Free Questions for S90.19 by certsinside

Shared by Mills on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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 2

Question Type: MultipleChoice

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

Options:

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 3

Question Type: MultipleChoice

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?

Options:

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 4

Question Type: **MultipleChoice**

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?

Options:

A- Buffer overrun attack

B- Exception generation attack

C- XML parser attack

D- None of the above

Answer:

A

Question 5

Question Type: MultipleChoice

Service A is an agnostic service that is part of a complex service composition that relies on the use of several intermediaries for message routing purposes. Due to a recent malicious intermediary attack, public key cryptography and digital signatures have been added to Service A . Subsequently, the attacks stop. However, legitimate service consumers are experiencing latency when interacting

with services from this complex service composition. Following an investigation, it is discovered that Service A has increased its system resource consumption in order to perform its new security-related functions. How can you improve Service A's performance without compromising its security requirements and without introducing new security mechanisms?

Options:

A- Use symmetric encryption in combination with the Service Perimeter Guard pattern and SAML tokens.

B- Use key agreement security sessions by deriving different keys from a session key for signing as well as encryption.

C- Use base 64 encoded certificates in order to provide integrity and confidentiality.

D- None of the above.

Answer:

B

Question 6

Question Type: MultipleChoice

A service uses specialized logic to compare the size of a request message to the maximum allowable size that is specified for request messages. Upon a mismatch, the service triggers an error that results in the issuance of a message with detailed error information. What

type of attack does this specialized logic not help protect the service from?

Options:

A- XML parser attack

B- buffer overrun attack

C- exception generation attack

D- XPath injection attack

Answer:

C

Question 7

Question Type: MultipleChoice

Architects have applied the Service Perimeter Guard pattern to a service inventory by adding a perimeter service inside the firewall that receives all incoming request messages and then routes them to the appropriate services. The firewall has been configured to allow any service consumers to send messages to the perimeter service. You are told that this security architecture is flawed. Which of the following statements describes a valid approach for improving the security architecture?

Options:

A- The Trusted Subsystem pattern needs to be applied to the perimeter service so that it can authenticate all incoming requests before forwarding them to services within the service inventory.

B- The perimeter service needs to be outside the firewall and the firewall needs to be configured so that only the perimeter service has access to the services within the service inventory.

C- The described security architecture is not flawed because the Service Perimeter Guard pattern was applied correctly.

D- None of the above.

Answer:

B

Question 8

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

A, D

Question 9

Question Type: MultipleChoice

Architects responsible for a domain service inventory are being asked to make some of their services available to service consumers from outside the organization. However, they are reluctant to do so and consult you to help define a security architecture that will keep all of the existing services within the domain service inventory hidden within a private network. Which of the following is a valid approach for fulfilling this requirement?

Options:

A- Apply the Brokered Authentication pattern to position an authentication broker outside the private network that has been configured to access the internal services via a firewall. The authentication broker becomes the sole contact point for external service consumers.

B- Apply the Service Perimeter Guard pattern in order to position a perimeter service outside the private network that has been configured to access the internal services via a firewall. The perimeter service becomes the sole contact point for external service consumers.

C- Apply the Trusted Subsystem pattern in order to position a service outside the private network that authenticates each incoming request and then uses its own set of credentials to get access to internal services. This service becomes the sole contact point for external service consumers.

D- None of the above.

Answer:

B

Question 10

Question Type: MultipleChoice

The Message Screening pattern can be used to avoid which of the following types of attacks?

Options:

A- buffer overrun attack

B- XPath injection attack

C- SQL injection attack

D- exception generation attack

Answer:

A, B, C