# Android Platform Realities


- What makes the malware to rise high?
  - Android provenance system
    - Application masquerading (repackaging) is easy
  - Permissions are user centric
    - Its hard to imagine that every user is security driven or knowledgeable
      - » **Ignorance is exploited !**
  - Encryption is offered in platforms beginning with version 3 (Honey Comb)
    - Version >= 3 → dm-crypt kernel (block device layer) feature is used.
    - All the android versions < 3 do not have proper encryption model
      - » **ALERT – What about android devices running 2.x versions ?**
  - No inbuilt mechanism to prevent social engineering and web trickeries
  - Existence of alternative android application markets
    - Increases the attack surface with mobility and flexibility

# Introduction to Android Malware


- Android Malware Classification - Overview

  - Type-A
    - Exploits the application layer
      - » Example:- **Zitmo, Spitmo, Hippo SMS**
  - Type-K
    - Exploits the integrity of kernel to compromise the device
    - Typically, used as a pillar in hybrid android malware
      - » Example: **Ginger Master, Droid Deluxe**
  - Type-Z
    - Basically, an information stealer that does not modify any component of the android device
      - » Example: **Fake Netflic, Android Dogo War, Android Snake Tap**
  - Type-H
    - Hybrid in nature.
    - Harnesses the power of Type-A , Type-K and Type-Z malware collaboratively
      - » Example: **Android Root Smart, Droid Coupon**

# Techniques and Tactics


- Android Malware Tactics
  - Application Masquerading and Repackaging
    - Adding malicious code in the legitimate applications
    - Signing repackaged application with different signature
  - Native Code Execution
    - Exploiting kernel vulnerabilities to gain root access
  - Over The Air (OTA) Infections
    - Pushing malicious content on the android devices
  - Device Administration APIs
    - Fooling users to treat malware as applications having administrative rights
  - Hijacking (Spoofing and Eavesdropping)
    - Manipulating the communication flow - broadcasts, activities and services
  - Exploiting Custom ROM's
    - Signing custom ROM with public keys and installing them on android devices
  - Android Bootkits