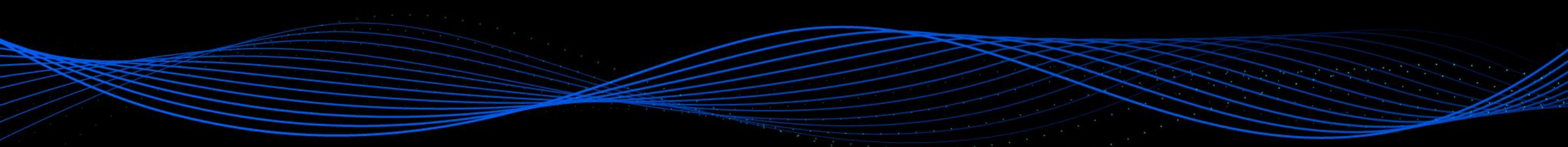
分身大师那些事儿

王云鹏 / 360技术经理



1.分身大师及技术架构

2.基本原理解析

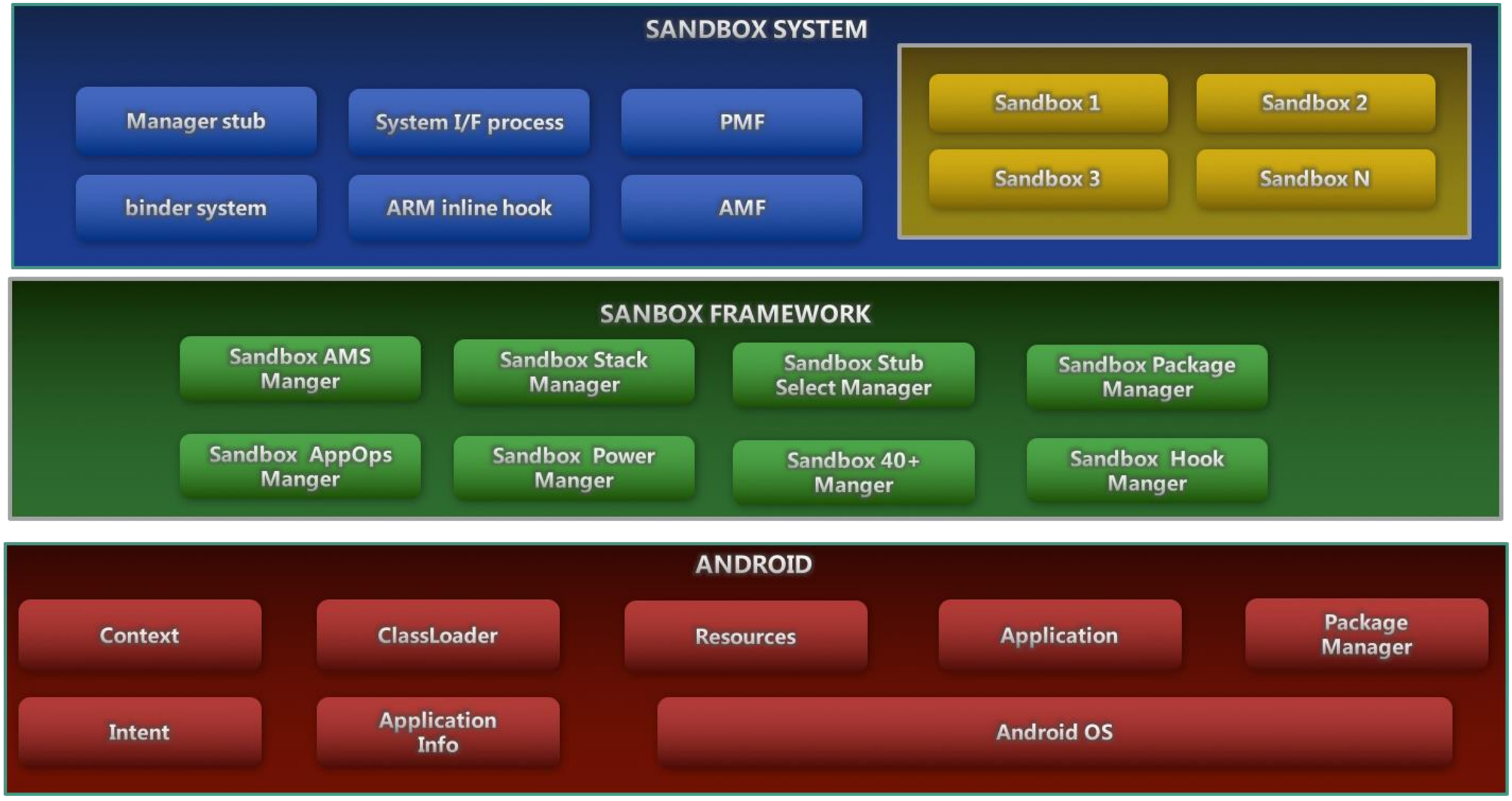
3.分身大师实战经验

4.分身技术展望

分身大师

- 基于沙箱机制打造的Android App
- 内部运行原生Android应用
- 依赖Android的Hook机制
- 轻量级的Android虚拟机

整体技术架构



1.分身大师及技术架构

2.基本原理解析

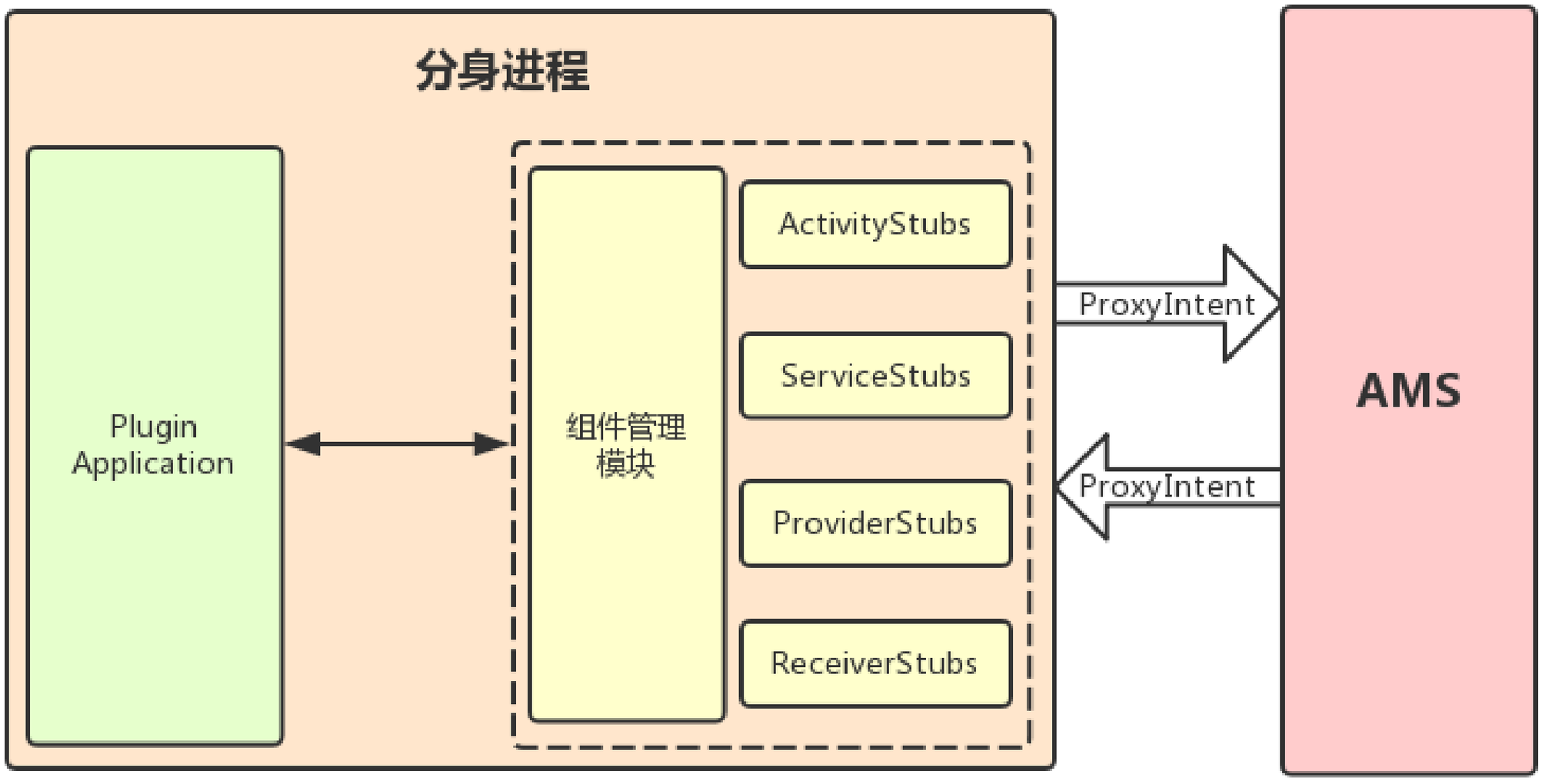
3.分身大师实战经验

4.分身技术展望

需要解决的问题

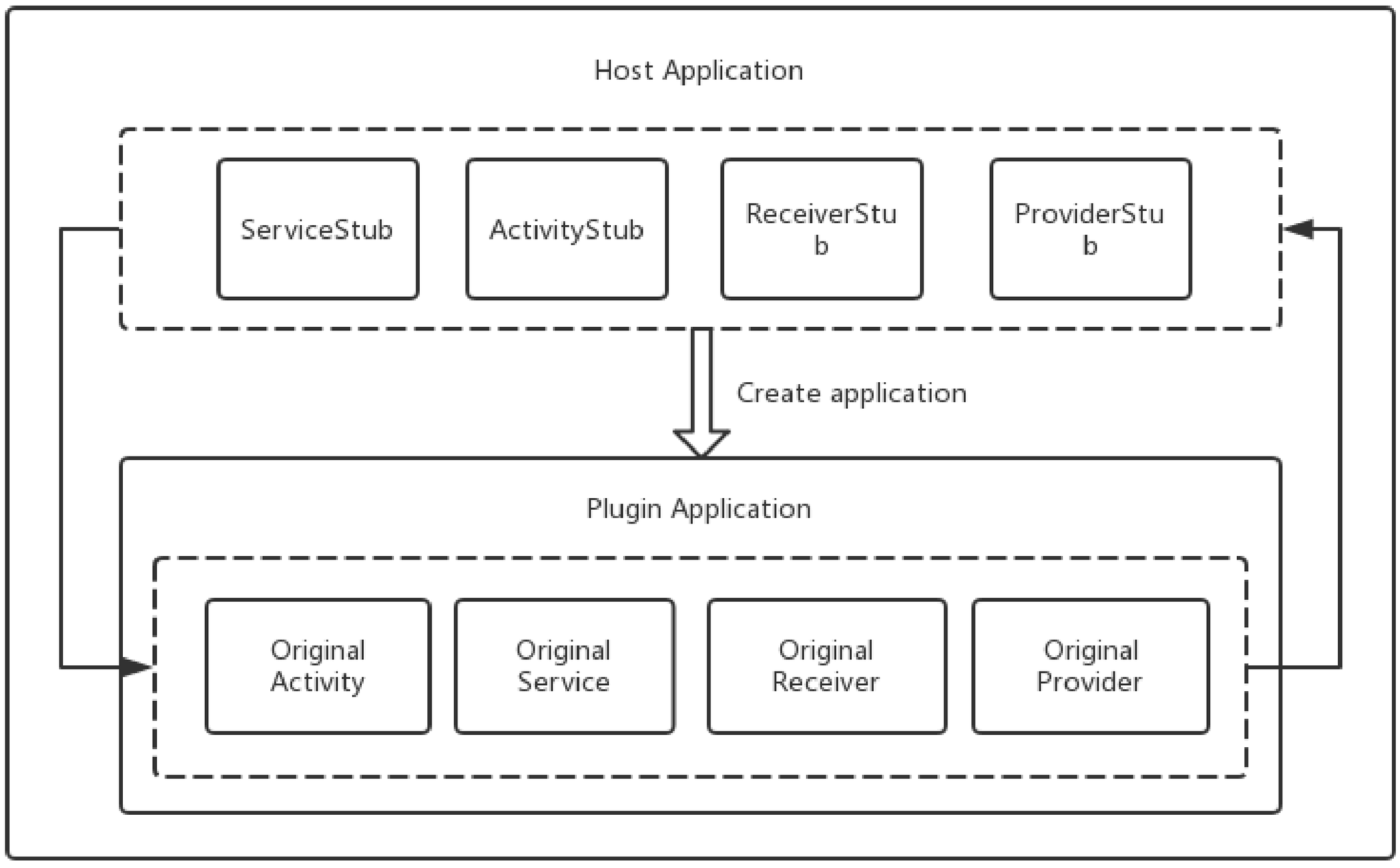
- Android 4大组件代理机制
- 初始化Application
- 和系统服务通信(Binder Hook)
- 文件路径重定向(Native Hook)
- 运行Android 4大组件

组件代理机制

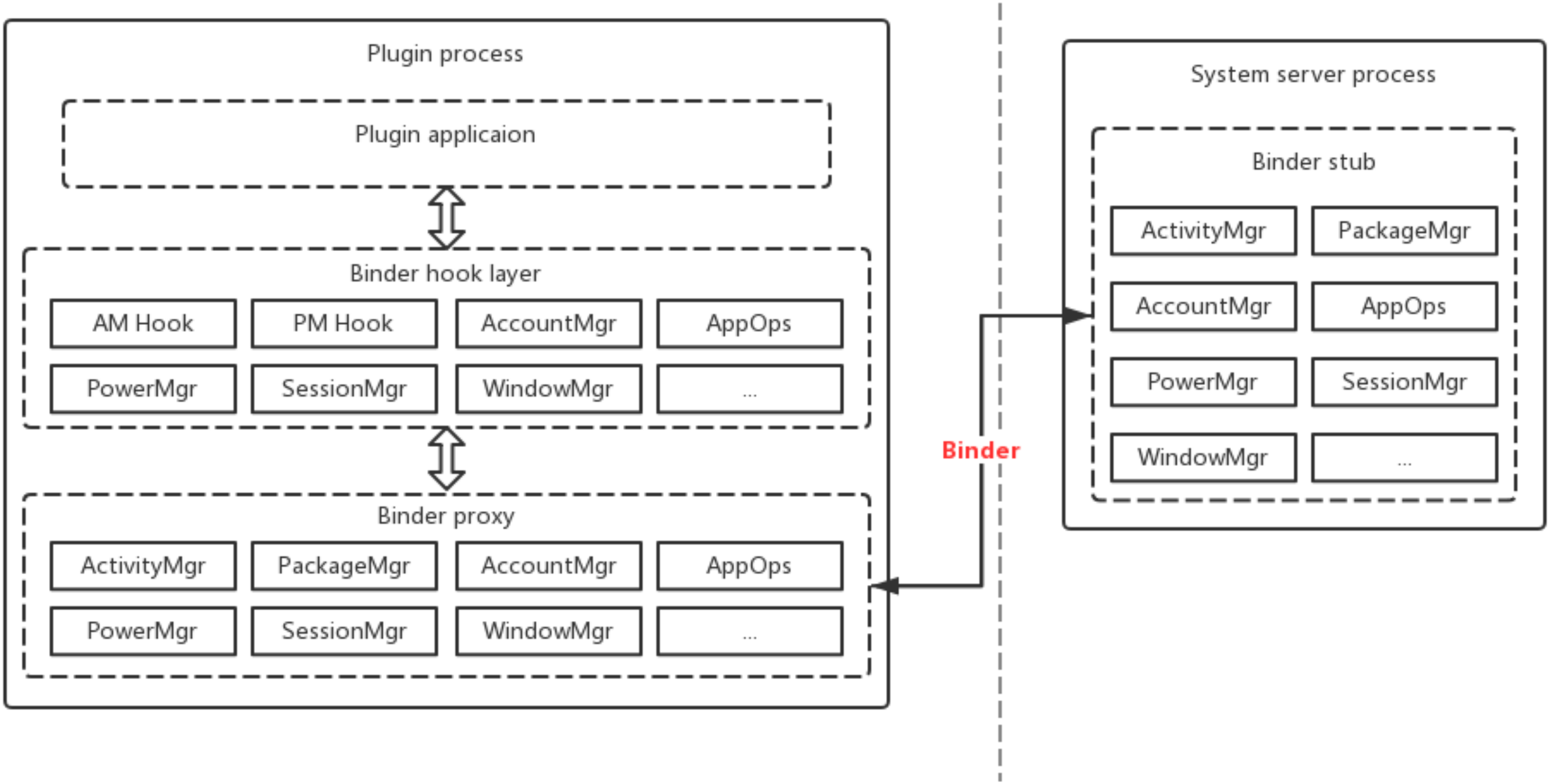


OriginalIntent

Application初始化

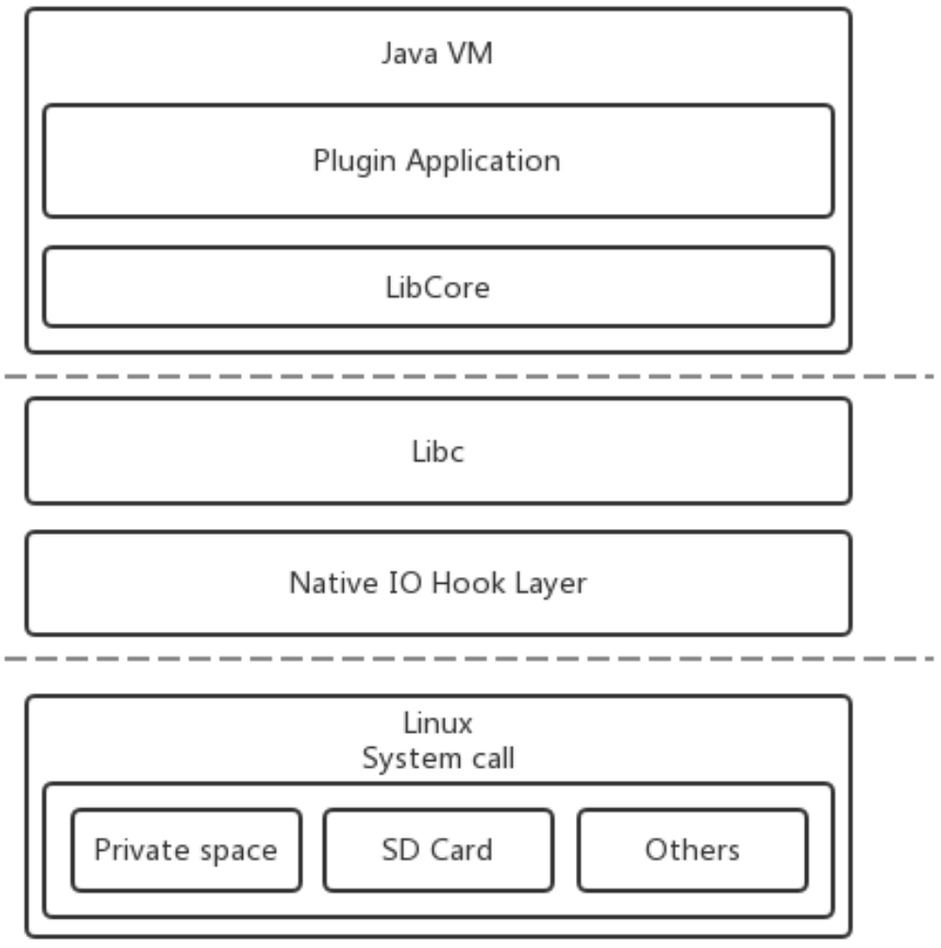


和系统服务通信

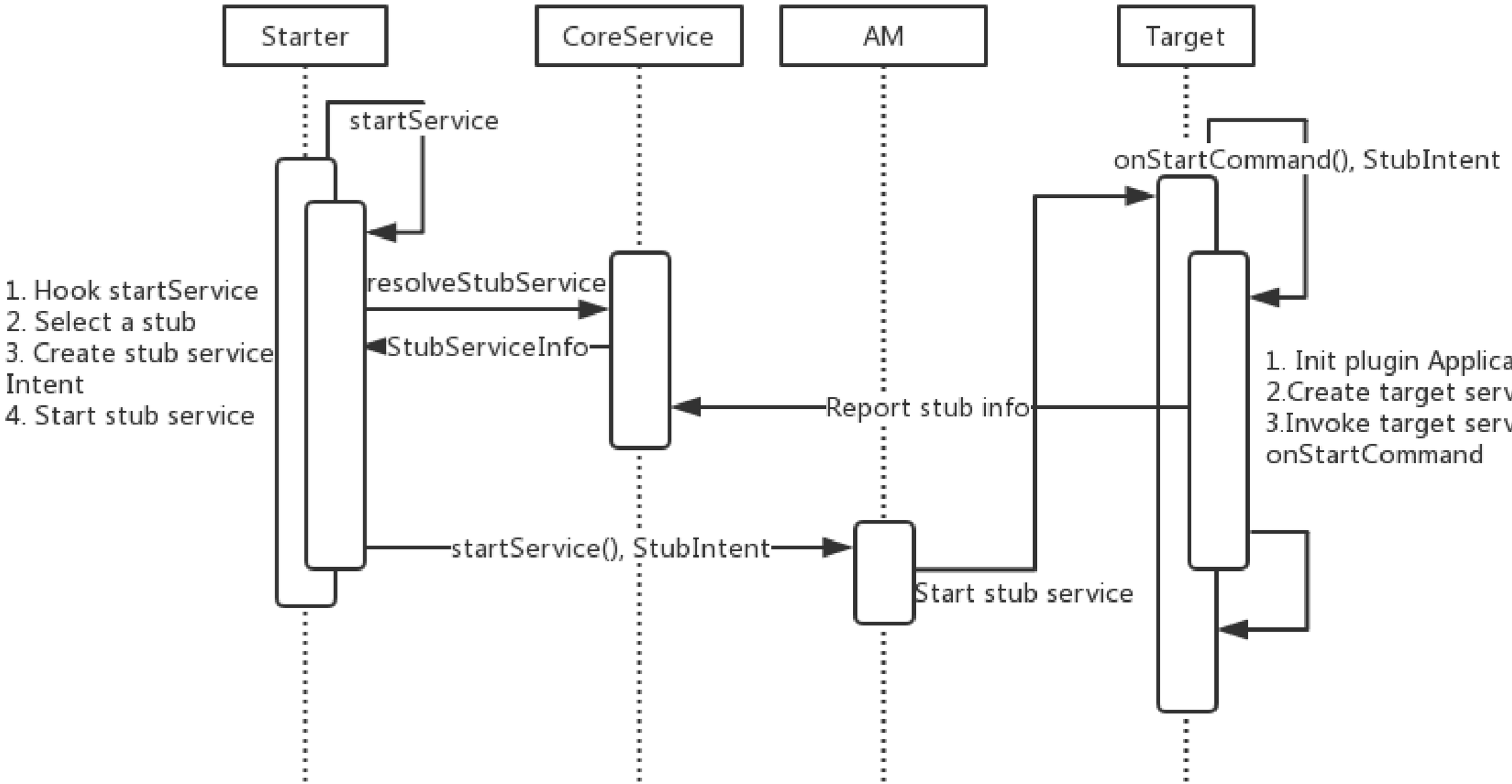


文件路径重定向

- 通过Native IOHook实现运行时替换
- SD卡目录隔离
- 与外部应用通信时，路径的正向和反向替换
- 加固类应用DEX目录重定向处理



组件启动流程



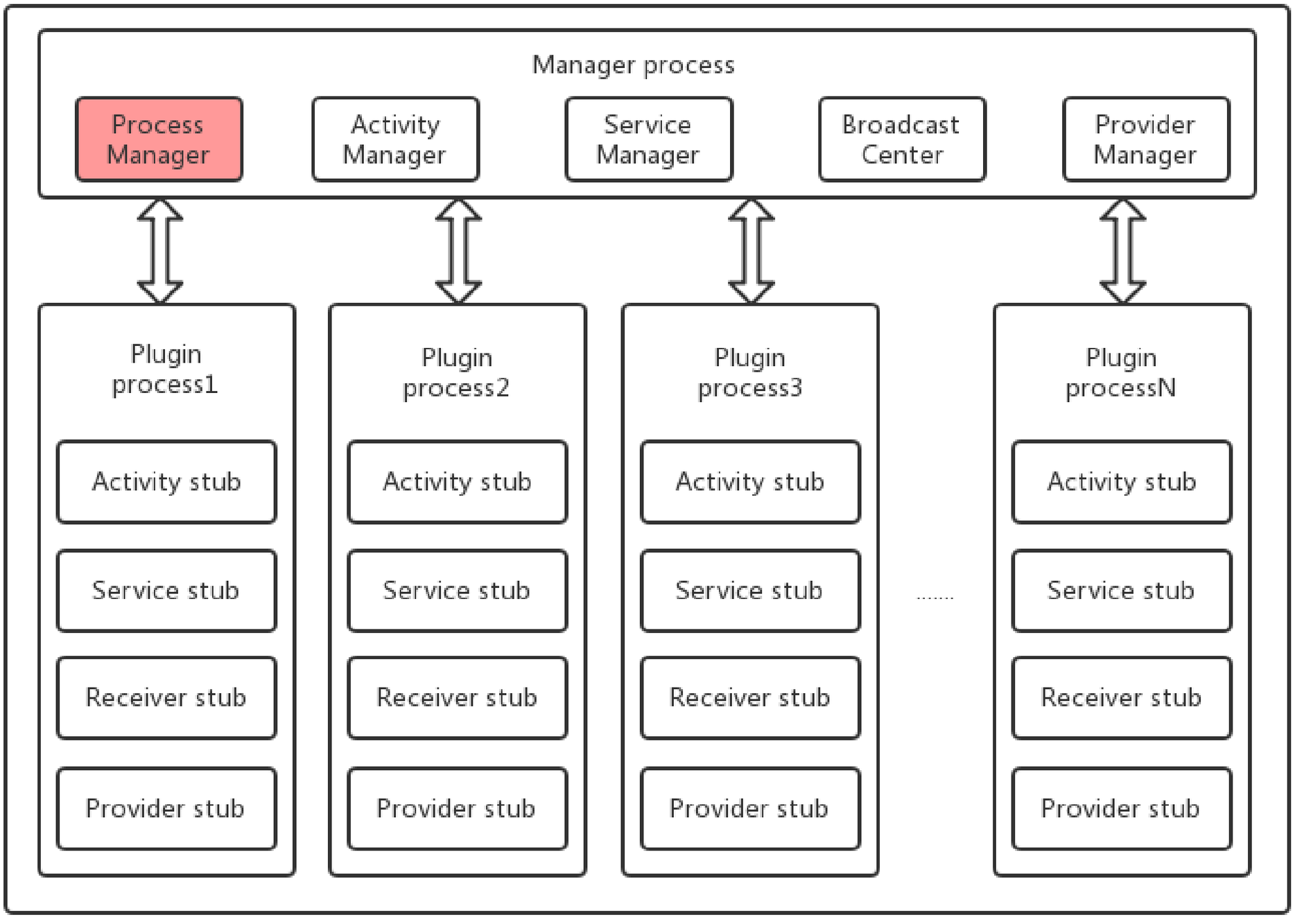
1.分身大师及技术架构

2.基本原理解析

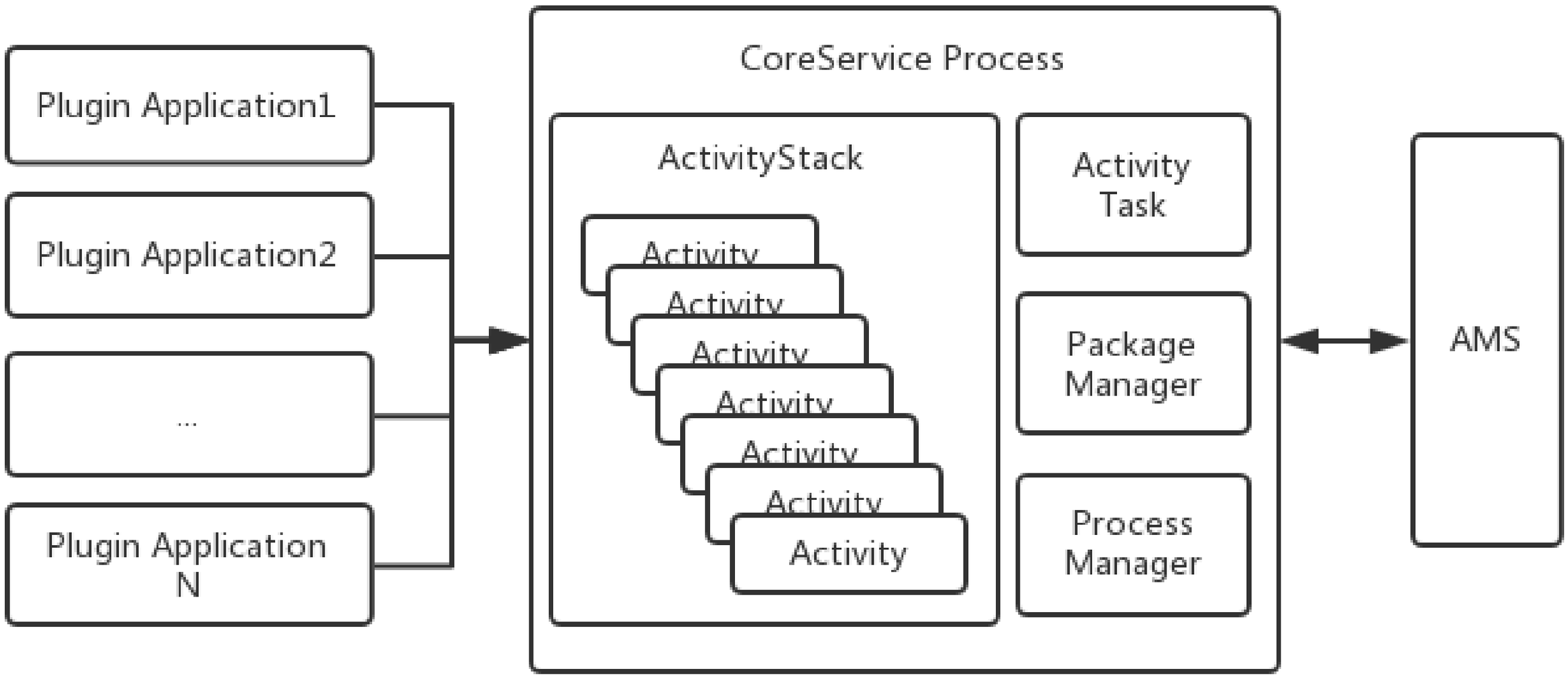
3.分身大师实战经验

4.分身技术展望

组件管理



Activity技术方案



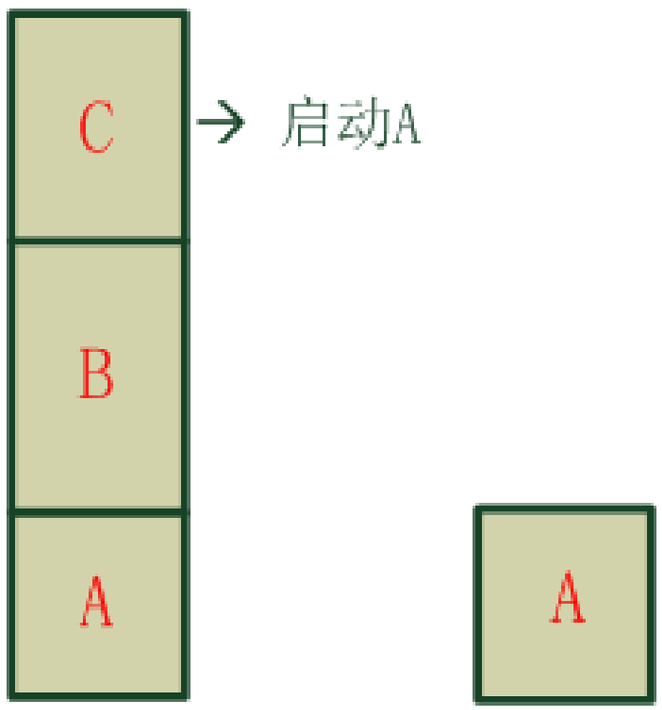
模拟SingleTask

典型SingleTask实例对比图

C → standard

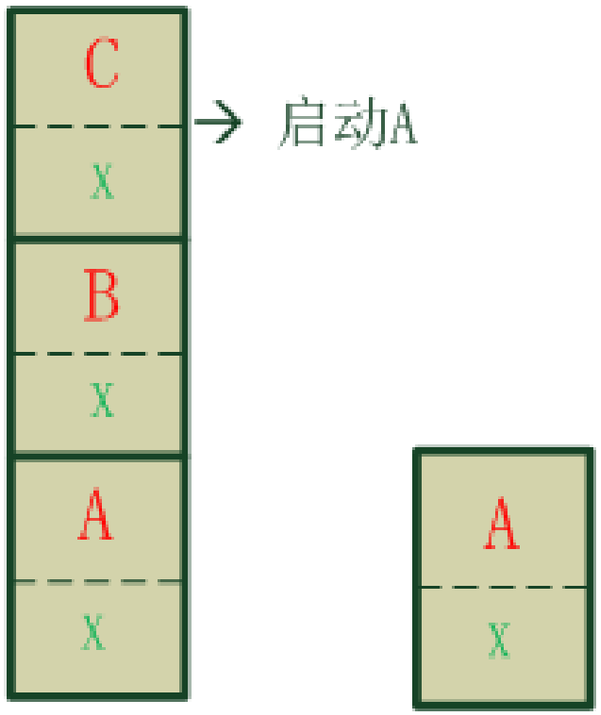
B → standard

A → singleTask



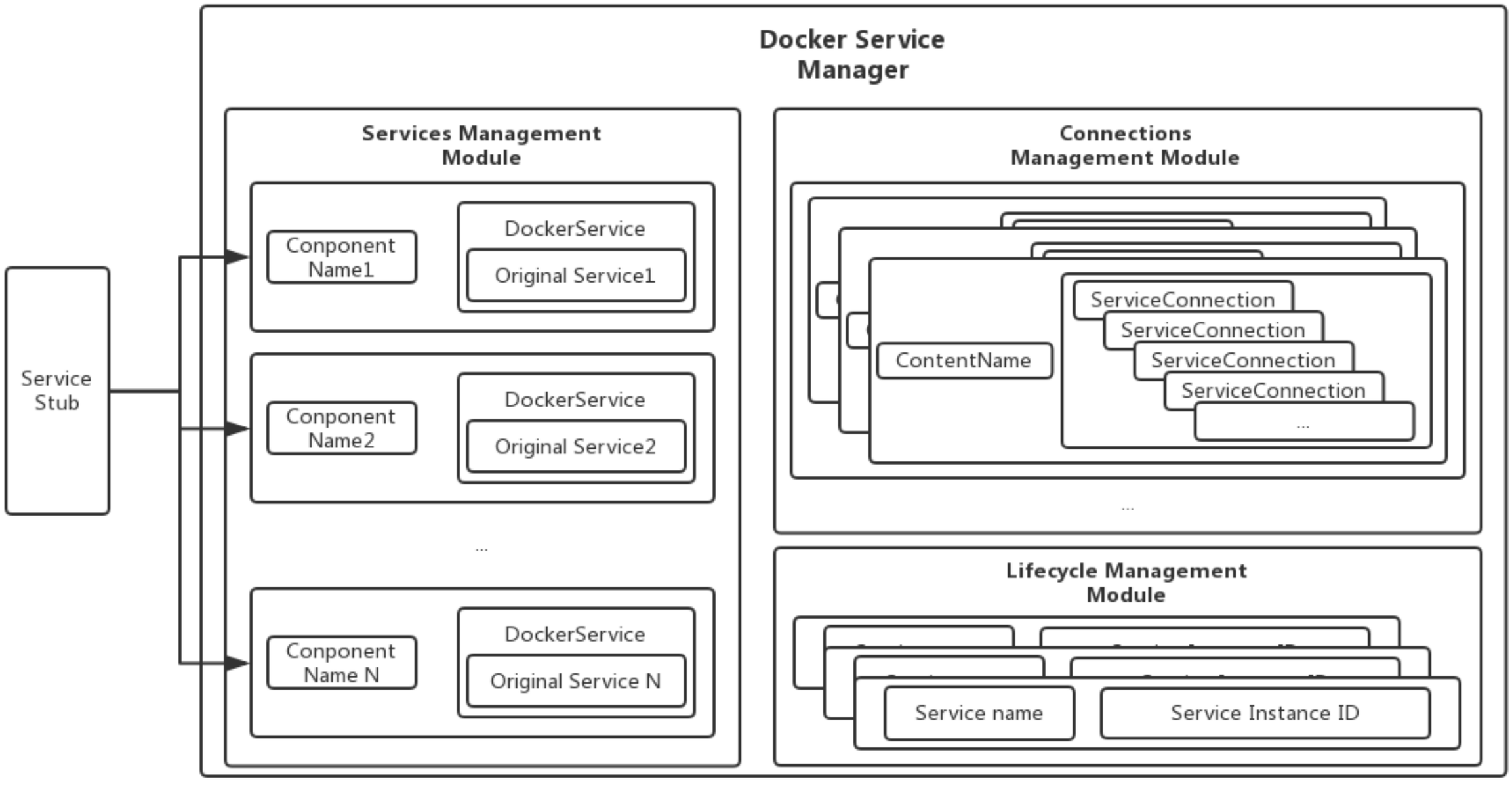
AMS自动清理B、C

X → standard
坑

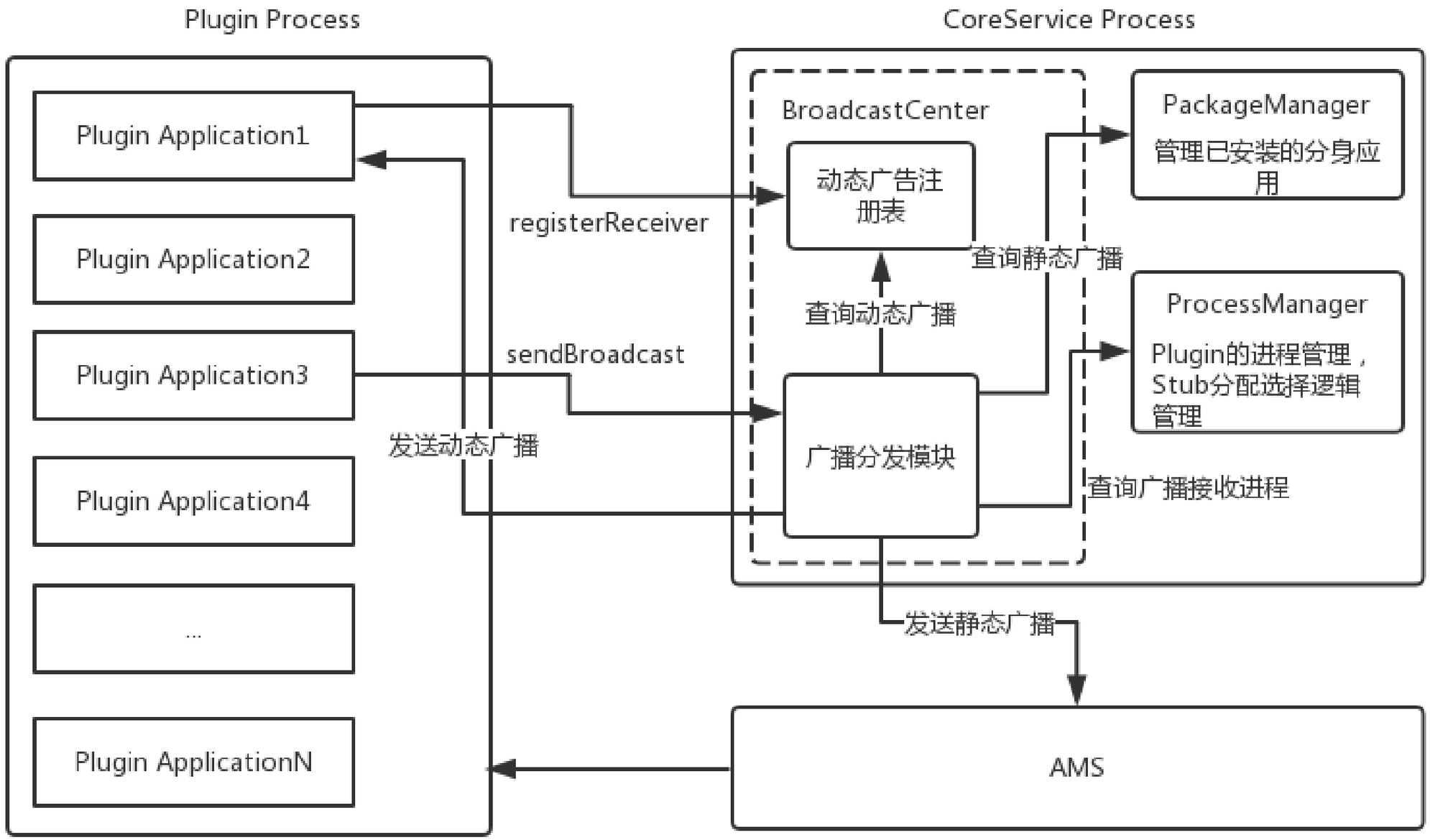


自己栈清理B、C

Service技术方案



Receiver技术方案



1.分身大师及技术架构

2.基本原理解析

3.分身大师实战经验

4.分身技术展望

技术挑战

- 需要Hook的点多，适配量巨大
- Android版本不断迭代，权限收紧
- Apk千差万别
- 加固应用方案变更

分身技术优势

- 原生APK无缝接入
- 免安装运行
- 替代ROOT，提供类似环境
- 提供较Android系统更丰富的接口

Contacts

wangyunpeng@360.cn

THANKS!