S90-19A Q&As

Advanced SOA Security

Pass SOA S90-19A Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/s90-19a.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SOA Official Exam Center

QUESTION 1

The application of the Message Screening pattern can help avoid which of the following attacks?

A. Buffer overrun attack

B. XPath injection attack

C. SQL injection attack

D. Insufficient authorization attack

Correct Answer: ABC

QUESTION 2

Service A acts as a trusted subsystem for a shared database. The database contains sensitive information and performs strict validation on all incoming data modification requests. In case of any invalid input values, the database throws detailed error messages that are required for debugging purposes and are automatically relayed back to service consumers by Service A. Recently, while going through the access logs of the database, it has been reported that attempts have been made to connect to the database from outside the organization.

What can be done to prevent such attacks while preserving the existing database debugging requirements?

A. The Data Confidentially pattern needs to be applied so that all request and response messages exchanged by Service A are encrypted.

B. The Data Origin Authentication pattern needs to be applied in order to incorporate digital signatures in request and response messages exchanged by Service A.

C. The Service Perimeter Guard pattern needs to be applied in order to centralize access to the database.

D. None of the above.

Correct Answer: D

QUESTION 3

A service uses specialized screening logic that compares the size of a message against a maximum allowable size value. This value is specified for an incoming request message for a specific service capability. Upon a mismatch, the service rejects the request message and instead generates an error message.

What type of attack has this security architecture not addressed?

A. XML parser attack

B. Buffer overrun attack

C. Exception shielding attack

D. None of the above

Correct Answer: D

QUESTION 4

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

A. True

B. False

Correct Answer: A

QUESTION 5

An IT enterprise has three domain service inventories that map to three different departments. Each service inventory uses a security token service (STS) based authentication broker to enable single sign-on for services within the respective service inventory boundary. The tokens used for all single sign-on mechanisms are based on SAML assertions. You are given a new requirement to extend this security architecture so that services from different domain service inventories can communicate.

What new security mechanisms are required to fulfill this requirement?

A. The individual authentication brokers need to be replaced with one single authentication broker so that one single token can be used by services across all domain service inventories.

B. An additional authentication broker needs to be added in between each domain service inventory in order to enable communication between services using disparate security tokens.

C. There is no need to introduce a new security mechanism. The individual domain service inventories need to be combined into a single enterprise service inventory. That way, the Service Perimeter Guard pattern can be applied so that services won\\'t need to authenticate each other.

D. There is no need to introduce a new security mechanism. The existing SAML tokens can be used by services across the domain service inventories as long as the existing authentication brokers are configured to issue service inventory-specific assertions for SAML tokens from specific domain service inventories.

Correct Answer: D

QUESTION 6

Service A is a Web service that accesses the Student table in a shared database in order to store XML-based student records. When invoked, the GetStudent operation of Service A uses a StudentID value to retrieve the record of a single student by executing an XPath query. An attacker sends a malicious message that manipulates the XPath query to return all the student records.

Which of the following attacks was carried out?

A. XML parser attack

B. SQL injection attack

C. XPath injection attack

D. None of the above

Correct Answer: C

QUESTION 7

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 element needs to be avoided.

C. The element can be used to create more restrictive user-defined simple types.

D. All of the above.

Correct Answer: BD

QUESTION 8

The difference between the Exception Shielding and Message Screening patterns is in how the core service logic processes incoming messages received by malicious service consumers?

A. True

B. False

Correct Answer: B

QUESTION 9

Service A contains reporting logic that collects statistical data from different sources in order to produce a report document. One of the sources is a Web service that exists outside of the organizational boundary. Some of Service A\\'s service consumers are encountering slow response times and periods of unavailability when invoking Service A. While investigating the cause, it has been discovered that some of the messages received from the external Web service contain excessive data and links to files (that are not XML schemas or policies).

What can be done to address this issue?

A. define cardinality in message schemas

B. correlate request and response messages across different services

C. use precompiled XPath expressions

D. avoid downloading XML schemas at runtime

Correct Answer: AD

QUESTION 10

Within a certain service activity, two services are using certificates in order to guarantee the integrity of messages. With every message exchange, certificates are sent and received. These certificates are checked against an external Certificate Authority (CA) in order to verify whether or not they have been revoked. The current security architecture is suffering from increased latency resulting from the extra communication required with the CA.

How can this problem be addressed without compromising message integrity?

A. WS-Trust based SAML tokens can be used via an authentication broker.

B. WS-SecureConversation security context tokens can be used together with session keys and symmetric cryptography.

C. The security architecture can be redesigned so that the CA is only accessed for the first message exchange.

D. None of the above

Correct Answer: A

QUESTION 11

Which of the following statements is true?

A. When the maxOccurs attribute in an XML schema element is not specified it creates a security risk because attackers can specify this element multiple times.

B. When numeric ranges within an XML schema are not specified it creates a security risk because attackers can introduce very large numeric values within the message data.

C. When the xsd:any element is used within an XML schema it can introduce a security risk because it allows attackers to extend the schema.

D. All of above.

Correct Answer: D

QUESTION 12

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

Correct Answer: B

QUESTION 13

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.

Correct Answer: B

QUESTION 14

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

Correct Answer: ACD

QUESTION 15

The Exception Shielding pattern was applied to the design of Service A. During testing, it is revealed that Service A is disclosing sensitive error information in one of its response messages.

How is this possible?

A. It is the Message Screening pattern, not the Exception Shielding pattern, that prevents a service from transmitting sensitive error information in response messages.

B. The Trusted Subsystem pattern has already been applied to Service A, thereby conflicting with the application of the Exception Shielding pattern.

C. The Exception Shielding pattern states that, in case of an error, the service should not send back any message at all, because this would implicitly tell the service consumer that something has gone wrong, thereby exposing vulnerabilities.

D. None of the above.

Correct Answer: D