Unit 4 Android App Sec-1

* Current state of Android Application Security :

- Now, Snapdea (slw hai jisse android ka access pr pe milta hai) would try to fool your android device with 12 different exploit.
- Two exploit found vRoot [CVE-2013-6282] and Towel Root [CVE-2014-3153].
- When the rooting of the device was complete the malware would install several other malicious apps.

* Android App Permissions :

° App permissions helps support user privacy by protecting access to the following:

1] Restricted data : such as system state and users contact info.
2] Restricted actions : such as connecting to a paired device and recording audio.

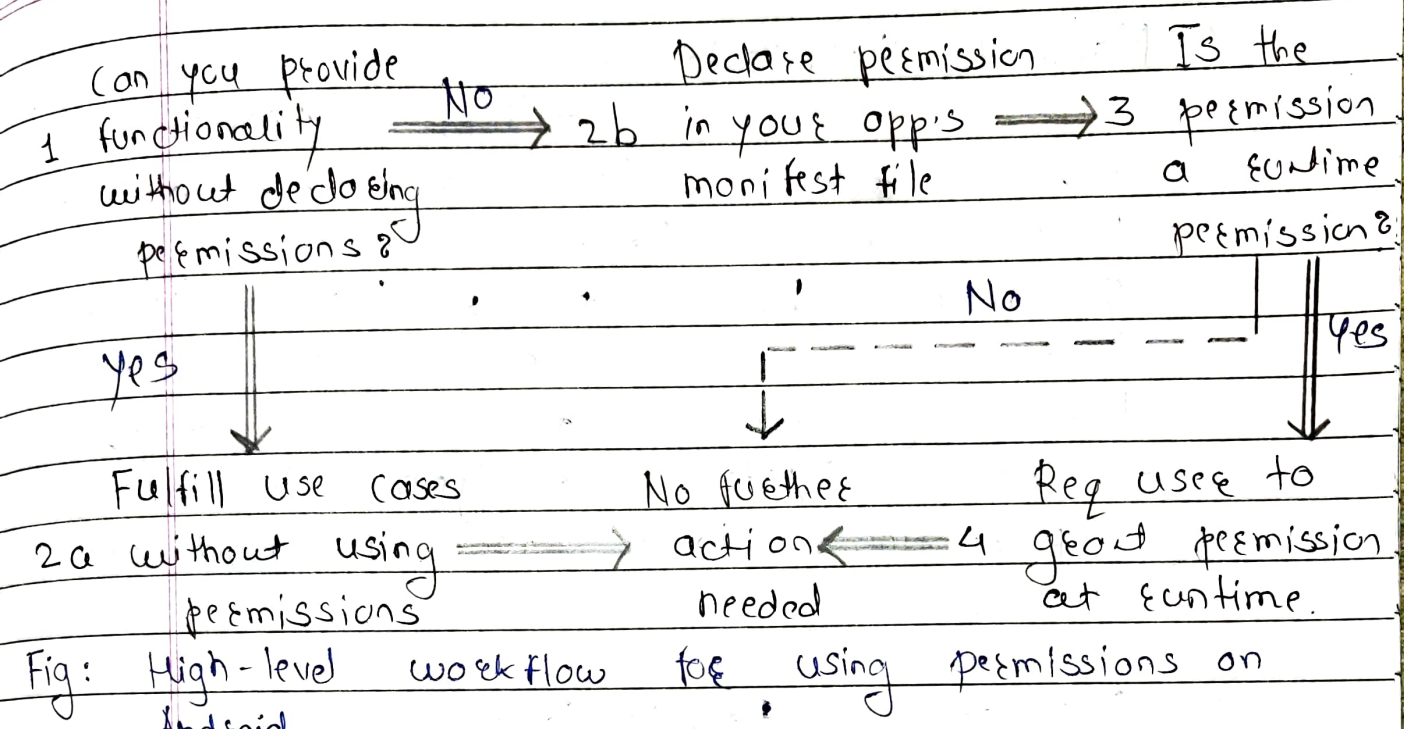


Fig: High-level workflow for using permissions on Android.

* Types of permissions:

- Install-time permissions give your app limited access to restricted data or let your app perform restricted actions that minimally affect the system or other apps.

- Normal Permissions:
  - These permission allow access to data and actions that extend beyond your app's sandbox but present very little risk to the user's privacy and the operation of other apps.
  - The system assigns the normal protection level to normal permissions.

- Signature Permissions:
  - The system grants a signature permission to an app only when the app is signed by the same certificate as the app of the OS that defines the permission.
  - Application that implement privileged services, such as autofill or VPN services, also make use of signature permissions.

- Runtime Permissions:
  - also known as Dangerous Per, give your app additional access to restrict data or let your app perform restricted actions that affect the sys and other apps.

Note: Allow
Allow only this time
Deny
} yee wali hogai 'Runtime Per.'

- Special Permissions:
  - Special per correspond to particular app operations. Only the platform and OEMs (Original Equipment Manufacturer)
  Eg: - Drawing over other apps
  - Accessing all storage
  - Picture - in - picture
  - Install unknown apps
  - The Special App Access page in System Setting contains set of user-toggleable operations. many of these ops are implemented as special permissions.

Note: System settings mai Special App Access mai ye sare options dekhte hai Special Per wale.

- Permission Groups:
  - Permissions are belongs to per Groups.
  - Eg: Per to send and rec SMS might belong to same group, as they both relate to apps interaction with SMS.
  - However, permission can change groups without notice, so don't assume that a particular permission is grouped with any other permission.

* Best Practices to be followed for Security and Privacy for building Android Apps:

App Permissions builds on Sys Security feature and help Android support the following goals related to User Privacy:

1] Control:
The User has control over the data that they share with apps.

2] Transparency:
The User understands what data an app uses and why the app accesses this data.

3] Data Minimization:
An app accessess and uses only the data that's required for a specific task or action that the user invokes.

4] Request a Minimal Number of permission.
When User request a particular action in your app, your app should req only

the permissions that it needs to complete that action.

5] Associate runtime permissions with specific actions :

Connect permissions to particular tasks in your app. Wait as long as you can before asking for permission.
Eg: If your app allows ppl to send voice msg, wait until they click on the button to do so before asking for permission to access the microphone.

6] Consider your app dependencies :

When you include library be aware of the permission that each dependency require and what those per used for

7] Be Transparent :

When you make per request, be clear about what you're accessing why and what functionalities are affected if per is denied, so user can make informed decisions.

8] Make System Access Explicit :

When you access sensitive data or h/w, such as cam or microphone provide indicators of it.

* Basic Android Testing :

* Benefits of Testing :

1] By running test against your app you can verify app correctness.
2] You can verify Functional behaviour and usability before releasing it publically.
3] We can manually test app using devices and emulators.
4] We can also use Automated test that involves tools that perform tests for you.
5] Testing gives us more actionable feedback about your app, earlier in the dev process.

- Functional Testing : does my app do what it is supposed to ?
- Performance Testing : does it do it quickly and efficiently ?
- Accessibility Testing : does it work well with accessibility services ?
- Compatibility Testing : does it work well on every device and API level ?

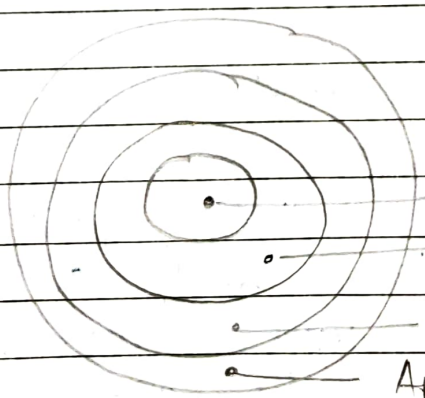
- Unit Test or Small Tests : only verify a very small portion of the app, such as method of class.

- End-to-end test or Big Test verify larger parts of the app at the same time, such as a whole screen or user flow.

- Medium Test are in betwn and check the integration betwn two or more units.

- Instrumented Tests run on an Android device, either physical or emulated. Instrumented tests are usally UI tests, launching an app and then interacting with it.

- Local Tests execute on your development machine or a server, so they are also called host-side tests. They are usally small and fast, isolating the subject under test from the rest of the app.



Date
Page

* Owasp Mobile Top 10 :

M1: Improper Platform Usage.
M2: Insecure Data Storage.
M3: Insecure Communication
M4: Insecure Authentication
M5: Insecure Authorization
M6: Insufficient Cryptography
M7: Client Code Quality
M8: Code Tampering
M9: Rev Engg
M10: Extraneous Functionality.

* Three Ways to Protect your Android Device :

1] Use TLS Enc :

By using TLS you can encrypt internet traffic of all types for securly generating and exchanging session keys.

2] Test Third Party App security

3] Use Caution when using SMS Payments :

Set your Android phone to limit the ability of apps to automatically spend your money. We should avoid payment via sms isko red flag bolte.

Date
Page

* Hacking Android Apps :

- The Three Biggest Threats to Android Devices

1] Threat One : Data in Transit

Mobile devices, including those Android as an OS, are susceptible to man-in-the-middle-attack and various exploits that hacked into unsecure communications over public Wi-Fi network.

- By Hijacking a user's signal, attacker can impersonate web services, steal data, or intercept calls and text messages.

2] Threat Two : Untrustworthy App Stores

Untrustworthy app store can cause headaches due to lack of security protocols.

3] Thread Three : SMS Trojan

Malicious apps can cause sometimes include SMS trojans; which come in the form of compromised apps.