Computer Security Capstone
Spring 2024
Midterm Exam

Problem 1: Multiple choices (2 points each). Select one correct answer from the four choices.

1. Which of the following viruses cannot conceal itself from the signature-based virus detection software?

   - Your answer _____ (A) Polymorphic virus; (B) Metamorphic virus; (C) Encrypted virus; (D) None of the above.

2. Consider the following propagation steps of a worm. Please give a correct order of the steps.
   (1) Execute the new worm.
   (2) Execute a short bootstrap program through the shell.
   (3) The bootstrap program calls back the parent program and downloads the remainder of the worm.
   (4) Exploit a vulnerability of the target system to successfully communicate with the system shell.

   - Your answer _____ (A) (1)(2)(3)(4); (B) (4)(2)(3)(1); (C) (4)(3)(2)(1); (D) (2)(4)(3)(1).

3. Which of the following statements about payload is FALSE?

   - Your answer _____
     (A) Both viruses and worms can have payloads.
     (B) Backdoor installs hidden programs on a system to maintain covert access to the system with root privilege.
     (C) Botnet is a collection of bots capable of acting in a coordinated manner, and controlled remotely.
     (D) Phishing exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source.

4. Which of the following statements is TRUE?

   - Your answer _____
     (A) Scripting viruses are platform dependent, so each of them can only be launched on specific platforms.
     (B) The access controls of current file systems can be used to defend against macro viruses.
     (C) Metamorphic worms can change both appearance and behavior patterns at different stages of propagation.
     (D) None of the above.

5. Which of the following statements is FALSE?

   - Your answer _____
     (A) A program or user interface should always respond in the way that is least likely to astonish the user.
     (B) Design should be kept secret rather than open; otherwise, attackers can know the design and easily break it.
     (C) Access decisions should be based on permission rather than exclusion.
     (D) For mutual security, design should minimize the functions shared by different users.

6. Which of the following statements about challenges of computer security is FALSE??

   - Your answer _____
     (A) Ciphering algorithms can be cracked one day when the computing power keeps increasing.
     (B) Security is usually not an integral part of the design process.
     (C) Strong security is regarded as an impediment to use of system.
     (D) Users are not perceived on benefits until a security failure.

7. Which of the following statements about attack trees is FALSE?

   - Your answer _____
     (A) The attack goal is specified at the root.
     (B) Each leaf indicates a way to initiate an attack, which is possible or impossible.
     (C) Each node (other than a leaf) always indicates a possible attack.
     (D) It can be used to effectively exploit the information available on attack patterns.

8. Disruption threats against system can be caused by incapacitation, corruption, or obstruction. Which objectives can be lost for the system due to the disruption threats?

   - Your answer _____
     (A) Confidentiality and availability.
     (B) Integrity and confidentiality.
     (C) Availability and integrity.
     (D) Confidentiality, integrity, and availability.

9. AES is introduced to replace 3DES due to several drawbacks of 3DES. Which of the following drawbacks is not included?

   - Your answer _____ (A) 64-bit block size is not efficient; (B) sluggish algorithm; (C) inefficient software code; (D) vulnerable algorithm.

10. Which of the following statements about Stream Ciphers is FALSE?

    - Your answer _____
      (A) They are almost always faster and use far less code than do block ciphers.
      (B) They would perform better than block ciphers for the encryption/descryption of a stream of data over a data communication channel.
      (C) They require a pseudorandom byte generator to generate key streams, which can be reused for different data streams.
      (D) They process input elements continuously.

11. Consider a scenario of the public key cryptography that Bob encrypts a message using his private key and sends this encrypted message to Alice. What kinds of security objectives can be achieved for the message?

    - Your answer _____ (A) sender authentication and data integrity; (B) sender authentication and data confidentiality; (C) data integrity; (D) data confidentiality.

12. Which of the following statements about smart tokens is FALSE?

    - Your answer _____
      (A) They have an embedded microprocessor for cryptographic operation.
      (B) They cannot be used for the authentication of web services.
      (C) They may be used as a dynamic password generator.
      (D) They have two types of electronic interface: contact and contactless.

13. Credential and token are cornerstones for E-authentication. For the password-based authentication method, which of the following statements is TRUE?

    - Your answer _____
      (A) Credential: the password.
      (B) Token: the username.
      (C) Credential: the data structure that binds a identity to a token possessed by the subscriber.
      (D) Token: the data structure that binds a identity to a credential possess by the subscriber.

14. Given the ACL of a file as follows, what is the effective access right of User Alice for the file?
    user::rwx
    user:Alice:rw-
    group::rwx
    mask::-wx
    other::r–

    - Your answer _____ (A) r–; (B) rw-; (C) -wx; (D) -w-.

15. Which of the following statements about ABAC is FALSE?

    - Your answer _____
      (A) It cannot be used to enforce the mandatory access control concept.
      (B) It allows an unlimited number of attributes to be combined to satisfy any access control rule.
      (C) Its cost is larger than that of the other access control approaches.
      (D) Compared with RBAC, ABAC has more complex trust relationships.

16. Consider that a user is authorized to connect a Wi-Fi network, but he launches an Man-in-the-Middle attack to intercept packets from some Wi-Fi devices and drop some of them to impede a specific service. Which of the following attack types for the Wi-Fi network does this attack belong to?

    - Your answer _____
      (A) Active and outside attack; (B) active and inside attack; (C) passive and outside attack; (D) passive and inside attack.

17. Which of the following statements about IPSec is FALSE?

- Your answer _____
  (A) To secure a TCP connection using the IPSec transport mode, two security associations are required.
  (B) The tunnel mode provides protection to the entire IP packet.
  (C) In the transport mode, ESP protects only the IP payload.
  (D) With the transport mode, hosts on networks behind firewalls can engage in communications without implementing IPSec.

18. Which of the following descriptions about TLS is FALSE?

- Your answer _____
  (A) Every TLS connection can be associated with multiple TLS sessions.
  (B) The change cipher spec protocol consists of a single message, which consists of a single byte with the value 1.
  (C) TLS sessions are used to avoid the expensive negotiation of new security parameters for each connection.
  (D) In Phase 2 of the TLS handshake, it is not necessary for the server to provide its certificate.

19. Which of the following statements about Kerberos is FALSE?

- Your answer _____
  (A) User's password is never passed over the network.
  (B) To enable interrealm authentication, the Kerberos server in each realm needs to share a secret key with the server in the other realm.
  (C) Ticket-granting server (TGS) allows the user to get multiple service tickets using only a single ticket-granting ticket.
  (D) The goal of using multiple realms is usually to maintain performance.

20. Consider the 802.1X access control in the wireless LAN (WLAN). There are three access paths in the WLAN: (1) one to the authentication server, (2) another to other wireless stations in the same WLAN, and (3) the other to distribution system (DS). For each of these access paths, which of uncontrolled and controlled ports shall be assigned?

- Your answer _____
  (A) (1) controlled; (2) controlled; (3) controlled.
  (B) (1) uncontrolled; (2) controlled; (3) controlled.
  (C) (1) uncontrolled; (2) uncontrolled; (3) uncontrolled.
  (D) (1) controlled; (2) uncontrolled; (3) uncontrolled.

21. Which of the following statements about wireless LAN security is FALSE?

- Your answer _____
  (A) EAP is an authentication framework for providing some common function, but not a specific mechanism.
  (B) Authentication is mutual between the client and the authentication server.
  (C) The protected data transfer phase includes TKIP and CCMP methods, both of which are not compatible to the old security method (i.e., WEP).
  (D) Both TKIP and CCMP support both message integrity and data confidentiality.

22. Which of the following statements does not belong to the issues with the PKI model?

    - Your answer _____
      (A) Relying on the user to make an informed decision when there is a problem verifying a certificate.
      (B) Assuming that all of the CAs in the trust store are equally trusted.
      (C) The hierarchical structure of the CA trust store is similar to that of the DNS with a single, large structure.
      (D) Different implementations in various web browsers and OS use different trust stores.

Problem 2: Short answer questions (2 points each). Please be brief and concise (No more than three sentences).

1. Consider that an email is sent to a group of people. The sender considers to use the type of clear-signed data, instead of signed data, to form the email. Please explain what objective the sender wants to achieve.

2. Why did Bruce Schneier, a computer security expert, say "if you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"? Please give your reason with an example.

3. Please give an example showing that a system's network attack surface decreases.

4. A fundamental security design principle is fail-safe defaults that access decisions should be based on permission rather than exclusion. Please explain the drawback of the exclusion-based access control or give an example showing its drawback.

5. Please give an example showing a repudiation threat.

6. Please explain what the weakness of the ECB (Electronic Codebook) is and why it happens.

7. Please give an example showing that the symmetric encryption is not a suitable tool for data authentication.

8. What is the reason for the recommended hash function, MD5, to have an inner loop with 1000 iterations?

9. When the Bloom filter is applied to the proactive password checking, it may cause false positive matches. Why do they not affect the security degree of the method?

10. Please give an access control example which ABAC can support but RBAC cannot by considering an online game.

11. Please explain why if a program with SetUID is not carefully implemented, network privileges may be leaked.

12. When the virus code is prepended to infected programs, it is easily detected. Why? How can the virus bypass such detection?

13. Why are traditional file system access controls of limited use for macro and scripting viruses?

14. Why cannot TCP packets be used for the amplification attacks that direct requests to the broadcast address of a network?

15. Please describe a countermeasure which can address or alleviate the HTTP-based attack, Slowloris, and explain why it is effective.

16. To defend against SYN spoofing attacks, we can use a cookie with cryptographically encoded critical information in reply to each initial SYN packet. However, it is not practical to apply this solution. Please describe a drawback of this solution.

17. How to solve the TLS Heartbleed exploit?

18. Consider that two gateways set up an IPSec tunnel. For each IP packet sent to the tunnel, it encrypts the entire IP packet, and then prepends a new IP header and an ESP header to the encrypted packet. How to enable this IPSec tunnel to support NAT (Network Address Translation)?

19. Due to the overheads in retrieving and storing certificate revocation lists, very few application actually do this. A lightweight protocol for the revocation was thus introduced in RFC 6960. It uses a new extension "Authority Information Access" in the certificate to check whether a certificate has been revoked. What is the major concept of this lightweight protocol? Why does it have smaller overhead?

20. Why do we always need to do encoding over encrypted copies of email messages (e.g., using the Radix-64 format)?

21. Why is DKIM transparent to end users when employing S/MIME?

22. What is the major concept for confirming continuity in time to improve the verification of X.509 certificates?

Problem 3: Message authentication (4 points). Suppose that a government agency releases a one-way hash function and its public key for the prevention of fake announcements. Some people may verify the sources of their received announcements, whereas some people even do not know how to use the public key or the hash function. However, all the people shall be able to get the information specified in the announcements. Please illustrate how the agency shall deal with each announcement and illustrate how the people verify that the announcement message is indeed sent by the agency. If your figure is not self-explained, please add some explanation

Problem 4: Proactive password checking: Bloom filter (4 points). Consider a Bloom filter with a bit array of 200 bits and 2 different hash functions, H_1 and H_2, for the checker of bad passwords. Assume that there have been two bad passwords: `abc` and `def`. Please use a string `123`, which is not a bad password, to give an example to explain when a false positive match can happen for the string.

Problem 5: DNS reflection attack (4 points). Consider a DNS reflection attack scenario where an attacker, a DNS server, and a victim have IP addresses, 1.2.3.4, 1.1.1.1, and 6.7.8.9, respectively. The attacker seeks to create a loop between the DNS server and the victim. Assume that the echo service bound to port 1050 at the victim is active. Please illustrate the packets exchange (three different packets) between these three parties for this attack, and specify source IP/Port and destination IP/Port for each packet.