Short Answer questions. Answer each of these in 1-3 sentences. Each question is worth 5 points.

22/25

1. Why is length an important property of an initialization vector?

In the past, security protocols like WEP have been exploited due to using a short initialization ~~N~~ vector. Longer initialization vectors are better because they make the initial encryptions performed by a stream cipher less predictable.

3

2. Why do capabilities used in a distributed system typically need to be cryptographic?

Since capabilities used in a distributed system are transmitted over the network, they need to be cryptographic ~~in order~~ so that malicious users cannot spoof bit patterns that look like a valid capability. Users are not checked against an aceess control list, so capabilities better be valid since there is no other last line of defense.

5

3. Why did users of non-Microsoft operating systems have a concern about the SecureBoot element of the UEFI?

Secure Boot in UEFI only allows certain versions of certain operating systems to boot by keeping a list of valid OS signatures.

5 Linux users were concerned that they would not be able to install Linux on new UEFI hardware because they did not think Microsoft would include Linux OS signatures in SecureBoot.

4. Why does full disk encryption fail to provide protection against a compromised operating system on the machine hosting the file system?

The OS is still able to decrypt files when they are read and encrypt files when they are written, because it has the key in a secure location.

5 The OS is in complete control. Therefore, if the OS is compromised, an attacker could make the OS do whatever they please, including read encrypted data since this is a valid action of the OS.

5. What is the purpose of an IPSec security association?

4 IPSec security associations are used in order to pick the type of encryption used during the communication of the secure one way channel.

more