SOA S90-19A

Advanced SOA Security

Version: 4.0

QUESTION NO: 1

Which of the following types of attack always affect the availability of a service?

A. Exception generation attack
B. SQL injection attack
C. XPath injection attack
D. None of the above

Answer: D
Explanation:

QUESTION NO: 2

The use of XML schemas for data validation helps avoid several types of data-centric threats.

A. True
B. False

Answer: A
Explanation:

QUESTION NO: 3

The use of session keys and symmetric cryptography results in:

A. Increased performance degradation
B. Increased reliability degradation
C. Reduced message sizes
D. None of the above

Answer: D
Explanation:

QUESTION NO: 4

An alternative to using a _____ is to use a _____.

A. Public key, private key
B. Digital signature, symmetric key
C. Public key, key agreement security session
D. Digital signature, asymmetric key

Answer: C
Explanation:

QUESTION NO: 5

Service A's logic has been implemented using managed code. An attacker sends an XML bomb to Service A. As a result, Service A's memory consumption started increasing at an alarming rate and then decreased back to normal. The service was not affected by this attack and quickly recovered. Which of the following attacks were potentially avoided?

A. XML parser attack
B. Buffer overrun attack
C. Insufficient authorization attack
D. Denial of service

Answer: A,D
Explanation:

QUESTION NO: 6

When designing XML schemas to avoid data-centric threats, which of the following are valid considerations?

A. The maxOccurs attribute needs to be specified using a restrictive value.
B. The <xsd:any> element needs to be avoided.
C. The <xsd:restriction> element can be used to create more restrictive user-defined simple types.
D. All of the above.

Answer: B,D
Explanation:

QUESTION NO: 7

_____ is an industry standard that describes mechanisms for issuing, validating, renewing

and cancelling security tokens.

A. WS-Security
B. WS-Trust
C. WS-SecureConversation
D. WS-SecurityPolicy

Answer: B
Explanation:

QUESTION NO: 8

Security policies defined using WS-SecurityPolicy can be used to convey which of the following requirements to a service consumer?

A. Whether transport-layer or message-layer security needs to be used
B. The encryption type that needs to be used for transport-layer security
C. The algorithms that need to be used for cryptographic operations
D. The type of security token that must be used

Answer: A,C,D
Explanation:

QUESTION NO: 9

Service A needs to be designed so that it supports message integrity and so that only part of the messages exchanged by the service are encrypted. You are asked to create the security policy for this service. What type of policy assertions should you use?

A. Token assertions
B. Protection assertions
C. Security binding assertions
D. Service A's security requirements cannot be expressed in a policy

Answer: B
Explanation:

QUESTION NO: 10

How can the use of pre-compiled XPath expressions help avoid attacks?

A. Pre-compiled XPath expressions execute faster and therefore help avoid denial of service attacks.
B. Pre-compiled XPath expressions reduce the chance of missing escape characters, which helps avoid XPath injection attacks
C. Pre-compiled XPath expressions contain no white space, which helps avoid buffer overrun attacks
D. They can't because XPath expressions cannot be pre-compiled

Answer: B
Explanation:

QUESTION NO: 11

The Service Perimeter Guard pattern has been applied to help avoid denial of service attacks for a service inventory. As a result, services within the service inventory are only accessible via a perimeter service However, denial of service attacks continue to succeed and services within the service inventory become unavailable to external service consumers. What is the likely cause of this?

A. The application of the Service Perimeter Guard pattern needs to be combined with the application of the Message Screening pattern in order to mitigate denial of service attacks.
B. The perimeter service itself is the victim of denial of service attacks. As a result, none of the services inside the service inventory can be accessed by external service consumers.
C. The Trusted Subsystem pattern should have been applied so that each service has a dedicated trusted subsystem.
D. The Service Perimeter Guard pattern does not help avoid denial of service attacks.

Answer: B
Explanation:

QUESTION NO: 12

The application of the Service Loose Coupling principle does not relate to the use of security policies as part of service contracts.

A. True
B. False

Answer: B

Explanation:

QUESTION NO: 13

Service A has recently been the victim of XPath injection attacks. Messages sent between Service A and Service C have traditionally been protected via transport-layer security. A redesign of the service composition architecture introduces Service B, which is positioned as an intermediary service between Service A and Service C. The Message Screening pattern was applied to the design of Service B. As part of the new service composition architecture, transport-layer security is replaced with message-layer security for all services, but Service A and Service C continue to share the same encryption key. After the new service composition goes live, Service A continues to be subjected to XPath injection attacks. What is the reason for this?

A. The message screening logic can only work for Service C. Therefore, Service A is not protected.
B. Because message-layer security is being used, it is not possible for the message screening logic in Service B to inspect messages without having the encryption key that is shared by Service A and Service C.
C. XPath injection attacks are not prevented by message screening logic or message-layer security.
D. None of the above.

Answer: B

Explanation:

QUESTION NO: 14

Which of the following can directly contribute to making a service composition architecture more vulnerable to attacks?

A. Reliance on intermediaries
B. Reliance on transport-layer security
C. Reliance on open networks
D. All of the above

Answer: D

Explanation: