

Computer Security Capstone

Sample Midterm Exam

PROBLEM	MAX SCORE
1	30
2	40
3	5
4	5
5	5
6	5
Roll call	10
TOTAL	100

DO NOT TURN TO THE NEXT PAGE UNLESS YOU GET PERMISSION !!

Problem 1: Multiple choices (1.5 points each). Select one correct answer from the four choices.

1. Ransomware, which attempts to encrypt the victim's files, can result in a loss of ____.
 - Your answer ____ (A) confidentiality; (B) integrity; (C) authenticity; (D) availability.
2. DoS attacks impair the ____ of networks, systems, or applications.
 - Your answer ____ (A) availability; (B) privacy; (C) integrity; (D) confidentiality.
3. ____ allows a security breach to be traced back to a responsible party.
 - Your answer ____ (A) Integrity; (B) Authenticity; (C) Accountability; (D) Availability.
4. ____ is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.
 - Your answer ____ (A) Perturbation; (B) Inference; (C) Compromise; (D) Partitioning.
5. Which of the following statements about fundamental security design principles is FALSE?
 - Your answer ____
 - (A) Design should be open rather than secret.
 - (B) Access decisions should be based on exclusion rather than permission.
 - (C) Design should minimize the functions shared by different users for mutual security.
 - (D) A program or user interface should always respond in the way that is least likely to astonish the user.
6. The purpose of a ____ is to produce a “fingerprint” of a file, message, or other block of data.
 - Your answer ____ (A) secret key; (B) digital signature; (C) keystream; (D) hash function.
7. Recognition by fingerprint, retina, and face are examples of ____.
 - Your answer ____ (A) face recognition; (B) static biometrics; (C) dynamic biometrics; (D) token authentication.
8. A concept that evolved out of requirements for military information security is ____.
 - Your answer ____ (A) reliable input; (B) mandatory access control; (C) open and closed policies; (D) discretionary input.
9. 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::r-x
other::r-
 - Your answer ____ (A) r-; (B) rw-; (C) rwx; (D) r-x.
10. ____ provide a means of adapting RBAC to the specifics of administrative and security policies in an organization.

- Your answer ____ (A) Constraints; (B) Mutually Exclusive Roles; (C) Cardinality; (D) Prerequisites.
11. 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 larger than that of the other access control approaches.
 - (D) Compared with RBAC, ABAC has less complex trust relationships.
12. Suppose Alice agrees to sign a contract with Bob, and they use a secure hash function for message authentication of the contract. By exploiting a vulnerability of the hash function, Bob prepares two contracts and then lets Alice sign the first contract. Afterwards, Bob is able to claim that the second contract is authentic. Which of the following properties is not satisfied by this hash function so that the above attack can happen?
- Your answer ____
 - (A) $H(x)$ is relatively easy to compute for any given x .
 - (B) Pre-image resistant: for any given code h , it is computationally infeasible to find x such that $H(x) = h$.
 - (C) Second pre-image resistant: for any given block x , it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
 - (D) Collision resistant: it is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
13. 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.
14. 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.
15. Which of the following reasons about using DKIM is TRUE?
- Your answer ____
 - (A) Users need to have certificates to enable DKIM.
 - (B) DKIM depends on both the sending and receiving users employing S/MIME.

- (C) DKIM signs only the message content.
 (D) DKIM is transparent to the end user.
16. Which of the following descriptions about TLS is FALSE?
- Your answer ____
 - (A) Each 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 1 of the TLS handshake, two exchange messages, client_hello and server_hello, are not encrypted.
17. To set up an HTTPS session, what is the establishment order of the following three connections/sessions?
- Your answer ____
 - (A) HTTP session → TLS session → TCP connection.
 - (B) TCP connection → TLS session → HTTP session.
 - (C) HTTP session → TCP connection → TLS session.
 - (D) TCP connection → HTTP session → TLS session.
18. 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.
19. Which of the following statements about PKI is FALSE?
- Your answer ____
 - (A) A certificate can be revoked 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) It relies on the user to make an informed decision when there is a problem verifying a certificate.
20. 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.

Problem 2: Short answer questions (2.5 points each). Please be brief and concise (No more than three sentences).

1. By considering one web page, please give an example of the condition that its attack surface is increased.
2. Why should the key stream of the stream cipher NOT be reused?
3. For the message authentication, why is the one-way hash function better than the message authentication code (MAC)?
4. How can a salt value in the hashed password techniques greatly increase the difficulty of offline dictionary attacks?
5. In the traditional UNIX implementation, the password scheme repeats the modified DES encryption for 25 times. What is the reason for so many encryption iterations in terms of security?
6. Offenders can easily duplicate your memory cards after the cards are swiped through their readers, but this duplication does not work for smart cards. Why?
7. 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.
8. Please give an access control example which ABAC (Attribute-based Access Control) can support but RBAC (Role-based Access Control) cannot.
9. Why is the increased performance cost of the ABAC mechanism less noticeable for Web services and cloud computing?
10. Why do we need a random number in most challenge-response protocols for remote user authentication?
11. How to solve the TLS Heartbleed exploit?
12. 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. Does this IPSec tunnel support NAT (Network Address Translation)? Why?

13. The Kerberos system keeps a password for each user to do user authentication. How does the user authentication proceed with the password?
14. 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?
15. Consider the 802.1X access control in the wireless LAN (WLAN). There are three access paths in the WLAN: one to the authentication server, another to other wireless stations in the same WLAN, and the other to distribution system (DS). For each of these access paths, which of uncontrolled and controlled ports shall be assigned?
16. TKIP ensures that every data packet is sent with a unique encryption key. How can it be achieved?

Problem 3: Message authentication (5 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 (5 points). Consider a Bloom filter with a bit array of 500 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: 123 and 456. Please use a string `abc`, which is not a bad password, to give an example to explain when a false positive match can happen for the string.

Problem 5: 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 6: 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.