Name

CWID

Exam
A

CS458 - Spring 2022 - Final Exam

Wednesday, May 4th, 2022
2:00-4:00pm

Please leave this empty!

1.1	□	1.2	□	1.3	□	1.4	□	Sum	□

Question 1.1 True or False (10 Points)

1. [True/False] Diffe-Hellman can be used to sign a message.
2. [True/False] The Bell-LaPadula security model allows a subject S at the Top Secret level to write object O at the Unclassified level.
3. [True/False] A public-key certificate scheme alone does not provide the necessary security to authenticate the public key.
4. [True/False] In Kerberos, the information inside a TGT (Ticket Granting Ticket) can only be understood by the KDC (Key Distribution Center).
5. [True/False] In a traffic analysis attack, a malicious user observes patterns of communications, without having to read the message contents.
6. [True/False] In `Mandatory Access Control`, resource owners can override system policy and allow other users access to his resources when the system forbids it.
7. [True/False] SQL injection attacks do not exploit a specific software vulnerability; instead they target websites that do not follow secure coding practices for accessing and manipulating data stored in a relational database.
8. [True/False] `X.509` defines the format for private-key certificates.
9. [True/False] Access control is a security service that controls who can have access to a resource
10. [True/False] Although public announcement of public keys is convenient, anyone can forge a public announcement.

Question 1.2 (15 Points)

Circle the right answer(s):

1. The likelihood of a threat source taking advantage of a vulnerability is called? (*circle only one*)
   (a) Vulnerability
   (b) Threat
   (c) Risk
   (d) Exposure

2. A security policy provides a way to . . .? (*circle only one*)
   (a) establish a cost model for security activities.
   (b) allow management to define system recovery requirements.
   (c) identify and clarify security goals and objectives.
   (d) enable management to define system access rules.

3. Which of the following feature does a digital signature provide? (*circle only one*)
   (a) It provides the ability to encrypt an individual?s confidential data.
   (b) It ensures an individual?s privacy.
   (c) It identifies the source and verifies the integrity of data.
   (d) It provides a framework for law and procedures.

4. A company is experiencing overwhelming visits to a main web server. The IT department is developing a plan to add a couple more web servers for load balancing and redundancy. Which requirement of information security is addressed by implementing the plan? (*circle only one*)
   (a) integrity
   (b) scalability
   (c) availability
   (d) confidentiality

5. What are two security implementations that use biometrics? (*circle all that apply*)
   (a) voice recognition
   (b) phone
   (c) fingerprint
   (d) credit card

6. A type cryptographic attack where it is based on the probability of two different messages using the same hash function to produce the same message digest is? (*circle only one*)
   (a) Birthday attack
   (b) Statistic attack
   (c) Differential cryptanalysis attack
   (d) Known ciphertext attack

7. An access control system that grants users only those rights necessary for them to perform their work is operating on which security principle? (*circle only one*)
   (a) Discretionary Access
   (b) Least Privilege
   (c) Mandatory Access
   (d) Separation of Duties

8. Which of the following refers to a series of characters used to verify a user's identity? (*circle only one*)
   (a) Token serial number
   (b) User ID
   (c) Password
   (d) Security ticket

9. What is the trusted registry that guarantees the authenticity of client and server public keys? (*circle only one*)
   (a) Public key notary.
   (b) Certification authority.
   (c) Key distribution center.
   (d) Key revocation certificate.

10. When downloading software from Internet, why do vendors publish MD5 (or sha-1/sha-2) hash values when they provide software to customers? (*circle only one*)
    (a) Recipients can confirm the authenticity of the site from which they are downloading the patch.
    (b) Recipients can request future updates to the software by using the assigned hash value.
    (c) Recipients can verify the software's integrity after downloading.
    (d) Recipients need the hash value to successfully activate the new software.

11. The accounting branch of a large organization requires an application to process expense vouchers. Each voucher must be input by one of many accounting clerks, verified by the clerk's applicable supervisor, then reconciled by an auditor before the reimbursement check is produced. Which access control technique should be built into the application to best serve these requirements? (*circle only one*)
    (a) Mandatory Access Control (MAC)
    (b) Password Security
    (c) Role-based Access Control (RBAC)

12. What best describes two-factor authentication? (*circle only one*)

    (a) Something you know.

    (b) Something you have.

    (c) Something you are.

    (d) A combination of two listed above.

13. Which of the following protects Kerberos against replay attacks?(*circle only one*)

    (a) Passwords.

    (b) Cryptography

    (c) Time stamps.

    (d) Tokens.

14. Which item is the responsibility of key management? (*circle only one*)

    (a) Access controls and encryption.

    (b) Access control, user authentication and authorization.

    (c) Key generation and destruction.

    (d) Key length and algorithm propriety.

15. What is the main difference between a “Normal” SQL injection and a “Blind” SQL injection vulnerability? (*circle only one*)

    (a) The request to the web server is not visible to the administrator of the vulnerable application.

    (b) The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.

    (c) A successful attack does not show an error message to the administrator of the affected application.

    (d) The vulnerable application does not display errors with information about the injection results to the attacker.

Question 1.3 (10 Points)

A company is implementing `Bell-Lapadula model` for access control. Below are the access control matrix and the classifications of various objects and people. After going through them answer the following questions. Make sure to show the decision process that lead to your answer.

	`Salaries`	`Vacations`	`Building map`	`Orientation`
`Bob`	write, read	-	read	read
`Chris`	-	write, read	read	read
`Amy`	write, read	-	read	write, read
`Laura`	read	-	write, read	-

- There are three levels: *secret* > *confidential* > *normal*.
- `Amy` and `Chris` are cleared as *confidential*
- `Bob` is cleared as *secret*
- `Laura` is cleared as *normal*
- Files `Salaries` and `Vacations` are classified *secret*
- File `Building map` is classified *confidential*
- File `Orientation` is classified *normal*

(a) Which files can `Chris` read?

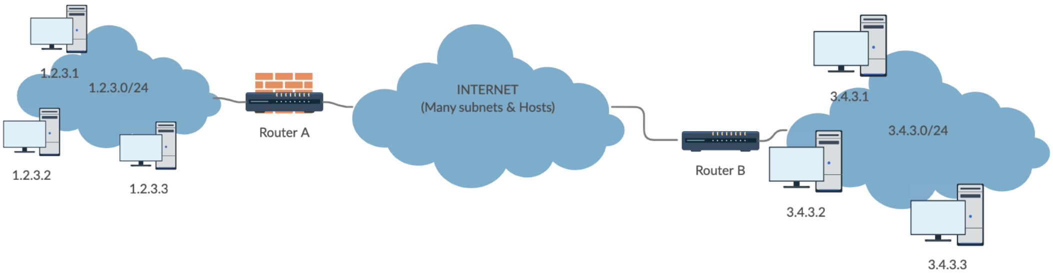
(b) Who can read the file `Building map`?

(c) Who can write on file `Vacations`?

(d) How can we grant to `Laura` permission to read the `Vacations` and `Orientation` files?

Question 1.4 (15 Points)

Consider the following network diagram. On the two subnets assume there are many hosts (although only three hosts are shown for each subnet due to space). Assume the firewall is running on `Router A` and the default policy is `allow/accept`.



For each of the following policies, write a rule that implements it by filling in the table. For each part, assume initially there are no firewall rules except the default policy; i.e. your answer in *part (b)* is independent of your answer in *part (a)*.

(a) Block all hosts on network `3.4.3.0/24` from accessing any `SSH` servers on network `1.2.3.0/24`.

Direction	**Source IP**	**Destination IP**	**Protocol**	**Source Port**	**Destination Port**	**ACTION**

(b) Block host `1.2.3.3` from browsing to any websites in network `3.4.3.0/24`.

Direction	**Source IP**	**Destination IP**	**Protocol**	**Source Port**	**Destination Port**	**ACTION**

(c) Block any host in subnet `3.4.3.0/24` from Ping any host in subnet `1.2.3.0/24`

Direction	Source IP	Destination IP	Protocol	Source Port	Destination Port	ACTION

(d) Assume the default policy is `drop`. Allow any host on network `1.2.3.0/24` to browsing to any secure websites in network `3.4.3.0/24`.

Direction	Source IP	Destination IP	Protocol	Source Port	Destination Port	ACTION