National University of Computer and Emerging Sciences

Lahore Campus

Information Security (CS3002)

Date: January 2nd, 2025

Course Instructor(s)

AK, AIS, MZH, SMI, AH, RAR

Final Exam

Total Time (Hrs): 2.5

Total Marks: 75

Total Questions: 8

SOLUTION

_____ _____ _____

Roll No Section Student Signature

Do not write below this line

Note: Attempt Question No. 1 & 2 on this sheet. Attach this question paper with your Answer Book. Students will also write the formula used in each calculation, no direct answer will be accepted. If you think some information is missing then make an assumption and write it clearly.

CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management
CLO-2	Discuss legal, ethical, and professional issues in information security
CLO-3	Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy
CLO-4	Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security
CLO-5	Describe issues related to ethics in the field of information security

CLO #: 1

Question No. 1: Choose the correct option. [10 marks]

1. The UNIX password scheme verifies a password by providing a _____; then looking up a _____ and extracting the relevant _____ to calculate the _____.
   a. User ID; Password file; Salt; Hashed password.
   b. Password; Password file; Checksum; Cleartext password.
   c. Salt; Salt file; Salt; Cleartext password.
   d. Password; Password file; Salt; Hashed password.

2. For an N-system symmetric cryptographic network, if a new system comes in, __ new keys are generated, whereas if a system leaves, __ keys are removed, and each system remembers ___ keys.
   a. 2N; N-1; N
   b. N; N-1; N-1
   c. N; 2N; N-1
   d. N/2; N+1; N+1

3. Biometric verification is considered to be _____ authentication, since it involves characteristics whose proof of origin _____, and _____ is difficult.
    a. repudiable; cannot be denied; miscalculation
    b. non-repudiable; can be denied; forgery
    c. repudiable; cannot be described; forgery
    d. non-repudiable; cannot be denied; forgery

4. In a _____ XSS attack, user input is _____ in a response that includes ____, without _____ storing the user provided data.
    a. Reflected; immediately returned by a web application; browser output; permanently
    b. Reflected; immediately returned by a web application; user input; permanently
    c. Stored; immediately returned by a web application; browser output; temporarily
    d. Stored; immediately returned by a web application; user input; permanently

5. XSS countermeasures include:
    a. Decoding, input classification (using blacklists/whitelists), and public key exchange
    b. Encoding, using stored procedures, and input sanitization
    c. Encoding, input classification (using blacklists/whitelists), and input sanitization
    d. Encoding, input classification (using blacklists/whitelists), and SQL injection

6. An XSS attack can be of the following forms:
    a. Cookie theft & keylogging
    b. Phishing
    c. STP theft
    d. Both (a) and (b) are correct

7. Within cross-site request forgery attacks, an end user is forced to execute _____ on a web application in which they are _____. If the victim is a normal user, such an attack _____.
    a. unwanted actions; currently authenticated; may change state
    b. unwanted actions; currently unauthenticated; may change the DOM environment
    c. malicious executable files; currently authenticated; may change the DOM environment
    d. unwanted actions; currently authenticated; may compromise the entire web application

8. Which of the following is NOT a part of the Ten Commandments of Computer Ethics?
    a. Thou shalt not use a computer to steal.
    b. Thou shalt not use a computer to bear false witness.
    c. Thou shalt not upgrade software without informing the vendor.
    d. Thou shalt not copy or use proprietary software without payment.

9. The origin header is a countermeasure for _____ attacks, it contains origin properties of URL such as port, _____ and _____
    a. CSRF; scheme; IP version
    b. DDoS; hostname; IP version
    c. SQL Injection; hostname; scheme
    d. CSRF; hostname; scheme

10. Which of the following is NOT a function of SSL?
    a. Peer authentication
    b. Message confidentiality
    c. Header encryption
    d. Protection against replay attacks

CLO #: 2

Question No. 2 [6 marks]

Pakistan Electronic Crimes Ordinance (PECA) defines several offences, some of which are listed below:

a) unauthorized access
b) unauthorized access to critical infrastructure systems
c) unauthorized copy
d) unauthorized copy of critical infrastructure data
e) unauthorized modifications
f) unauthorized modifications to critical infrastructure systems
g) electronic forgery
h) distributing and transmitting malicious code
i) cyber stalking

For each of the following case studies, pick one offense from the above list that best matches the case description.

Statement	Answer
An individual uploads spyware disguised as a free utility on a public forum.	h
A hacker steals a company's product designs and sells them to a competitor.	c
A cybercriminal creates a fake email that mimics a bank's official communication, tricking users into sharing their login credentials.	g
A man repeatedly sends unwanted, threatening messages to a woman on social media platform.	i
An attacker gains access to the control system of a power grid, disrupting the electricity supply for several hours.	f
A hacker exploits a vulnerability in a bank's online portal to access customer accounts and retrieve personal financial information.	a

CLO #: 3

Question No. 3 [4 × 3 = 12 marks]

Given the following database schema:

Table: Employees

EmployeeID	Name	Department	Salary
1	John Smith	HR	70,000
2	Alice Brown	Finance	85,000
3	Bob Johnson	IT	95,000
4	Sarah White	HR	75,000
5	Kevin Lewis	IT	100,000

Table: Projects

ProjectID	ProjectName	Department
101	Recruitment Drive	HR
102	Annual Report	Finance
103	System Upgrade	IT
104	Security Audit	IT

Table: WorkHours

EmployeeID	ProjectID	HoursWorked
1	101	20
2	102	30
3	103	40
4	101	25
5	103	45

Answer the following questions:

A. Analyze the tables to identify any way in which sensitive information can be inferred indirectly.

- The Employees table contains **salary** information, which is sensitive.
- By combining information from the **WorkHours** and **Projects** tables, one could indirectly infer departmental salaries if correlated with employee work.

B. Identify which type of sensitive information can be inferred indirectly from the given query. Justify your answer with proper arguments.

```
SELECT e.EmployeeID, SUM(w.HoursWorked)
FROM Employees e
JOIN WorkHours w ON e.EmployeeID = w.EmployeeID
JOIN Projects p ON w.ProjectID = p.ProjectID
WHERE p.Department = 'IT'
GROUP BY e.EmployeeID;
```

It could be used to indirectly infer **the total salary of the IT department** using only non-sensitive data. This query could be combined with outside knowledge about hourly rates or payroll information to estimate total salaries.

C. Suggest ways to prevent this type of inference without losing essential functionality for legitimate queries.

- **Data Masking**: Mask or obfuscate sensitive data fields in reports.
- **Query Restrictions**: Implement row-level security or limit user access based on roles.
- **Noise Addition**: Add noise to query results for aggregate data to make precise inference difficult.
- **Auditing**: Track and audit user queries to detect patterns indicative of inference attempts.

CLO #: 4

Question No. 4 [6 + 2 + 4 = 12 marks]

Dr. Kaka Munna, a professor at FAST, uses three Kerberized services, namely FLEX, SLATE and NUMUN on a daily basis whenever he comes to university. Normally he accesses FLEX 10 times a day, SLATE 5 times a day, and NUMUN twice a day. Assuming no power outages and no automatic sign outs:

A. How many times will Dr. Munna interact with the

(i) Authentication server (i.e., the AS)
Once (1)
(ii) Ticket-granting server (i.e., the TGS)
Thrice (3)
(iii) NUMUN server?
Twice (2)

B. In the context of Kerberos, what is the difference between K_{TGS} and $K_{C, TGS}$?

$K_{C, TGS}$ is the session key that is shared between the client and the TGS (ticket granting server). It is generated by the Authentication Server and included in the TGT (ticket granting ticket).

K_{TGS} is the TGS's secret key, it is known only to the TGS and the Kerberos Key Distribution Center (KDC).

C. Dr. Munna says that Kerberos can be

(i) described as a MAC protocol; and
(ii) is effective in protection from eavesdropping.

Would you agree with his statements?

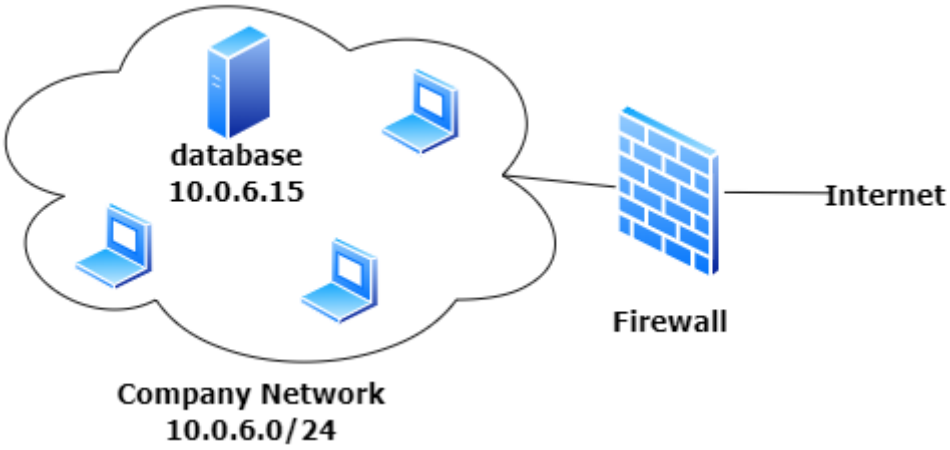
I would agree with his second statement, but not his first.

Since Kerberos can be described as a network authentication protocol, not a MAC protocol. Whereas it does provide protection from eavesdropping and firewall limitations to users and replay attacks.

CLO #: 4

Question No. 5 [8 marks]

Babar works as a junior network administrator at a company. The company's network architecture is shown in the following diagram. A packet filtering firewall serves as the single choke point for all incoming and outgoing traffic.



Babar receive instructions to configure the firewall for the following requirements:

a) allow remote SSH access (port 22) to the database server (rules 1-2).
b) allow the internal users to browse the World Wide Web (rules 3-4).
c) no other traffic should pass through the firewall.

After looking at Babar's configuration, you find that it may contain some errors and security flaws. Identify all of them and suggest a fix.

#	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	ACTION
1	In	External	10.0.6.0/24	TCP	22	≥1024	Permit
2	Out	10.0.6.0/24	External	TCP	≥1024	22	Permit
3	Out	10.0.6.0/24	External	TCP	≥1024	any	Permit
4	In	External	10.0.6.0/24	TCP	any	≥1024	Permit
5	Either	any	any	any	any	any	Permit

Rule 1 dest and rule 2 src address is incorrect – instead of whole subnet, we should allow access to only the database server 10.0.6.15. Furthermore, the src/dest port numbers should be swapped. For incoming packet, dest port will be 22.

Rules 3-4 should use port 80 for web instead of 'any'.

Rule 5: default rule must have a Block action.

CLO #: 5

Question No. 6 [3 + 5 = 8 marks]

A. What role do professional associations play in maintaining ethical conduct in IT and Cybersecurity professionals?

Professional associations publish their codes of ethics as a **set of guidelines** that members are expected to follow. They can **organize trainings/workshops** and **provide resources** to enhance ethical knowledge and decision-making skills. They can also **revoke certifications** or membership when someone is found to be involved in unethical behavior.

B. Deterrence against illegal and unethical behavior works only if three conditions are met. List those conditions. Moreover, specify which condition can be enforced using technical controls?

Conditions: Fear of penalty, Probability of being apprehended, Probability of penalty being applied.

Second condition (probability of being apprehended) can be enforced using technical controls such as logging and monitoring systems to track user activities. Using such controls, the user involved in illegal behaviour can be easily identified and apprehended.

CLO #: 4

Question No. 7 [5 + 2 + 2 = 9 marks]

HBL's online banking website secures all transactions using SSL/TLS. However, a customer reports a problem where the browser produces an error message that indicates "Cannot establish a secure connection." Upon further analysis, the IT team identifies that the SSL handshake fails because the cipher suite chosen by the server is not supported by the browser.

1. Explain the phases of the SSL handshake process and where this might be failing in the scenario.
    a. **Client Hello**: Client will share supported protocols, cipher suites, and send a random number.
    b. **Server Hello**: Server will select and send the protocol and cipher suite, its certificate and provides a random number.
    c. **Key Exchange**: Pre-master secret will be generated using RSA or DH and a symmetric session key is derived.
    d. **Session Established**: Both server & client will agree on a session key and start encrypted communication.
    e. **Possible Failure Point**: The handshake failed if the server's chosen cipher suite will be unsupported by the client machine.

2. What steps must the bank's IT team undertake for solving the compatibility issue and keeping security intact?

Configure the server settings to include commonly used secure cipher suites as well as intimate the client users to update browsers to support modern TLS protocols like TLS 1.3.

3. Suggest an updated SSL/TLS configuration to prevent similar issues in the future.

Only enable secure cipher suits like TLS 1.3. regularly verify and update server & client software to support latest secure cipher suites.

CLO #: 1

Question No. 8 [5+5 = 10 marks]

This problem explores the use of a one-time pad version of the **Vigenère cipher**. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 ..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

a. Encrypt the plaintext "**sendmoremoney**" with the key stream

9 0 1 7 23 15 21 14 11 11 2 8 9

s	e	n	d	m	o	r	e	m	o	n	e	y
18	4	13	3	12	14	17	4	12	14	13	4	24
9	0	1	7	23	15	21	14	11	11	2	8	9
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H

b. Using the ciphertext produced in **Part (a)**, find a **key** so that the cipher text decrypts to the plaintext "**cashnotneeded**".

c	a	s	h	n	o	t	n	e	e	d	e	d
2	0	18	7	13	14	19	13	4	4	3	4	3
25	4	22	3	22	15	19	5	19	21	12	8	4