LinkDroid: Reducing Unregulated Aggregation of App Usage Behaviors

DEC 29TH, 2015

论文下载：https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-feng.pdf

Abstract & Introduction

- unregulated aggregation: 在用户不知道的情况下，可以收集一个设备上多个APP的行为或信息的恶意行为
- Linkability: 如果两个APP可以传递用户行为或信息，就是linkable。

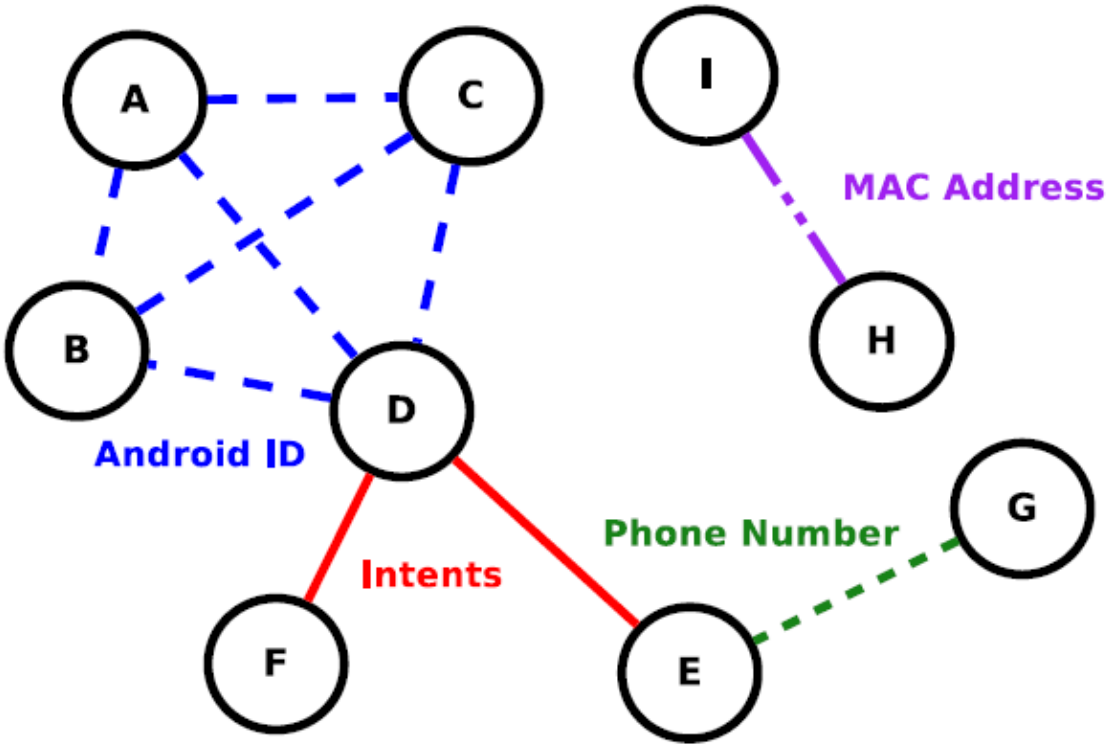
分两种形式：

1. 首先收集设备（MAC,IMEI），用户（phone number，account），位置（IP,Location）相关的识别信息，之后在云端将数据结合。
2. 在系统内部通过IPC，传递各种信息，还可以隐蔽的通过SD卡，数据库来共享信息。

现实中主要包括几类：1）广告库。2）监视机构 NSA国家安全局 GCHQ通信局 3）IT公司

Dynamic Linkability Graph

点代表APP，线代表之间是linkable. 如果两个APP读取同一设别信息，则认为是linkable。如果两个APP之间有IPC连接，也认为是linkable。



Category	*Type*	*Source*
OS-level Info.	Device	IMEI Android ID MAC
	Personal	Phone # Account Subscriber ID ICC Serial #
	Contextual	IP Nearby APs Location (PoIs)
IPC Channel	Explicit	Intent Service Binding
	Implicit	Indirect RW

Table 2: DLG considers the linkability introduced by 10 types of OS-level information and 3 IPC channels.

通过修改系统，动态收集信息，画出DLP。

Linkability in RealWorld

文章找了13个人测试47天，发现现实生活中存在很多这种Linkability。

LinkDroid

1 安装时混淆，为每个APP生成一个独立的mask code，去混淆系统的识别信息，比如deviceID等。这样可以减少很多link.

2 当DLG要改变前，会询问用户是否阻拦。比如一个APP读取系统识别信息时，或向另一个APP发送intent时。

3 unlinkable mode.

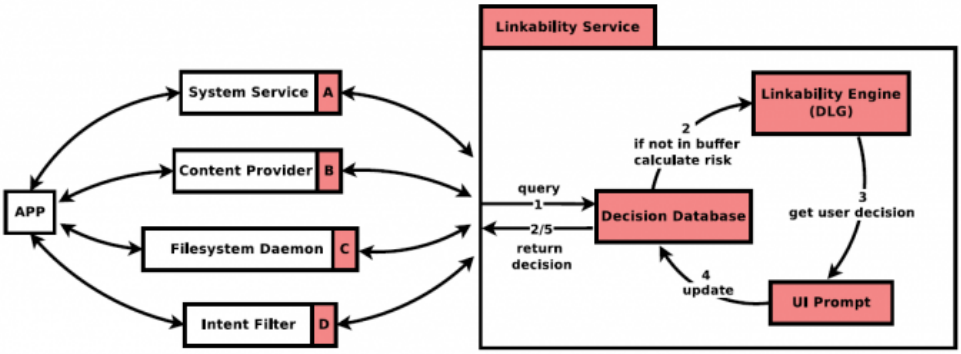


Figure 10: An overview of LinkDroid. Shaded areas (red) represent the parts we need to extend/add in Android. (We already explained how to extend A, B, C and D in Section 3.4.)