National University of Computer and Emerging Sciences, Lahore Campus

Course Name:	Information Security	Course Code:	CS3002
Degree Program:	BS (CS)	Semester:	Fall 2022
Exam Duration:	60 mins	Total Marks:	30
Paper Date:	10/11/22	Weight:	12.5
Exam Type:	Mid II	Page(s):	4

Student : Name:_____________________________ Roll No.________________ Section:_______

Instruction: If you think some information is missing then make assumption and write it clearly.

Question 1: MCQs **[5 Marks] [CLO 1]**

1.1 If a file is infected by ________ malware, its total size remains the same as it was before infection.

A. pre-pending
B. appending
C. multi-cavity
D. None of the above

1.2 Hard-coded credentials in an IoT device is an example of _________ vulnerability.

A. hardware
B. firmware
C. communication
D. radio

1.3 ____________ is an attack that injects code in one or more conditional statements so that they always evaluate to true.

A. Piggybacked
B. Tautology
C. cascading
D. none of the above

1.4 Which one of the following is NOT a valid advantage of IPsec?

A. It can be implemented on routers.
B. It is transparent to end users.
C. It can selectively encrypt HTTP traffic.
D. It allows to choose one or both, encryption and authentication.

1.5 An attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder is called _________.

A. Anomaly based detection
B. Signature based detection
C. Specification based detection
D. None of the above

Question 2: **[3+4+4 marks] [CLO 2]**

a) Biometric authentication sounds like a very reliable security measure. Despite that, it is not used everywhere. Discuss three reasons why.

- It involves extra cost for sensor hardware.
- Biometric data is never exactly matched, instead a scoring system is used. As a result, false acceptances and false rejections happen in some cases.
- All biological characteristics are variable (due to wound, aging, emotion etc.). Hence biometric verification will fail in such cases.
- It makes anonymous access impossible.

b) Suppose an app is heavily used at your workplace. The app was written a long time ago in C language. Unfortunately the app source code was lost due to a hard disk failure. Your boss is concerned about some buffer overflow vulnerabilities that may exist in the app. What (technical) actions would you recommend to prevent buffer overflow exploits?

Run time defenses should be applied, like non executable address space, address space randomization, guard pages etc. (Briefly explain all three).

Compile time defenses are not an option since source code is not available.

c) In the context of IoT security, discuss two examples for each of the following types of attacks:

Physical attacks:

Sleep deprivation: Preventing a node from going to idle sleep mode so that its battery is quickly drained.

Node tampering: Physically modifying the node hardware, e.g. to disable communication, to input fake sensor data etc.

Network attacks:

Traffic analysis: Recording and analyzing the wirelessly transmitted packets.

Sinkhole attack: Malicious routing node advertising incorrect routes and attracting all traffic to itself.

Question 3: **[2+6 marks] [CLO 3]**

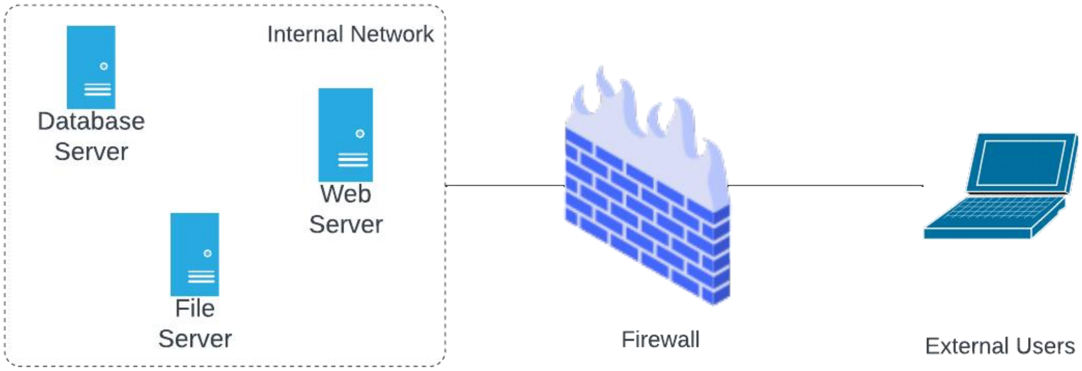
a) What is a packet-filtering firewall? What are its pros and cons?

A firewall that allows or drops the packets according to on pre-defined rules of checking layer 3 and layer 4 headers.

Pros: It is fast and simple in operation. Transparent to end users.

Cons: Can't protect against IP spoofing attacks, can't analyze packet contents to see if they are malicious etc.

b) Configure the following packet-filtering firewall at network layer by filling in the table below such that only the Web server is accessible to external users.



#	Direction	Source	Destination	Protocol	Src Port	Dst Port	Action
1	In	External	Web server	TCP	Any (or >1023)	80	Allow
2	Out	Web server	Extrernal	TCP	80	Any (or >1023)	Allow
	Either	Any	Any	Any	Any	Any	Drop

Question 4: **[4+3] [CLO 2]**

a) Consider a university database where all students' assessment marks are stored in one giant table:

Marks (<u>StudentID</u>, <u>CourseID</u>, Assignment, Quiz, Mid, Project, Final, Total)

Now suppose this table is encrypted at the field level (i.e. every piece of data is individually encrypted). Analyze the following queries and argue whether these can be executed quickly or slowly on the encrypted database.

SELECT StudentID, Assignment FROM Marks WHERE CourseID='CS1004' AND Assignment < 50;

SELECT Total FROM Marks WHERE StudentID=254 AND CourseID='CS3002';

1st query will be slower because the filter Assignment < 50 cannot be applied on encrypted fields. Whole Marks table (or at the very least, the complete Assignment column) should be downloaded and decrypted at the client side before filtering out correct rows.

2nd query can be quickly executed by encrypting the params 254 and CS3002 at the client side, and then running the query on server-side encrypted database, that will easily match the single row containing encrypted values of 254 and CS3002.

[Note: only the client has got encryption/decryption keys, not the server. Refer to Lec 17 slides 40 onwards]

b) What is the concept of Perturbation? What are the different types of perturbation?

Adding noise to the results of a database query. It is applied on statistical databases as a protection against inference attacks.

<u>Some types</u>

Data perturbation: swapping data between rows

Random sample query: run the query on a selected subset of rows.

Statistic adjustment: Adjust the statistical answers up or down by a small amount.