RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -9

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

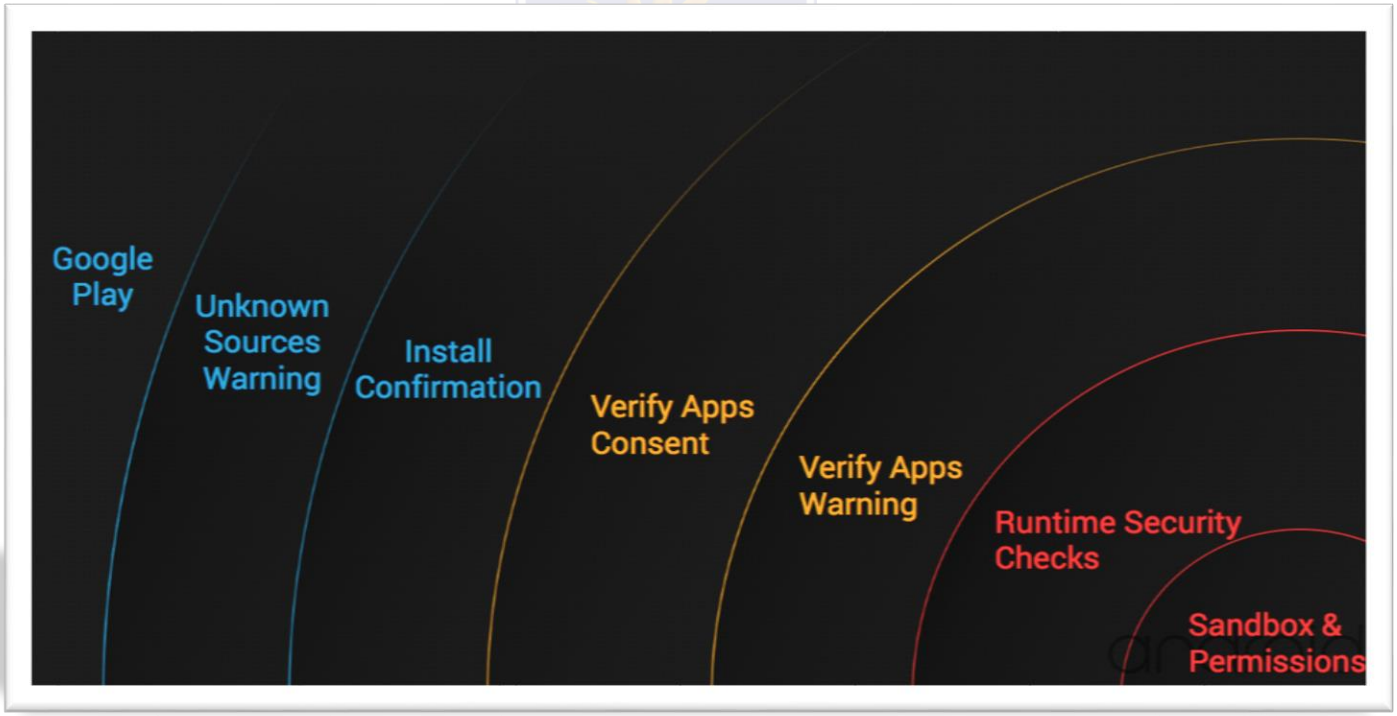
OUTLINE

- Android security mode
- Common Android vulnerabilities
    - Android threat
        - Leaking Information to Logs
        - SD-card Use
        - Unprotected Broadcast Receivers
        - Intent Injection Attacks
        - Wi-Fi Sniffing
- MCQ
- References

RAMA UNIVERSITY UTTAR PRADESH KANPUR

Android security model

Android is a multi-process system, in which each application (and parts of the system) runs in its own process. Most security between applications and the system is enforced at the process level through standard Linux facilities, such as user and group IDs that are assigned to applications.



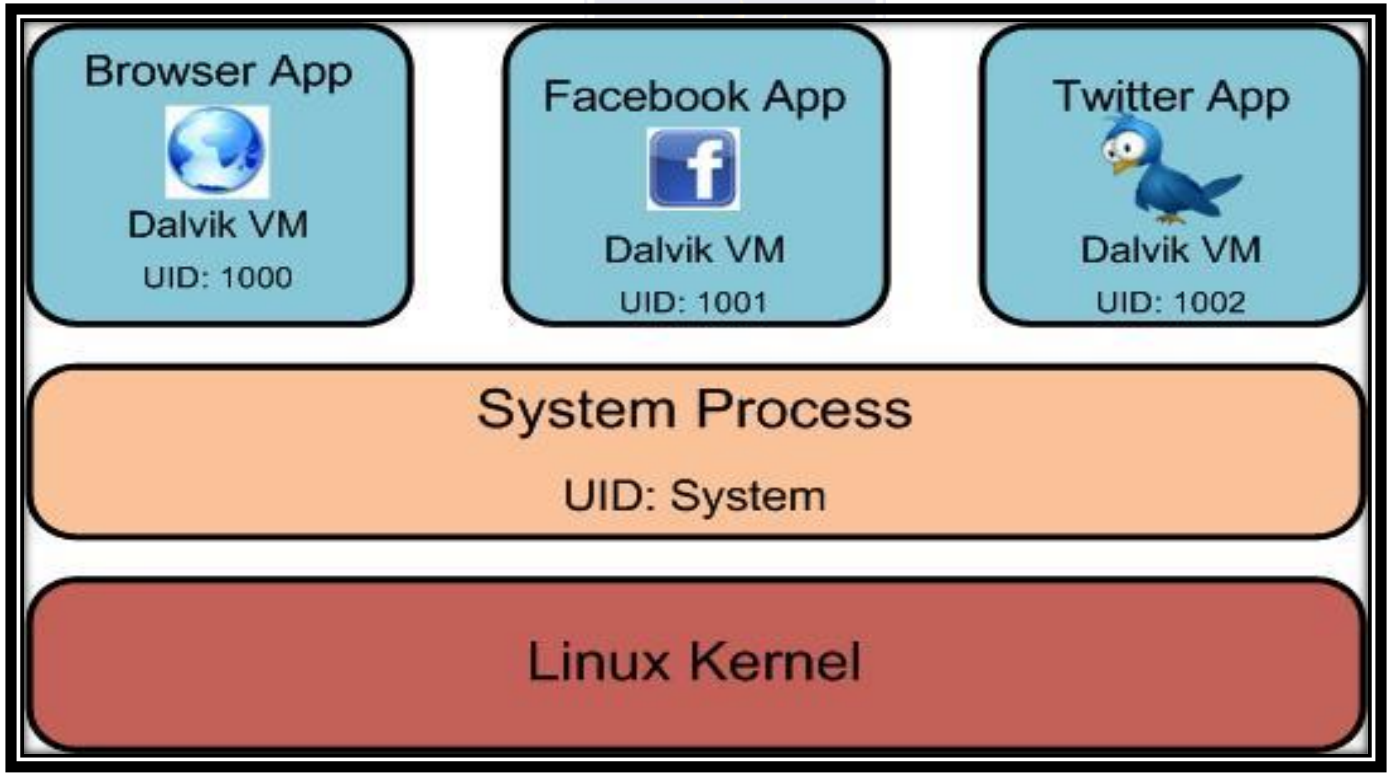
Android security model

- The Android security model is primarily based on a sandbox and permission mechanism. Each application is running in a specific Dalvik virtual machine with a unique user ID assigned to it, which means the application code runs in isolation from the code of all others applications.
- As a consequence, one application has not granted access to other applications' files. (1)
- Android application has been signed with a certificate with a private key Know the owner of the application is unique.
- This allows the author of The application will be identified if needed. When an application is installed in The phone is assigned a user ID, thus avoiding it from affecting it Other applications by creating a sandbox for it.
- This user ID is permanent on which devices and applications with the same user ID are allowed to run in a single process. This is a way to ensure that a malicious application has Can not access / compromise the data of the genuine application.

Android security model

It is mandatory for an application to list all the resources it will Access during installation. Terms are required of an application,

in The installation process should be user-based or interactive Check with the signature of the application.



Android threat

However, the Android operating system also revealed some of its faults for the user may be attacked and stolen personal information.

✓ Some security vulnerabilities on Android:

❑ Leaking Information to Logs:

Android provides centralized logging via the Log API, which can displayed with the “logcat” command. While logcat is a debugging tool, applications with the READ_LOGS permission can read these log messages. The Android d documentation for this permission indicates that “the logs can contain slightly private information about what is happening on the device, but should never contain the user’s private information.”

RAMA UNIVERSITY UTTAR PRADESH KANPUR

ANDROID THREAT

- **SD-card Use:**

  Any application that has access to read or write data on the SD-card can read or write any other application's data on the SD-card

- **Unprotected Broadcast Receivers:**

  Applications use broadcast receiver components to receive intent messages. Broadcast receivers define "intent filters" to subscribe to specific event types are public. If the receiver is not protected by a permission, a malicious application can forge messages.

- **Intent Injection Attacks:**

  Intent messages are also used to start activity and service components. An intent injection attack occurs if the in-tent address is derived from un-trusted input.

- **Wi-Fi Sniffing:**

  This may disrupt the data being transmitted from A device like many web sites and applications does not have security measures strict security. The application does not encrypt the data and therefore it can be Blocked by a listener on unsafe lines.

RAMA UNIVERSITY UTTAR PRADESH KANPUR

MCQ

11. How many basic processes or steps are there in ethical hacking?

a) 4

b) 5

c) 6

d) 7

2. _____ is the information gathering phase in ethical hacking from the target user.

a) Reconnaissance

b) Scanning

c) Gaining access

d) Maintaining access

3. Which of the following is not a reconnaissance tool or technique for information gathering?

a) Hping

b) NMAP

c) Google Dorks

d) Nexpose

4. There are _____ subtypes of reconnaissance.

a) 2

b) 3

c) 4

d) 5

5. Which of the following is an example of active reconnaissance?

a) Searching public records

b) Telephone calls as a help desk or fake customer care person

c) Looking for the target's details in the database

d) Searching the target's details in paper files

RAMA UNIVERSITY UTTAR PRADESH KANPUR

REFERENCES

- https://hydrasky.com/mobile-security/android-security-model-and-threat/

RAMA UNIVERSITY
UTTAR PRADESH
KANPUR