组会前-20210809

进度情况：

- 完成了规定文章的阅读，其中Systematic Detection of Capability Leaks in Stock Android Smartphones.还需要进一步阅读。
- 解决了之前运行Androguard的报错信息，后续的问题也大多是Python中缺少相应的库或者库的版本问题，现在能正常分析apk文件了；整理了一些Androguard中基本函数的功能。
- 对callback函数、Manifest文件的作用、IMEL等有了更加细化的了解。

问题：

- 选择的六篇paper中至少有三篇用到了Soot，目前知道它是一个Java字节码的分析架构，有必要细化了解其具体功能吗?
- 安卓中的documented API与undocumented API是否是特指?
- 不太明白安卓的field（字段）是用来干什么的?
- Signature-based malware detection是泛指基于与已有库的特征匹配的一类检测吗?
- 在按照androguard的指导书尝试其各种作用时，自己不怎么能理解产生的结果，比如产生的控制流图（CFG）， abstract syntax trees (AST) 等等，要学习下吗？要的话从何入手呢?