Android Security Essentials

1. By default, all Android applications have no permission to access any protected resource that would have adverse effects on the system or on other applications.

A. True

B. False

Answer(s): A

---

2. It is not necessary that every application installed on an Android device be signed by the developer before being published.

A. True

B. False

Answer(s): B

---

3. If two applications are developed by the same developer, they can share each other's data if they have the same signature and the same android:sharedUserId flag set in their manifest files.

A. True

B. False

Answer(s): A

---

4. Releasing updates of an application into Google Play requires signing it with the same certificate, or else all the previous users will not be notified of the update and eventually are lost.

A. True

B. False

Answer(s): A

---

5. A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).The message is encrypted with the Private key, and can only be decrypted with the Public key.

A. True

B. False

Answer(s): B

---

6. Permission is the right given to an application by Android to allow access to restricted system API (Application Programming Interface) such as Camera, Bluetooth, GPS, etc...

A. True

B. False

Answer(s): A

---

7. During an application run-time, permissions may be enforced at a number of places when calling into the system, starting an activity, sending and receiving broadcasts, accessing and manipulating a content provider, and binding to or starting a service.

A. True

B. False

Answer(s): A

---

8. Any Android application can protect itself by declaring permissions that can be accessed by other applications. This can be achieved using the tag in the activity_main.xml file of the Android applications providing the permission.

A. True

B. False

Answer(s): B

---

9. Content providers can help an application manage access to data stored by it or by other apps. They also provide a way to share data with other apps.

A. True

B. False

Answer(s): A

---

10. Android application developers can create custom permissions that should be labeled properly.

A. True

B. False

Answer(s): A

---

11. Which of the following choices is one of the different levels of permission protection? (Select four)

- [ ] A. Normal
- [ ] B. Dangerous
- [ ] C. Signature
- [ ] D. Sharing

- [ ] E. System

Answer(s): A B C E

---

12. Which of the following Android levels of permissions are granted automatically without the user's approval?

A. Normal Permissions or Level-Zero Permissions.

B. Dangerous Permissions or Level-one Permissions.

C. Signature Permission or Level-two Permissions.

D. Signature and System Permissions or Level-three Permissions.

Answer(s): A

---

13. Which level of permissions is related to READ_CALENDAR, WRITE_CALENDAR, CAMERA, and READ_CONTACTS?

A. Normal Permissions or Level-Zero Permissions.

B. Dangerous Permissions or Level-one Permissions.

C. Signature Permission or Level-two Permissions.

D. Signature and System Permissions or Level-three Permissions.

Answer(s): B

---

14. Permissions required for an application to perform its operations are called application level permissions.
Which are the types of application level permissions a developer can use? (Select two)

- [ ] A. System-defined permissions.

- [ ] B. Application-defined permissions.
- [ ] C. GPS - defined permissions.
- [ ] D. Payment - defined permissions.

Answer(s): A B

---

15. Android uses "Intents" to communicate and send data between different components which make it vulnerable to malicious attacks.
Which of the following choices are component-level Permissions to protect this type of communication? (Select Four)

- [ ] A. Activity
- [ ] B. Service
- [ ] C. Content Provider
- [ ] D. Broadcast Receiver
- [ ] E. Widgets

Answer(s): A B C D

---

16. Any application which would like to receive a message can receive the broadcast.
Which of the following mechanisms can be used to protect broadcasts? (Select two)

- [ ] A. Broadcast receiver decides which broadcast it will receive.
- [ ] B. Broadcast receiver cannot decide which broadcast it will receive.
- [ ] C. Broadcast decides which receiver can receive its broadcast.
- [ ] D. Broadcast receiver does not decide which broadcast it will receive.

Answer(s): A B

---

17. If you are developing more than one application that is signed with the same certificate, and you want these applications to share access to each other's data and run in the same process, you need to give them the same .....

A. user ID (sharedUserId).

B. user name and password.

C. app description.

D. Ad unit I

Answer(s): A

---

18. Which of the following choices represent the flow of states of data within any app? (Select three)

- [ ] A. Stored data
- [ ] B. Data under processing
- [ ] C. Data in transit
- [ ] D. Printed Data

Answer(s): A B C

---

19. If your database contains sensitive information, it is recommended not to store it on external storage. If you want to share the database with other applications, then you have to use a ..... to protect your app's data.

A. Separate Storage

B. Content Provider

C. Shared Folder

D. Internal Storage

Answer(s): B

---

20. Android stores cache files in the filesystem and sandboxes along with the application. Cache files are created under directory .....

A. /data/data//cache/

B. /data/files//cache/

C. /data/personal//cache/

D. /data/cache//cache/

Answer(s): A
