CYB0103: Cybersecurity Design Principles
Question Bank

Chapter 7
Prepared by: Rana Al Haj Fakeeh

Part I: multiple choice questions:

1) 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.

Answer: D

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

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

Answer: C

3) The goal of both functional safety and security is that system's _____ is preserved in the face of the hazard or threat, no matter whether the source is malicious intent or malfunction. In other words, ensuring the software running has not been altered intentionally or unintentionally:

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

Answer: B

4) 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.

Answer: D

5) Which of the following is NOT a Safety feature of System Integrity:

A) Protection from hardware or software specification errors.
B) Software key and provisioning.
C) Protection from human errors.
D) Freedom from interference.

Answer: B

6) _____ to stop people from causing harm to computers and equipment through the internet:

A) Security.
B) Cybersecurity.
C) Safety.
D) Cybersafety.

Answer: B

7) _____ most often relates to a personal feeling of being free from harm or danger:

A) Security.
B) Cybersecurity.
C) Safety.
D) Cybersafety.

Answer: C

8) _____ often has to do with a group's efforts to protect its members from harm:

A) Security.
B) Cybersecurity.
C) Safety.
D) Cybersafety.

Answer: A

9) _____ describes the effort to stop others from attacking and stealing private information:

A) Security.
B) Cybersecurity.
C) Safety.
D) Cybersafety.

Answer: B

Part II: true / false questions:

#	Question	Answer
1	Security in IT focuses on preventing accidental (i.e., unintentional) harm and damage.	F
2	Safety in IT focuses on protecting against intentional threats and malicious activities.	F
3	The difference between security and functional safety can be summed up in one word – Function.	F
4	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
5	The National Institute of Standards and Technology (NIST) recognizes six lifecycle phases that companies work through once a data breach or cybercriminal attack has been discovered.	F
6	An organization should only worry about the traffic that comes into its network.	F
7	Safety seems to define efforts and measures that are outside of an individual, while security is closer to an inner feeling.	F
8	We would say "cybersafety" when talking about measures to protect the nation's computer systems.	F
9	An increase in the performance of server memory or hard drives is normal and doesn't indicate malicious activity.	F
10	For a company that only operates in one country, any traffic sent to other countries could indicate malicious activity.	T

Commented [R.1]: Safety

Commented [R.2]: Security

Commented [R.3]: Intent

Commented [R.4]: four

Commented [R.5]: should not

Commented [R.6]: Security seems to define efforts and measures that are outside of an individual, while safety is closer to an inner feeling.

Commented [R.7]: would not

Commented [R.8]: may mean

Part III: essay questions:

1) List the security features of system integrity.

- Physical security.
- Software key and provisioning.
- Runtime security.
- Foundation for security.

2) List the safety features of system integrity.

- Protection from systemic and random failures.
- Protection from human errors.
- Protection from hardware or software specification errors.
- Freedom from interference.

3) List the phases of incident response according to NIST.

- The preparation phase.
- The detection and analysis phase
- The containment, eradication, and recovery phase
- The post-event activity phase.

4) List four ways enterprises can detect security incidents.

- Unusual behavior from privileged user accounts.
- Unauthorized insiders trying to access servers and data.
- Anomalies in outbound network traffic.
- Traffic sent to or from unknown locations.
- Excessive consumption.
- Changes in configuration.
- Hidden files.
- Unexpected changes.
- Abnormal browsing behavior.