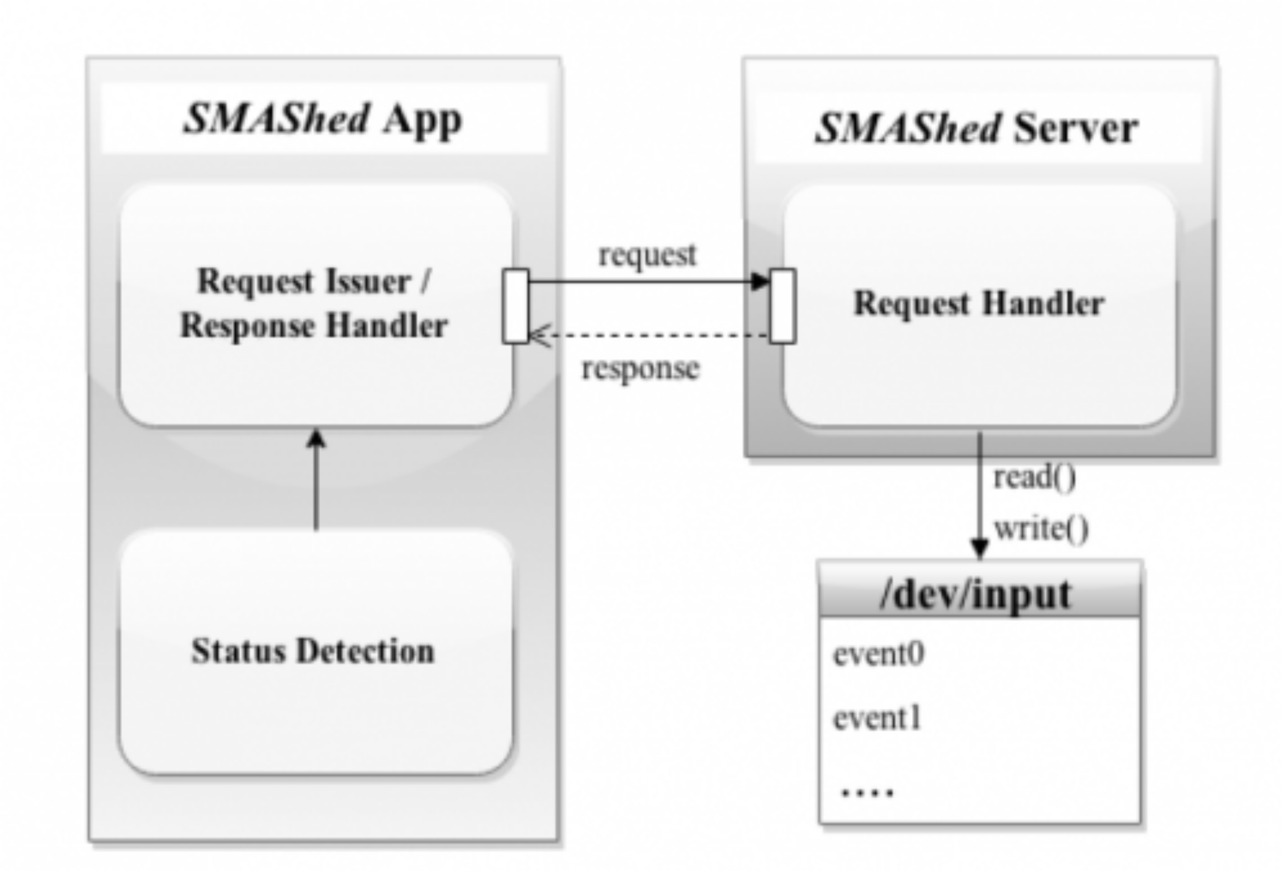
SMASheD: Sniffing and Manipulating Android Sensor Data

MAR 18TH, 2016

摘要

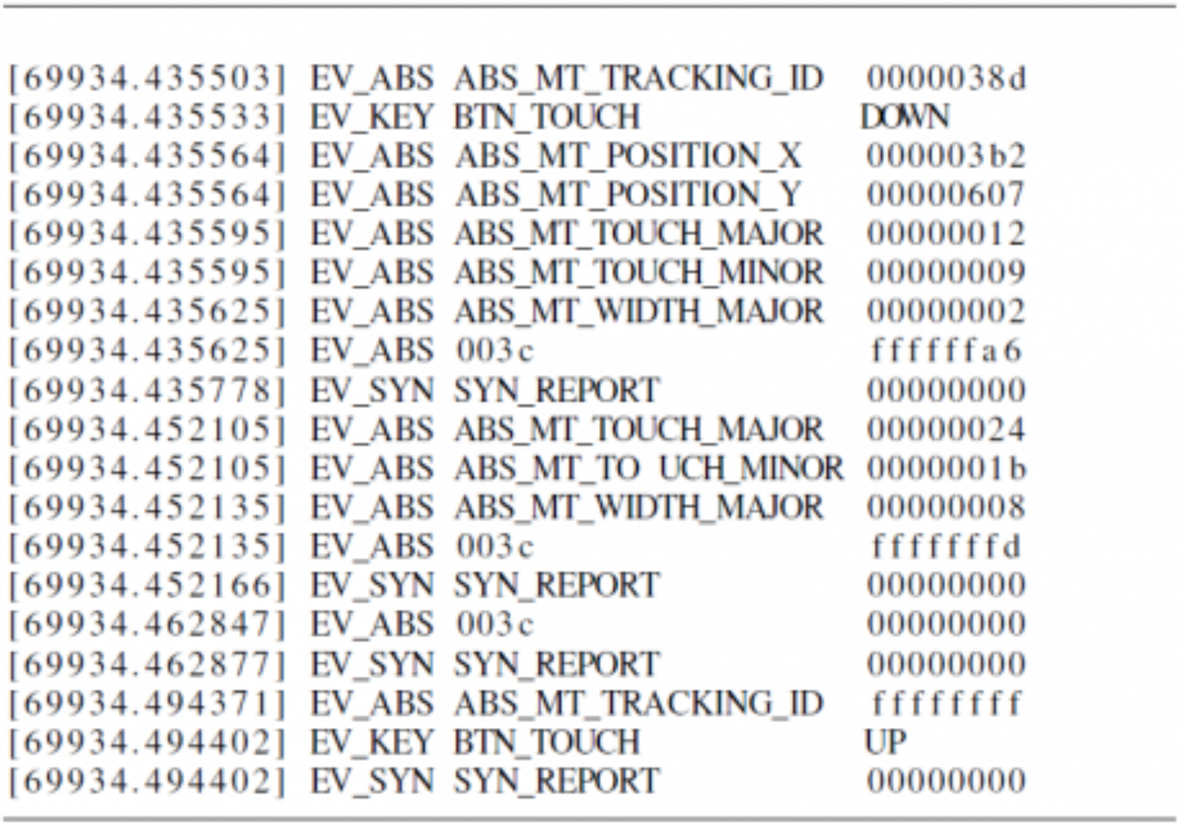
- 现在的传感器的安全模型主要是限制APP能访问的传感器或者在安装的时候限制了相关的权限
- 作者发现，可以利用安卓手机（不需要ROOT）中ADB的，能够使得APP在只有访问网络的权限下，实施读取传感器数据、劫持点击、篡改传感器数据等攻击
- 作者根据上述问题，开发了一个合法的APP，能够正常的实施攻击。

SMASheD



- Server:模拟了adb的命令getevent，sendeven

Listing 2: Sample output from running *getevent* for a single press release



```
[69934.435503] EV_ABS  ABS_MT_TRACKING_ID   0000038d
[69934.435533] EV_KEY  BTN_TOUCH            DOWN
[69934.435564] EV_ABS  ABS_MT_POSITION_X    000003b2
[69934.435564] EV_ABS  ABS_MT_POSITION_Y    00000607
[69934.435595] EV_ABS  ABS_MT_TOUCH_MAJOR   00000012
[69934.435595] EV_ABS  ABS_MT_TOUCH_MINOR   00000009
[69934.435625] EV_ABS  ABS_MT_WIDTH_MAJOR   00000002
[69934.435625] EV_ABS  003c                 ffffffa6
[69934.435778] EV_SYN  SYN_REPORT           00000000
[69934.452105] EV_ABS  ABS_MT_TOUCH_MAJOR   00000024
[69934.452105] EV_ABS  ABS_MT_TO UCH_MINOR  0000001b
[69934.452135] EV_ABS  ABS_MT_WIDTH_MAJOR   00000008
[69934.452135] EV_ABS  003c                 fffffffd
[69934.452166] EV_SYN  SYN_REPORT           00000000
[69934.462847] EV_ABS  003c                 00000000
[69934.462877] EV_SYN  SYN_REPORT           00000000
[69934.494371] EV_ABS  ABS_MT_TRACKING_ID   ffffffff
[69934.494402] EV_KEY  BTN_TOUCH            UP
[69934.494402] EV_SYN  SYN_REPORT           00000000
```

攻击

- 嗅探屏幕的点击事件数据
- 点击劫持：在安装恶意APP的时候模拟点击安装、解锁、攻击一些已有的基于生物特征的安全
- 篡改其他的传感器：比如亮光的传感器