Computer Security Capstone
Spring 2023
Midterm Exam

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

1. 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.

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

   - Your answer _____
   (A) Security is usually not an integral part of the design process.
   (B) Strong security is regarded as an impediment to use of system.
   (C) Users are not perceived on benefits until a security failure.
   (D) None of the above.

3. 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) a fatal weakness in the encryption algorithm; (D) inefficient software code.

4. 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.
   (D) They process the input one block of elements at a time.

5. Which of the following statements about Public-key Encryption is TRUE?

   - Your answer _____
   (A) It is more secure than symmetric encryption.
   (B) It has made symmetric encryption obsolete.
   (C) One of the factors on which its security strength depends is the key length.
   (D) Its key distribution is trivial.

6. Consider a scenario of the public key cryptography that Bob encrypts a message using Alice's public key and sends this encrypted message to Alice. What kind 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.

7. 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 data structure that binds a identity to a token possessed by the subscriber;
     (B) Token: the username;
     (C) Credential: the username;
     (D) Token: the data structure that binds a identity to a credential possessed by the subscriber.

8. Given the ACL of a file as follows, what is the effective access right of User Alice for the file?

   user::rwx

   user:Alice:-wx

   group::rwx

   mask::rw-

   other::r–

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

9. Consider that a user is authorized to connect a Wi-Fi network, but he eavesdrops on the wireless channel and steals data from other Wi-Fi users' wireless packets without affecting their Wi-Fi 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.

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

    - Your answer _____
      (A) To secure a TCP connection using the IPSec transport mode, only one security association is 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 tunnel mode, hosts on networks behind firewalls can engage in communications without implementing IPSec.

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

    - Your answer _____
      (A) Each TLS session can contain multiple TLS connections.
      (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 1 of the TLS handshake, two exchange messages, client_hello and server_hello, are encrypted.

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

- Your answer _____
  (A) Since it is inconvenient to query the user for his password for each service, the ticket-granting server (TGS) is introduced.
  (B) The user sends a pair of username and password to the authentication server (AS) for user authentication.
  (C) To enable interrealm authentication, the Kerberos server in each realm needs to share a secret key with the server in the other realm.
  (D) It prevents the ticket alteration by encrypting the ticket with a secret key known only to the AS and the TGS or the TGS and the application server.

13. 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) uncontrolled; (3) uncontrolled.
  (C) (1) uncontrolled; (2) controlled; (3) controlled.
  (D) (1) controlled; (2) uncontrolled; (3) uncontrolled.

14. 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.

15. Which of the following statements about PKI is TRUE?

- Your answer _____
  (A) A certificate cannot be revoked only based on a certificate revocation list.
  (B) The hierarchical structure of the CA trust store is similar to that of the DNS with a single, large structure.
  (C) The trust store includes a large list of CAs and their public keys.
  (D) The trust store can be used to make a decision when there is a problem verifying a certificate.

16. Bob wants to send an email about one important announcement to a group of people. In this group, some cautious people always read an email after the email signature has been verified, whereas some people even do not have S/MIME capability or encoding function in their email software. If all the people need to get the announcement, what kind of S/MIME content types should be used for the Bob's email?

- Your answer _____
  (A) Enveloped data; (B) Signed data; (C) Clear-signed data; (D) Any of the above types.

17. Which of the following reasons about using DKIM is FALSE?

- Your answer _____
  (A) Users need to have certificates to enable DKIM.
  (B) DKIM can prevent forgers from masquerading as good senders.
  (C) DKIM signs both message header and content.
  (D) DKIM is transparent to the end user.

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

    - Your answer _____
      (A) It can 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 smaller than that of the other access control approaches.
      (D) Compared with RBAC, ABAC has more complex trust relationships.

19. Which of the following statements is FALSE?

    - Your answer _____
      (A) Botnet is a collection of bots capable of acting in a coordinated manner.
      (B) Phishing exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source.
      (C) Worms need a host program to execute.
      (D) Both viruses and worms can have payloads.

20. Which of the following actions does not belong to the propagation behaviors of the malware?

    - Your answer _____
      (A) Infecting existing programs in a system.
      (B) Sending emails to the users in a contact list and attaching itself.
      (C) Disabling the antivirus software.
      (D) Exploiting a vulnerability to copy itself to another host.

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

1. 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.

2. Why should design be open rather than secret from fundamental security design principles?

3. Please give an example about applying least privilege, which is a fundamental security design principle.

4. Please give an example that a system's network attack surface increases.

5. How can the CBC (Cipher Block Chaining) mode overcome the weakness of the ECB (Electronic Codebook)?

6. The symmetric encryption can ensure authentic source, no altered content, and proper message timeliness with a shared key between only the sender and the receiver, an error-detection code, and a sequence number, respectively. Why is it not a suitable tool for data authentication?

7. How can a salt value in the hashed password techniques greatly increase the difficulty of offline dictionary attacks?

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 them not affect the security degree of the method?

10. Why do we need a random number in most challenge-response protocols for remote user authentication?

11. Please give an access control example which ABAC (Attribute-based Access Control) can support but RBAC (Role-based Access Control) cannot by considering an online shopping mall.

12. Capability tickets have greater security problem than ACLs, because tickets may be forged or tampered. Please recommend a solution to address it.

13. Bob wants to develop an anomaly detection program for normal users. But, he encounters an issue that the program needs the root privilege to use `RAW SOCKET` but the normal users are not allowed to have it. Please give an advice about how to achieve it and explain the reason.

14. Why is the traditional UNIX file access control not scalable so that the extended ACLs are needed?

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

16. Can the HTTP-based attack, Slowloris, be detected by signature-based solutions? Why?

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. In the Kerberos system, why can the ticket sent by the authentication server be decrypted by the ticket-granting server, but not be decrypted by the user?

Problem 3: Message authentication (5 points). Suppose that a company CEO allows employees to send secret messages, which can only be decrypted and read by the CEO, to him/her for recommendation; moreover, the CEO can verify the sender of each message. To this end, he releases a one-way hash function and his certificate to employees, and also collects certificates from all the employees. Please illustrate how an employee generates a secret message to the CEO, and how the CEO decrypts and verifies the secret message. If your figure is not self-explained, please add some explanation.

Problem 4: Interrealm authentication (5 points). Assume that Companies A and B both use the Kerberos system to provide authentication services between users and application servers. One day, these two companies collaborate on one project and decide to deploy a project server in Company B. They plan to use the interrealm authentication of their Kerberos servers to authenticate Company A's employees who want to access the project server in Company B. Certainly, to enable this authentication method, Company B trusts the Kerberos server of Company A to authenticate the users of the project server.

Assume that the interrealm authentication method has been deployed and the corresponding Kerberos servers have shared necessary secret keys. Please use a diagram to show necessary message exchanges among the following entities for a scenario that an employee of Company A wants to access the project server (the employee has not obtained any tickets): a client device belonging to the employee, the project server, Company A's AS/TGS, and Company B's AS/TGS. Please indicate the major purpose of each exchanged message (no more than 6 English words for each message).

Problem 5: DNS reflection attack (5 points). Consider a DNS reflection attack scenario where an attacker, a DNS server, and a victim have IP addresses, 1.2.3.4, 8.8.8.8, and 5.6.7.8, respectively. The attacker seeks to create a loop between the DNS server and the victim. Assume that the echo service 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.

Problem 6: ARP spoofing attack (5 points). Consider a Wi-Fi network with one AP (IP: 192.168.0.1; MAC: aa:aa:aa:aa:aa:aa) and two clients, Attacker (IP: 192.168.0.2; MAC: bb:bb:bb:bb:bb:bb) and Victim (IP: 192.168.0.3; MAC: cc:cc:cc:cc:cc:cc), both of which associate with the AP. Assume that Attacker has successfully launched an ARP spoofing attack to intercept all the traffic to/from Victim. Consider that Victim pings to 8.8.8.8 by sending an ICMP request to it and then receiving an ICMP reply. Please illustrate all the packets caused by the ping and observed by Attacker. For each packet, please specify five kinds of information: message type (request or reply), source/destination IP addresses, and source/destination MAC addresses.