

Quiz - An Architect's perspective on attack classifications

1. Which of the following statements is True?

1/1 p

- ☐ Passive attacks are easy to detect because of the latency created by the interception and second forwarding.
- ☒ Passive attacks are hard to detect because the original message is delivered unchanged and can pass an integrity check.
- ☐ Passive attacks are easy to detect because the original message wrapper must be modified by the attacker before it is forwarded on to the intended recipient.
- ☐ Passive attacks are hard to detect because the original message is never delivered so the receiving does not know they missed anything.

✓ Correct
Correct

2. The purpose of security services includes which three (3) of the following?

1 / 1 point

☒ Are intended to counter security attacks.

✓ Correct

Partially Correct

☒ Often replicate functions found in physical documents

✓ Correct

Partially Correct

☒ Enhance security of data processing systems and information transfer.

✓ Correct

Partially Correct

☐ Includes any component of your security infrastructure that has been outsourced to a third-party

3. Which statement best describes access control?

1 / 1 point

- ☐ Protection against denial by one of the parties in communication
- ☒ Prevention of unauthorized use of a resource
- ☐ Assurance that the communicating entity is the one claimed
- ☐ Protection against the unauthorized disclosure of data

✓ Correct

Correct

4. The International Telecommunication Union (ITU) X.800 standard addresses which three (3) of the following topics?

1 / 1 point

☒ Data Confidentiality

✓ Correct

Partially correct! It addresses the protection of data from unauthorized disclosure.

☐ Transmission cost sharing between member countries

☒ Access Control

✓ Correct

Partially correct! It addresses protecting data from unauthorized access.

☒ Authentication

✓ Correct

Partially correct! Both peer-entity and data origin authentication.

☐ Data transmission speeds

5. Protocol suppression, ID and authentication are examples of which?

1 / 1 point

- ☐ Business Policy
- ☐ Security Policy
- ☐ Security Architecture
- ☒ Security Mechanism

✓ Correct

Correct! These are the technical implementation of the Security Policy

6. The motivation for more security in open systems is driven by which three (3) of the following factors?

1 / 1 point

- ☒ Society's increasing dependance on computers.

✓ Correct

Partially correct! Especially those that are connected to the Internet.

- ☒ The appearance of data protection legislation in several countries.

✓ Correct

Partially correct! Think GDPR.

- ☐ New requirements from the WTO, World Trade Organization

- ☒ The desire by a number of organizations to use OSI recommendations.

✓ Correct

Partially correct! The spread of OSI recommendations brings with it the need for enhanced security.

7. True or False: The accidental disclosure of confidential data by an employee is considered a legitimate organizational threat.

1 / 1 point

☒ True

☐ False

✓ Correct

Correct! Not all threats are intentional

8. True or False: The accidental disclosure of confidential information by an employee is considered an attack.

1 / 1 point

☒ False

☐ True

✓ Correct

Correct. An attack has to be an intentional attempt to violate security.

Shafayet Bhuiyan

7. True or False: The accidental disclosure of confidential data by an employee is considered a legitimate organizational threat.

1 / 1 point

- ☒ True
☐ False

✓ Correct

Correct! Not all threats are intentional

8. True or False: The accidental disclosure of confidential information by an employee is considered an attack.

1 / 1 point

- ☒ False
☐ True

✓ Correct

Correct. An attack has to be an intentional attempt to violate security.

9. A replay attack and a denial of service attack are examples of which?

1 / 1 point

- ☐ Origin attack
☐ Masquerade attack
☒ Security architecture attack
☐ Passive attack

✓ Correct

Correct! These are both attacks against the security architecture itself.

Shafayet Bhuiyan