CompTIA

Exam ADR-001

CompTIA Mobile App Security+ Certification Exam (Android Edition)

Version: 6.0

[Total Questions: 102]

Question No : 1

What is the point of using an initialization vector in encryption? (Select TWO).

A. It stops readable patterns from forming
B. It creates randomization
C. It adds geometry to the encryption
D. It is required for any encryption process
E. It removes the need for the public key

Answer: A,B

Question No : 2

Which of the following is a disadvantage of using a static embedded API Key for client authentication to a web service?

A. API Keys require the use of a certificate issued by a commercial Certificate Authority.
B. API Keys are used with asymmetric cryptography, which is slow and can negatively impact the performance of the client application.
C. API Keys cannot be transmitted over HTTPS, so they are open to compromise.
D. API Keys can be discovered and abused by an attacker.

Answer: D

Question No : 3

Which of the following sensitive data items must be protected in transit at all times?

A. Username, password, and session tokens require protection
B. Only the username and session token, as long as the password is hashed using a cryptographically secure hash function
C. Only the password
D. Username and password require protection. Session tokens do not, as they are randomly generated.

Answer: A

Question No : 4

The digital certificate used to sign the production release should be:

A. regenerated for each version of the app.
B. stored inside the app package before deployment.
C. stored in a secure location separate from the passphrase.
D. stored with the source code so all developers can build the app.

Answer: C

Question No : 5

Which of the following attempts to inhibit an application from being trojanized and proliferating?

A. Tamper protection in code.
B. Encrypting config file.
C. Ensure appropriate permissions are deployed to every component.
D. Login credentials delivered over network with HTTPS.

Answer: A

Question No : 6

What is meant by one way function?

A. The input cannot be calculated from the output.
B. The function can only have an integer input.
C. The function can only be called from the parent class.
D. The function has no inputs only outputs.

Answer: A

Question No : 7

As a general best practice when logging application data which of the following is the BEST approach?

A. Log verbosely to the syslog.
B. Log everything so that the security team can figure out what occurred.
C. Log the operationally critical data, while preventing private data from being logged.
D. Log the critical data and quarantine anything sensitive in a separate log file.

Answer: C

Question No : 8

Which of the following must be protected in a symmetric encryption system?

A. The cipher text
B. The key
C. The algorithm
D. The initialization vector

Answer: B

Question No : 9

The filterTouchesWhenObscured property helps protect against which of the following attacks?

A. Tap Jacking
B. Intent Hijacking
C. Screen Bypass
D. Key Logging

Answer: A

Question No : 10

Which statement about native code in apps is TRUE?

A. Native code is faster because it runs as a separate user ID (UID) giving it direct access

to restricted APIs.
B. Native code is run under the same user ID (UID) as the Java app and therefore comes under the same sandbox restrictions.
C. Native code is executed by the kernel with increased privileges and is mainly used for root operations.
D. Native code runs outside the Dalvik VM and therefore is not restricted by the sandbox.

Answer: B

Question No : 11

When storing a PIN used to logon to the app, by applying a cryptographic hash function a developer will:

A. provide plausible deniability.
B. mitigate the salt used with the password.
C. mitigate the location of the encrypted data.
D. mitigate the password from being recovered.

Answer: D

Question No : 12

An attacker intercepts and potentially tampers with communication between two entities without the knowledge of either of the two entities. This BEST describes which of the following attacks?

A. SOCKS proxy attack
B. Man-in-the-middle attack
C. TCP relay attack
D. ARP poisoning attack

Answer: B

Question No : 13

An Intent Sniffing attack is where:

A. a malicious app intercepts network communications to capture Intent traffic.
B. cached Intent messages are read from storage by an attacker.
C. Intent declarations are read from the manifest in order to construct spoof Intents.
D. a malicious app registers to receive public broadcasts in order to intercept data.

Answer: D

Question No : 14

Which of the following mechanisms is MOST commonly used when attempting a privileged operation?

A. A public method interface to private data fields.
B. A private package containing only the privileged instructions.
C. A try/catch/finally block.
D. A security manager directive.

Answer: C

Question No : 15

Why must Android clients perform input validation on data received from publically accessible web service API calls?

A. As the data is being received over the network from public services, it must be treated as untrusted input with potential malicious intent.
B. Publically accessible web service APIs must be accessed using HTTP and not HTTPS, so an attacker could modify the data on the network as it is passed from the server to the Android application.
C. Data frequently becomes corrupted over unreliable cellular networks.
D. JSON objects transmitted by RESTful web services are not structured in the same manner as SOAP objects, so input validation is necessary to prevent one from being parsed as the other and exposing potentially hidden malicious code.

Answer: A

Question No : 16

Why is it important to security to follow defined naming conventions when coding?

A. To enhance the readability of the code and help prevent future developers from introducing flaws
B. To ease text searches using text editors, grep, etc.
C. To avoid namespace collisions with other code
D. So that static code analysis tools can more easily understand the code and detect vulnerabilities

Answer: A

Question No : 17

Session keys are useful because:

A. they temporarily provide a mechanism to maintain the state of user interaction.
B. they are generated on the Android device locally upon startup.
C. there is only one key to generate.
D. they are more secure than public/private keys.

Answer: A

Question No : 18

Which of the following will LEAST likely be detected through source code analysis?

A. Improper certificate validation
B. Buffer overflow vulnerability
C. Improper build process
D. Hardcoded credentials

Answer: C

Question No : 19

How does HTTP Basic Authentication work?