Cyber Security and Privacy, IIT Madras
Prof. Saji K Mathew

Week 8 Quiz
(All questions carry 1 point each)

1. The Cost-Benefit Analysis (CBA) formula for risk management decisions is given by:

a. CBA = ALE(prior) - ALE(post) – ACS
b. CBA = ALE(prior) - ALE(post) + ACS
c. CBA = ALE(prior) + ALE(post) – ACS
d. CBA = ALE(prior) + ALE(post) + ACS

Ans: a. CBA = ALE(prior) - ALE(post) – ACS
Explanation: ALE =Annualized Loss Expectancy, ACS = Annualized Cost of a Safeguard

2. In a cost-benefit analysis, _____ is the expected percentage of loss that would occur from a particular attack

a. Single Loss Expectancy
b. Exposure Factor
c. Annualized Loss Expectancy
d. None of the above

Ans: b. Exposure Factor
Explanation: Exposure Factor (EF) is the percentage of value lost by an asset because of an incident.

3. A _____ is a network security device that monitors traffic to or from a network and decides whether to allow or block specific traffic based on a defined set of security rules.

a. Intrusion Detection and Prevention System
b. Router
c. Intrusion Detection System
d. Firewall

Ans: d. Firewall
Explanation: Firewall monitors and filters network traffic based on an organization's security policies.

4. What risk management approach aims to minimize the impact of losses resulting from an actual incident, disaster, or attack by implementing thorough contingency plans and preparations?

a. Mitigation risk control strategy
b. Transference risk control strategy
c. Defense risk control strategy
d. Termination risk control strategy

Ans: a. Mitigation risk control strategy
Explanation: The mitigation risk control strategy aims to decrease the consequences of an attack, rather than focusing on diminishing the likelihood of the attack itself.

5. The product of the asset's value and the exposure factor is known as:

a. Single Loss Expectancy
b. Annualized Loss Expectancy (Prior)
c. Annualized Rate of Occurrence
d. Annualized Loss Expectancy (Post)

Ans: a. Single Loss Expectancy
Explanation: SLE is the calculated value associated with the most likely loss from an attack.

6. Which of the following is not true?
a.Bit Stream ciphers encrypt data one bit at a time, while block ciphers encrypt data in fixed-size blocks.
b.Bit Stream Cipher is used for Data in Transit Encryption, whereas Block Cipher is used for Data at Rest Encryption
c.Bit Stream Cipher can operate as a Block CIpher but Block Cipher cannot operate as a Bit Stream Cipher
b.Bit Stream ciphers are generally considered faster than block ciphers.

Ans: c.Bit Stream Cipher can operate as a Block CIpher but Block Cipher cannot operate as a Bit Stream Cipher
Explanation : Block Cipher can operate as a Bit Stream CIpher but Bit Stream Cipher cannot operate as a Block Cipher

7.The False Acceptance Rate (FAR) in biometrics refers to:
a.The system mistakenly accepting an unauthorized user.
b.The system correctly rejecting an unauthorized user.
c. The time it takes for a system to identify a user.
d.The user's frustration with the authentication process.

Ans: a.The system mistakenly accepting an unauthorized user.
Explanation : FAR measures the risk of unauthorized access due to the system mistakenly accepting someone who shouldn't be allowed.

8. The IAAA framework in the context of access control stands for?
a.Isolation, Authentication, Authorization, Availability
b.Identification, Authentication, Authorization, Accountability
c.Inspection, Authentication, Access, Authorization
d.Intrusion Detection, Analysis, Authorization, Administration

Ans: b.Identification, Authentication, Authorization, Accountability
Explanation : IAAA defines key steps in access control: Identifying users, verifying their credentials (authentication), granting appropriate access permissions (authorization), and holding them accountable for their actions.

9. What is a significant challenge associated with symmetric key encryption?

a.Slower encryption and decryption compared to asymmetric methods.
b.Limited compatibility with modern encryption algorithms.
c.Higher computational cost for key generation.
d.Key management: securely distributing and safeguarding the shared key.

Ans: d.Key management: securely distributing and safeguarding the shared key.
Explanation: In symmetric encryption, compromising the shared key compromises all communication. Securely distributing and managing this key can be difficult, especially as the number of communicating parties increases.

10.In risk management, which equation is used to calculate the expected loss per risk?

a. Single Loss Expectancy (SLE) = Asset Value × Exposure Factor (EF)
b. Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO)
c. Asset Value = Single Loss Expectancy (SLE) × Exposure Factor (EF)
d. Annualized Rate of Occurrence (ARO) = Asset Value × Single Loss Expectancy (SLE)

Ans: b.Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO)
Explanation:The equation for calculating the expected loss per risk in risk management is expressed as the Annualized Loss Expectancy (ALE) equals the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO).