Storage and interface vulnerabilities

Storage:sdcard vfat, world readable, source code reversing

Interfaces:Open interfaces with accessible dangerous functionality (Services, Broadcast Receivers, etc.)

Next Gen Attacks: Piggybacking on storage and interfaces

Find sensitive data storage location with code reversing

Access file if permissions available (steal permission to the data)

Send intents to open interfaces with dangerous functionality

Effectively gain the permission

Mitigations

No sensitive data: on the sdcard, in world readable files, in source code

No dangerous functionality directly accessible via open interfaces (ie ask users to click ok before sending an SMS)

Use require-permission tag in manifest for interfaces