Module 2

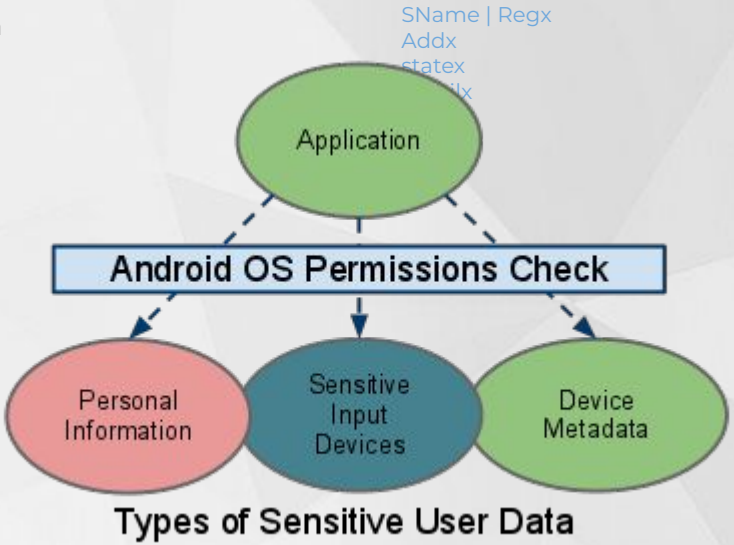
Mobile / Smartphone Security

Goals for Day

- Access control in Android operating system
- Rooting Android devices
- Repackaging attacks
- Attacks on apps
- Whole-disk encryption
- Hardware protection: TrustZone

Access control in Android operating system

- A formal specification for access control in Android (AciA) facilitates a deeper under- standing of the nature in which Android regulates app access to resources



Rooting Android devices

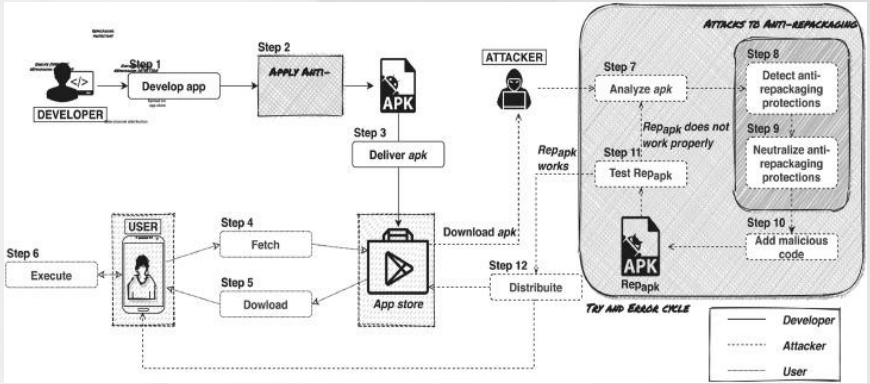
- Rooting is the process
- Which users of Android devices can attain privileged control
- Over various subsystems of the device, usually smartphones

SName | RegX
Addx
statex
emailx

Repackaging attacks

- Repackaging attack is a very common type of attacks on Android devices
- In such an attack, attackers modify a popular app downloaded from app markets
- Reverse engineer the app, add some malicious payloads
- Then upload the modified app to app markets
- Users can be easily fooled, because it is hard to notice the difference between the modified app and the original app
- Once the modified apps are installed, the malicious code inside can conduct attacks, usually in the background

SName | Regx
Addx
statex
emailx



Attacks on apps

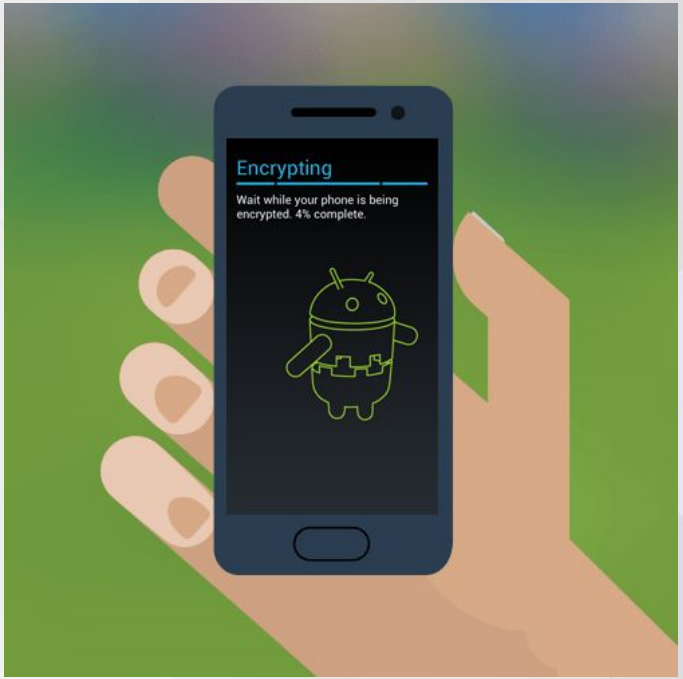
8 Most Dangerous Types of Mobile App Cyberattacks

- Malware in Mobile Apps
- On-Device Fraud (ODF)
- Rooting or Jailbreaking
- Phone Call Redirection
- Notification Direct Reply Abuse
- Domain Generation Algorithm (DGA)
- Bypassing App Store Detection
- Refined Development Practices

Whole-disk encryption

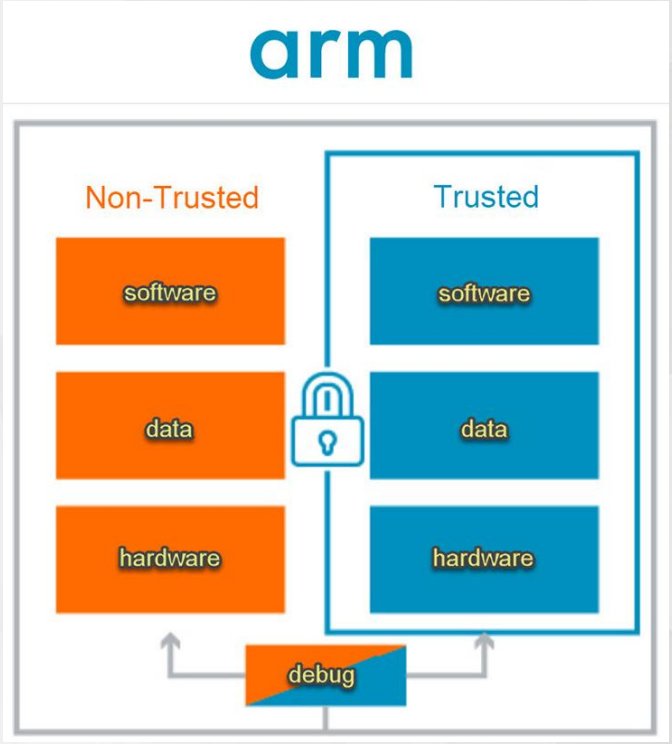
- Full-disk encryption is the process of encoding all user data on an Android device using an encrypted key

SName | RegX
Addx
statex
emailx



Hardware protection: TrustZone

- Abstract—ARM TrustZone is a hardware security extension technology
- Which aims to provide secure execution environment
- By splitting computer resources between two execution worlds
- Namely normal world and secure world



Time for Queries..!