CYB0103: Cybersecurity Design Principles
Question Bank

Chapter 1
Prepared by: Rana Al Haj Fakeeh

Part I: multiple choice questions:

1) _____ means keeping things secret that shouldn't be made known to the public:

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

Answer: A

2) _____ means that the information doesn't change or is only allowed to change in specific, authorized ways:

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

Answer: D

3) _____ means data is at hand in a timely manner:

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

Answer: B

4) _____ means the need for knowing who changed or accessed what data when:

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

Answer: C

5) Which one of the following is NOT one of the security concerns:

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

Answer: A

6) What is the Information Security definition:

A) Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
B) It is a broader category that protects all information assets, whether in hard copy or digital form.
C) It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
D) It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

Answer: B

7) What is the Cybersecurity definition:

A) Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
B) It is a broader category that protects all information assets, whether in hard copy or digital form.
C) It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
D) It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

Answer: D

8) What is the Traditional Approach to software security definition:

A) Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
B) It is a broader category that protects all information assets, whether in hard copy or digital form.
C) It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
D) It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

Answer: A

9) What is the Design definition:

A) Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
B) It is a broader category that protects all information assets, whether in hard copy or digital form.
C) It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
D) It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

Answer: C

10) Which one of the following is NOT true about the Design Approach to software security:

A) Design is a natural part of software development.
B) Business concerns and security concerns become of equal priority.
C) Non-security experts can naturally write secure code.
D) Developers should know about things like cross-site scripting (XSS) attacks, be aware of vulnerabilities in low-level protocols, and know the OWASP Top 10 like the backs of their hands.

Answer: D

Part II: true / false questions:

#	Question	Answer
1	The design approach to software security is better than traditional approach.	T
2	The traditional approach considered problematic because it requires every developer to be a security expert.	T
3	Integrity concern captures the need for knowing who changed or accessed what data when.	F
4	Security is a natural part of software development.	F
5	One advantage of design approach is that business concerns and security concerns become of equal priority.	T
6	One advantage of design approach is that non-security experts naturally write secure code.	T
7	A strong design focus lets you create code that's less secure compared to the traditional approach to software security.	F
8	A strong focus on traditional approach lets you create code that's less secure compared to the traditional approach to software security.	T
9	Login Page, Encryption, Firewall, and Antivirus are considered security concerns rather than security features.	F
10	Confidentiality, Integrity, Availability, and Traceability are considered security concerns rather than security features.	T
11	Implementing a login page to an application is enough to meet the information confidentiality concern.	F
12	Even when security features address a specific security problem, your concern about security may not have been met.	T
13	It's better to view security as a feature to implement than to view it as a concern to be met.	F
14	It is easier for developers to achieve security through design because most developers understand and appreciate software design.	T
15	The design approach creates a conflict between security concerns and business concerns for developers.	F

Commented [R.1]: Traceability

Commented [R.2]: Design

Commented [R.3]: more secure

Commented [R.4]: security features rather than security concerns

Commented [R.5]: Even when security features address a specific security problem, your concern about security may not have been met.

Commented [R.6]: It's better to view security as a concern to be met than to view it as a feature to implement.

Commented [R.7]: traditional approach