Introduction to Computer Security
Spring 2019
Midterm Exam

PROBLEM	MAX SCORE
1	42
2	33
3	7
4	6
5	6
6	6
TOTAL	100

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

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

1. A loss of ____ is the unauthorized disclosure of information.
    - Your answer ____ (A) confidentiality; (B) integrity; (C) authenticity; (D) availability.
2. ____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
    - Your answer ____ (A) Availability; (B) Privacy; (C) System Integrity; (D) Data Integrity.
3. A(n) ____ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action can be taken.
    - Your answer ____ (A) attack; (B) adversary; (C) countermeasure; (D) protocol.
4. Masquerade, falsification, and repudiation are threat actions that cause ____ threat consequences.
    - Your answer ____ (A) unauthorized disclosure; (B) disruption; (C) deception; (D) usurpation.
5. ____ is a procedure that allows communicating parties to verify that received or stored messages are authentic.
    - Your answer ____ (A) Encryption; (B) Digital signature; (C) Message authentication; (D) Cryptanalysis.
6. ____ 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.
7. The ____ is what the virus ”does”.
    - Your answer ____ (A) infection mechanism; (B) trigger; (C) logic bomb; (D) payload.
8. 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.
9. Recognition by fingerprint, retina, and face are examples of ____.
    - Your answer ____ (A) face recognition; (B) static biometrics; (C) dynamic biometrics; (D) token authentication.
10. To counter threats to remote user authentication, systems generally rely on some form of ____ protocol.
    - Your answer ____ (A) digital signature; (B) challenge-response; (C) authorization; (D) message authentication.

11. 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.

12. ____ 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.

13. Which of the following statements is TRUE for repudiation?

    - Your answer ____
      (A) An entity deceives another by falsely denying responsibility for an act.
      (B) An entity assumes unauthorized logical or physical control of a system resource.
      (C) An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
      (D) An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.

14. 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.

15. 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.

16. 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 $H(x) = H(y)$.

17. 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.

18. To have the cellular service, a user needs to apply for an account with an SIM card and install the SIM on the phone. When the user turns on the phone, the phone uses the SIM to do authentication with the cellular core network. Which of the following roles in the E-Authentication architecture model CANNOT be taken care of by the core network?

    - Your answer ____
      (A) relying party; (B) registration authority; (C) credential service provider; (D) verifier.

19. Suppose that Bob wants to secure a database for a web service, which requires user input on web pages. He knows the expected queries and understands how the database should behave normally, but have little knowledge about possible attacks. Which of the following countermeasures is NOT appropriate for Bob to take?

    - Your answer ____ (A) Signature-based detection; (B) Anomaly-based detection; (C) Parameterized query insertion; (D) Run-time prevention.

20. Which of the following statements about different kinds of viruses is FALSE?

    - Your answer ____
      (A) Encrypted virus: using encryption to obscure its content.
      (B) Stealth virus: hiding itself from detection by anti-virus software.
      (C) Polymorphic virus: rewriting itself completely at each iteration.
      (D) Metamorphic virus: changing both of its behaviors and appearance.

21. 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.

Problem 2: Short answer questions (3 points each). Please be brief and concise (No more than three sentences).

1. Why is the symmetric encryption NOT a suitable tool for data authentication?
   Please give two reasons.

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

3. 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?

4. 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?

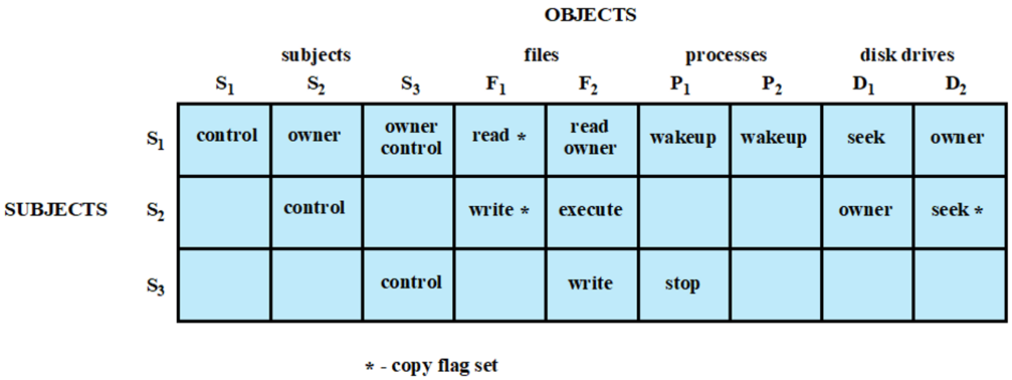
5. Why do we need a random number in most challenge-response protocols for remote user authentication?

6. 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.

7. Assume that you seek to launch a SQLi attack against a website where the following pseudo codes are used for user authentication.

```
/**Input parameters are userName and passWord **/
cmd = "SELECT * FROM users WHERE (name = '" + userName + "') and (pw = '"+ passWord +"');'
result = SQL_execute_command(cmd);
if result != null then
    login granted
else
    login rejected
```

   Please specify which values of userName and passWord can be used for a successful SQLi attack, where you can login this website without any legitimate username/password pairs.



		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
SUBJECTS	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Figure 1: Extended access control matrix.

8. Please answer True or False to judge whether the following operations are allowable, given the extended access control matrix in Figure 1.

   (1) S_1 can `destroy` itself (i.e., S_1). (2) S_2 can enable S_3 to `read` F_1. (3) S_1 can enable S_3 to transfer `read` of D_2 to other subjects.

9. Please give an access control example which ABAC (Attribute-based Access Control) can support but RBAC (Role-based Access Control) cannot.

10. What is the difference between a virus and a worm?

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

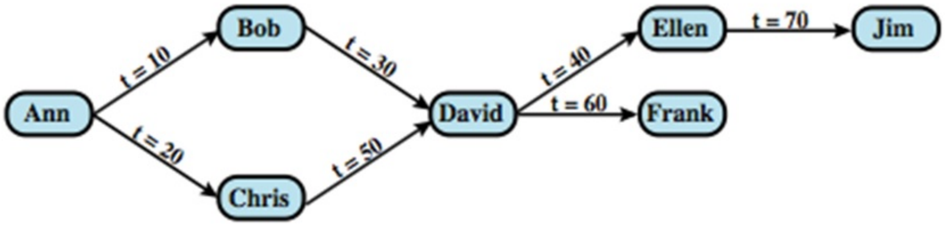


Figure 2: An example of cascading authorizations.

Problem 3: Message authentication (7 points). Suppose that a government agency releases a one-way hash function and its public key for the prevention of fake announcements. Please illustrate how the agency can send people an announcement message with message authentication using public-key encryption and the one-way hash function, and how people can verify the announcement message. Note that encrypting the original message is prevented. If your figure is not self-explained, please add some explanation.

Problem 4: Proactive password checking: Bloom filter (6 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: Cascading authorizations (6 points). Consider an example of cascading authorizations in Figure 2, which shows a sequence of grant operations for a specific access right on a table. An arrow represents that the granting of privileges cascades from one user to another using the grant option. The time associated with each arrow shows when the granting happens. Suppose that Ann revokes the access right from Bob at $t = 80$. Please show the resulting diagram of access right dependencies.

Problem 6: DNS reflection attack (6 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.