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) _____ is any part of a system that, by itself, provides all or a portion of the total functionality required of a system:

A) Component.
B) Trustworthy.
C) Trust.
D) Simplicity.

2) _____ is the degree to which the security behavior of the component is demonstrably compliant with its stated functionality:

A) Component.
B) Trustworthy.
C) Trust.
D) Simplicity.

3) _____ is the degree to which the user or a component depends on the trustworthiness of another component:

A) Component.
B) Trustworthy.
C) Trust.
D) Simplicity.

4) Which of the following is NOT a benefit of Modular Design:

A) Testing.
B) Reuse.
C) Scalability.
D) Documentation.

5) A good software design will have:

A) High cohesion and low coupling.
B) Low cohesion and high coupling.
C) High cohesion and high coupling.
D) Low cohesion and low coupling.

6) Firewalls, intrusion detection and prevention systems are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

7) _____ include security measures that consist of policies or procedures directed at an organization's employees:

A) Physical controls.
B) Technical controls.
C) Administrative controls.
D) None of the above.

All the best

8) Antivirus, antimalware, and e-mail security solutions are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

9) Virtual private networks (VPNs) are an example of security measures at TWO layers. Which are they:

A) Perimeter and Network.
B) Network and Access.
C) Perimeter and Access.
D) None of the above.

10) Which of the following is NOT an example of Safety measures:

A) Redundancy in critical systems.
B) Fire suppression systems.
C) Regular data backups.
D) Authentication.

11) Which of the following is NOT a Security feature of System Integrity:

A) Physical security.
B) Software key and provisioning.
C) Runtime security.
D) Freedom from interference.

12) The difference between security and functional safety can be summed up in one word:

A) Function.
B) Approach.
C) Intent.
A) Scope.

13) _____ makes vulnerabilities harder for developers and testers to find and fix:

A) Choke Point.
B) Hardening.
C) Minimization.
D) Complexity.

14) Remove or disable code known to create vulnerabilities, like JavaScript and Flash, is one way to apply:

A) Choke Point.
B) Hardening.
C) Minimization.
D) Simplicity.

15) Reduce the number of components used, keeping only those that are essential is one way to apply:

A) Choke Point.
B) Hardening.
C) Minimization.
D) Simplicity.

All the best

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

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

#	A	The answer	B
1	It is the degree to which the elements of the module are functionally related, and every aspect of the module is tied to its single purpose.	**6**	Safety in IT
2	It is the degree with which a component depends on other components in the system.	**7**	Encapsulation
3	It means that all unnecessary services off by default.	**4**	Choke Point
4	It is a centralized piece of code through which control must pass.	**3**	Hardening
5	It focuses on protecting against intentional threats and malicious activities.	**1**	Cohesion
6	It focuses on preventing accidental (i.e., unintentional) harm and damage.	**2**	Coupling
7	It means packaging the information inside a component.	**5**	Security in IT
8	It means reducing the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.	**8**	Minimization

Q3: Answer the following questions: 5 points

1) List the four phases of incident response according to NIST.

   1. The preparation phase.
   2. The detection and analysis phase.
   3. The containment, eradication, and recovery phase.
   4. The post-event activity phase.

2) Defense-in-Depth covers three levels/categories of security controls. List them.

   1. Physical controls.
   2. Technical controls.
   3. Administrative controls.

3) While many new solutions are being introduced to address security issues, they often ignore the problems caused by complexity. List three steps to improve Simplicity in these security solutions.

   1. Evaluate What You Need from Multipurpose Security Suites.
   2. Increase Clarity and Reduce Complexity with Automation.
   3. Intercept Attacks as Quickly as Possible.
   4. Keep designs as simple and small as possible.
   5. Reduce the number of components used, keeping only those that are essential.
   6. To keep software simple and security checks localized, you can take advantage of a concept called a choke point.

All the best

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

4) The goal of Modularization is to have each component / module meet four conditions. List them.

1. single-purpose: performs one function.
2. small: consists of an amount of information small enough in structure and content.
3. simple: is of a low degree of complexity so that a human can readily understand.
4. independent: performs a task isolated from other modules.

5) List three different ways to achieve Minimization.

1. Delete sensitive data when it is no longer needed, and don't store data in the first place if there is no need.
2. Remove unnecessary interfaces and functionality.
3. Remove or disable code known to create vulnerabilities, like JavaScript and Flash.
4. Remove unused code as soon as possible.
5. Give every element in an organization the minimum access needed to do their jobs—this includes nonhumans, such as servers and applications.

Q4: Put (T) for correct sentences and (F) for wrong sentences: 5 points

1) The worst enemy of security is simplicity. (**F**)
2) The more enabled features of a system the more potential exploits and decreased security. (**T**)
3) Modularization is effective to be used for small and large systems. (**F**)
4) Modularization supports security by improving testing and enabling more layers of defense. (**T**)
5) Defense-in-Depth is considered part of Layered Security. (**F**)
6) The layered security is about implementing the same defense multiple times. For example, having McAfee, Norton, and Avast antivirus tools installed on your windows computer. (**F**)
7) The main aim of incident response is to contain the threat, reducing the cost and recovery time associated with handling a breach or cybercriminal attack. (**T**)
8) An organization should only worry about the traffic that comes into its network. (**F**)
9) Easy to follow and maintain program statements is an example of simplicity. (**T**)
10) Automation with Machine Learning increases complexity hence decreases security. (**F**)

Commented [R.1]: complexity

Commented [R.2]: large

Commented [R.3]: Layered Security is considered part of Defense-in-Depth.

Commented [R.4]: is NOT about implementing the same defense multiple times

Commented [R.5]: Organizations should monitor for traffic leaving their perimeters as well.

Commented [R.6]: reduces complexity hence increases security

All the best