Kingdom of Saudi Arabia
Ministry of Education
Imam Mohammed bin Saud Islamic University
Applied College
Cybersecurity program
Cybersecurity Design Principles (CYB0103)

Midterm

Name:……. ID:……. Section#: …….

Q1: Choose the correct answer: 5 points

#	1	2	3	4	5	6	7	8	9	10
Answer										

1) A _____ describes the system, e.g., a high-level specification or an abstract machine description of what the system does:

A) Model.
B) Security Policy.
C) Security Model.
D) Verification.

2) A _____ defines the security requirements for a given system:

A) Model.
B) Security Policy.
C) Security Model.
D) Verification.

3) _____ techniques that can be used to show that a policy is satisfied by a system:

A) Model.
B) Security Policy.
C) Security Model.
D) Verification.

4) System Model + Security Policy = _____:

A) Model.
B) Security Policy.
C) Security Model.
D) Verification.

5) The Biba model focuses on:

A) Confidentiality.
B) Integrity.
C) Availability.
D) Traceability.

6) The Bell-LaPadula (BLP) model focuses on:

A) Confidentiality.
B) Integrity.
C) Availability.
D) Traceability.

7) A potential cause of an unwanted incident which may result in harm to a system or organization:

A) Asset.
B) Threat.
C) Vulnerability.
D) Risk.

All the best

Kingdom of Saudi Arabia
Ministry of Education
Imam Mohammed bin Saud Islamic University
Applied College
Cybersecurity program
Cybersecurity Design Principles (CYB0103)

8) A weakness in an asset or group of assets which can be exploited by a threat:

A) Asset.
B) Threat.
C) Vulnerability.
D) Risk.

9) The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets:

A) Asset.
B) Threat.
C) Vulnerability.
D) Risk.

10) Anything that has value to the organization:

A) Asset.
B) Threat.
C) Vulnerability.
D) Risk.

Q2: Match the correct answer from column A to column B: 5 points

#	A	The answer	B
1	No read up, No write down	2	Biba Model
2	No write up, No read down	1	BLP Model
3	Can be implemented via an Access Control List or via a Capabilities List	4	Clarke-Wilson Model
4	Deals with two types of transactions, namely Integrity verification procedures (IVPs) and transaction procedures (TPs).	3	HRU Model
5	Top Secret > Secret > Confidential > Unclassified	6	The Chinese Wall Model
6	Focused on conflict of interest, once you access the data belonging to one side, the other side's data becomes unavailable or inaccessible.	5	Security levels
7	A data security process that enables organizations to manage who is authorized to access corporate data and resources.	7	Access Control

All the best

Kingdom of Saudi Arabia
Ministry of Education
Imam Mohammed bin Saud Islamic University
Applied College
Cybersecurity program
Cybersecurity Design Principles (CYB0103)

Q3: Put (T) for correct sentences and (F) for wrong sentences: 5 points

1) Both Clarke-Wilson and Biba models focus on Confidentiality. (**F**)
2) Multi-level Security (MLS) uses Mandatory Access Control (MAC) because Discretionary Access Control (DAC) fails to achieve MLS's goals. (**T**)
3) Both BLP and HRU models focus on Integrity. (**F**)
4) BLP model has no mechanisms for changing access rights or for the creation and deletion of subjects and objects. (**T**)
5) The disadvantage of the Access Control List (ACL) is that it is difficult to determine which subjects are able to access specific objects by looking at the object itself. (**F**)
6) The Constrained Data Items (CDIs) can be manipulated by users via primitive read and write operations. (**F**)
7) Zero Trust assumes that there is a traditional network edge. (**F**)
8) Using design patterns requires extensive knowledge is one of design patterns disadvantages. (**T**)
9) Reusability in countless projects to solve problems with a common pattern is one of design patterns advantages. (**T**)
10) Formal Security Risk Assessment is a less systematic and more intuitive approach to identify, assess and prioritize potential risks e.g. meetings and brainstorming sessions. (**F**)

Commented [R.1]: Integrity

Commented [R.2]: Confidentiality

Commented [R.3]: Capabilities List

Commented [R.4]: Unconstrained Data Items (UDIs)

Commented [R.5]: there is NO traditional

Commented [R.6]: Informal

Q4: Answer the following questions: 5 points

1) List four types of security models.

    1. Bell-LaPadula (BLP) Model.
    2. Biba Model / Biba Integrity Model.
    3. The Harrison–Ruzzo–Ullman Model.
    4. The Clark-Wilson Model.
    5. The Chinese Wall Model.

2) List three components of Access Control.

    1. Authentication.
    2. Authorization.
    3. Access.
    4. Manage.
    5. Audit.

3) List the three stages of Implementing Zero Trust.

    1. Visualize.
    2. Mitigate.
    3. Optimize.

All the best

4) List the three Types of Design Patterns.

1. Creational.
2. Structural.
3. Behavioral.

5) List the four Advantages of Design Patterns.

1. Reusability in countless projects to solve problems with a common pattern.
2. Spend less time figuring out how to solve a particular issue.
3. Spend a safe time on implementing the solution and improve the quality of the software product.
4. Provides more value for money.

All the best