QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

SOA

S90.19A

Advanced SOA Security

QUESTION: 72
Service A is a Web service with an implementation that uses managed code. To perform a graphics-related operation, this managed code needs to access a graphics function that exist as unmanaged code. A malicious service consumer sends a message to Service A containing a very large numeric value. This value is forwarded by Service A' s logic to the graphics function. As a result, the service crashes and becomes unavailable. The service consumer successfully executed which attack?

A. Buffer overrun attack
B. Exception generation attack
C. XML parser attack
D. None of the above

Answer: A

QUESTION: 73
Service A retrieves data from third-party services that reside outside the organizational boundary. The quality of the data provided by these third-party services is not guaranteed. Service A contains exception shielding logic that checks all outgoing messages. It is discovered that service consumers are still sometimes receiving malicious content from Service A. Because digital signatures are being used, it is confirmed that Service A is, in fact, the sender of these messages and that the messages are not being altered by any intermediaries. Why do messages from Service A continue to contain malicious content?

A. Messages received from third-party services are the likely source of the malicious content.
B. Digital signatures alone are not sufficient. They need to be used in conjunction with asymmetric encryption in order to ensure that no intermediary can alter messages.
C. Exception shielding logic needs to be used in conjunction with asymmetric encryption in order to guarantee that malicious content is not spread to service consumers.
D. None of the above.

Answer: A

QUESTION: 74

When applying the Exception Shielding pattern, which of the following are valid options for implementing exception shielding logic?

A. as part of the core service logic
B. within a service agent
C. within a utility service
D. All of the above.

Answer: D

QUESTION: 75
A malicious passive intermediary intercepts messages sent between two services. Which of the following is the primary security concern raised by this situation?

A. The integrity of the message can be affected.
B. The confidentiality of the message can be affected.
C. The reliability of the message can be affected.
D. The availability of the message can be affected.

Answer: B

QUESTION: 76
Designing security policies with _____ is an extension of the _____SOA characteristic that supports interoperability and avoids_____.

A. industry standards, business-driven, vendor lock-out
B. industry standards, vendor-neutral, vendor lock-in
C. design standards, composition-centric, vendor lock-in
D. design standards, enterprise-centric, vendor lock-in

Answer: B

QUESTION: 77
The application of the Trusted Subsystem pattern can help centralize access to services.

A. True
B. False

Answer: A

QUESTION: 78
A service protected from an XML bomb attack will automatically also be protected from a schema poisoning attack.

A. True
B. False

Answer: B

QUESTION: 79
A service receives a message containing an XML document that expands to a very large size as it is processed by the parser. As a result, the service becomes unavailable to service consumers. The service was subjected to which type of attack?

A. XML parser attack
B. Exception generationattack
C. XPath injection attack
D. None of the above.

Answer: A

QUESTION: 80
An attacker is able to gain access to a service and invokes the service. Upon executing the service logic, the attacker is able to gain access to underlying service resources, including a private database. The attacker proceeds to delete data from the database. The attacker has successfully executed which type of attack?

A. exception generation attack
B. insufficient authorization attack
C. denial of service attack
D. None of the above.

Answer: B

QUESTION: 81
The application of the Trusted Subsystem pattern directly supports the goals of the Service Loose Coupling principle.

A. True
B. False

Answer: A

QUESTION: 82
Service A is only authorized to access one service capability of Service B. Service B acts as a trusted subsystem for several underlying resources which it accesses using its own set of credentials. Service B can therefore not become a victim of an insufficient authorization attack initiated by Service A.

A. True
B. False

Answer: B

QUESTION: 83
The use of derived keys is based on symmetric encryption. This is similar to asymmetric encryption because different keys can be derived from a session key and used separately for encryption and decryption.

A. True
B. False

Answer: B