备注：注意分章节，逻辑讲清楚。图表要有标题，插交叉引用。

2.1 性能摸底报告

承轩可以参考5-内核态app汇报-性能摸底-v2.pptx & 6-内核态app汇报-性能摸底-v3.pptx & 9-bilibili启动阶段syscall占比.pptx

旭安可以参考7-内核态app进展-0109.pptx中的2-系统调用各个阶段的时钟周期

2.2 ARMv8-A指令手册梳理报告

祺菁可以参考论文PPT中的敏感指令定义

2.3 框架设计方案

亦凡可以参考内核态app框架.docx，0-内核态APP.pptx，【230323】KAPP-2.pptx，基础框架主要做两件事：

1. 异常事件转发，包括跳板页的设置等。
2. 页面属性设置。划线部分是旧方案，现有的将用户页面从U-page转成S-page的方案是截获VMA的权限设置，在VMA上设置属性为S-page，具体见代码。

除了文档中已有的描述，有些内容也可以写一下，包括copy\_from/to\_user的处理等。

承轩可以参考10-内核态app进展汇报-0320.pptx

* 1. 安全设计方案

整理自己的材料即可。