



life.augmented

STM32MP1 OP-TEE

目标

OP-TEE简介

运行xtest

TF-A的OP-TEE编译选项

获取OP-TEE源代码

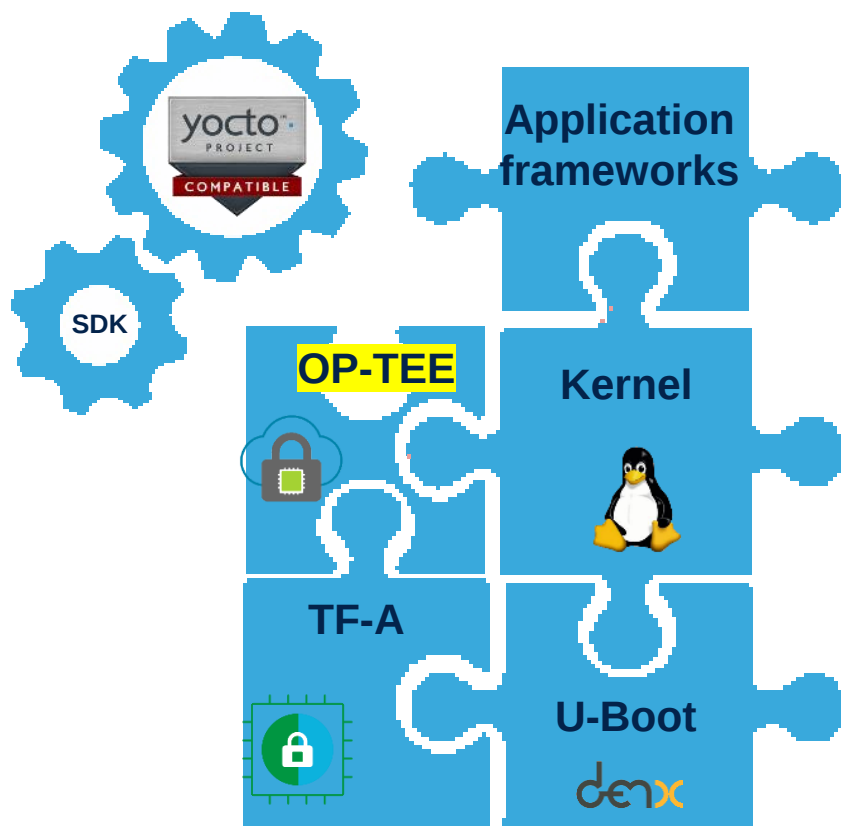
配置与编译
OP-TEE OS

下载OP-TEE
OS

修改与调试
OP-TEE OS

系统安全的补充说明

OP-TEE简介



STM32MP1 可选项

- 相对于TF-A自带的BL32, OP-TEE更容易扩展安全服务

OP-TEE

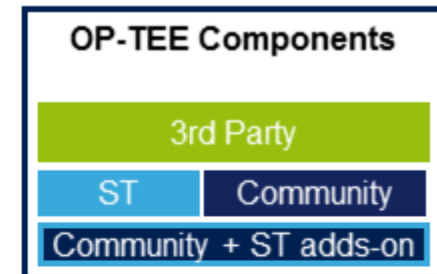
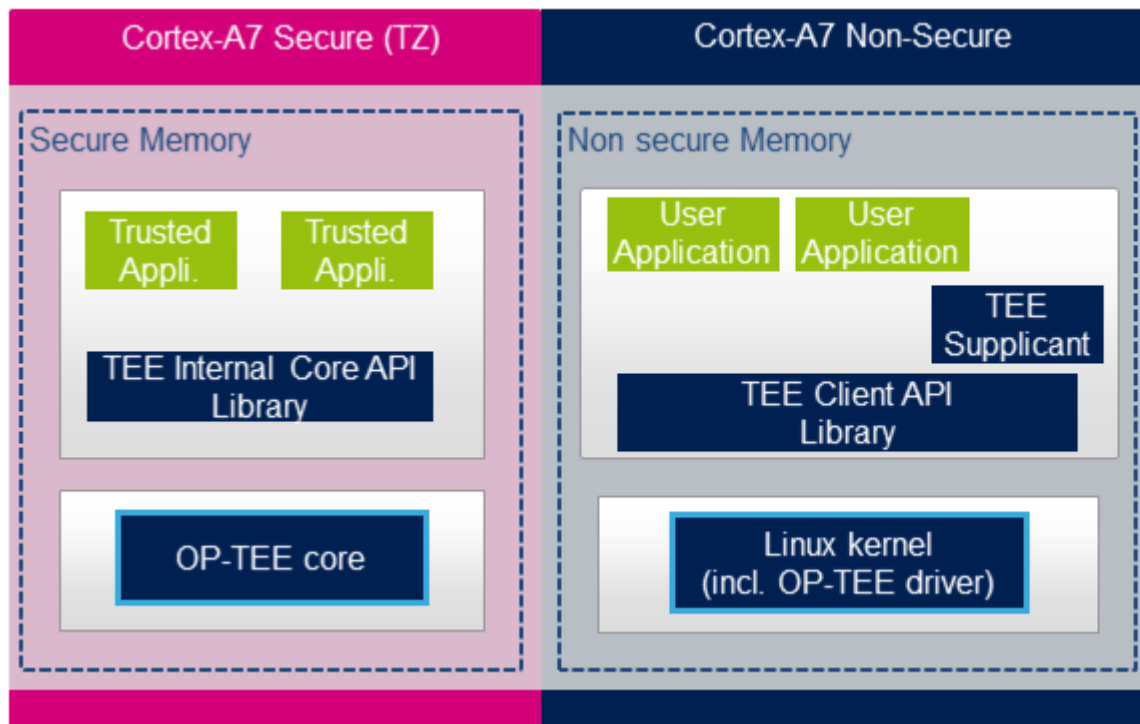
- 安全操作系统
- 由TF-A启动
- 可以动态加载TA
- 提供的安全服务可贯穿整个加电周期

Wiki资源

- 介绍
 - https://wiki.st.com/stm32mpu/wiki/OP-TEE_overview
- 开发
 - https://wiki.st.com/stm32mpu/wiki/STM32MP15_OP-TEE

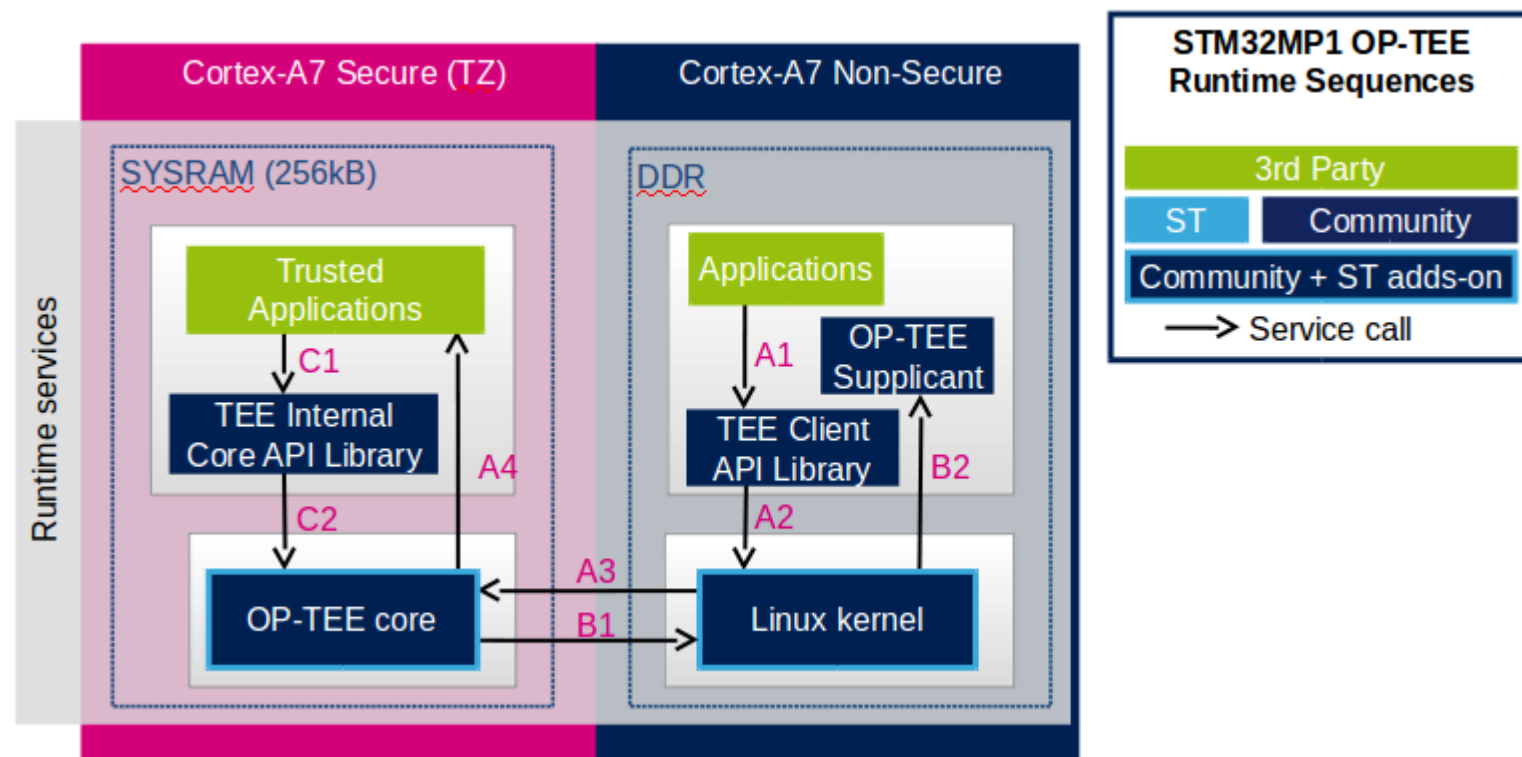
OP-TEE系统组成

- OP-TEE操作系统
 - Header
 - Pager
 - Pageable
- OP-TEE客户端
- OP-TEE例程与测试



运行xtest

- TF-A启动OP-TEE
- Linux启动OP-TEE驱动与客户端
- 用户可从Linux中调用OP-TEE服务
 - xtest



TF-A的OP-TEE编译选项

- Wiki资源
 - https://wiki.st.com/stm32mpu/wiki/STM32MP15_TF-A
- 要点
 - AARCH32_SP=optee
 - STM32MP_BOOT_ONLY=1

多种方式获取源代码

- 从Developer Package获取
 - 从www.st.com中下载指定版本
 - 从STM32 github获取更新版本
- 从OP-TEE github获取

推荐使用stm32 github

OP-TEE配置要点

PLATFORM

- 芯片平台
- 这里设为stm32mp1

CFG_SECURE_DT

- 设备树
- 这里设为stm32mp157a-dk1

CFG_TEE_CORE_LOG_LEVEL

- 日志等级

O

- 输出目录



OP-TEE编译要点

- 编译方法
 - 使用编译帮助文件Makefile.sdk
 - 直接配置编译
- 输出目录
 - ../build
- 内容
 - tee-header_v2.stm32
 - tee-pageable_v2.stm32
 - tee-pager_v2.stm32

OP-TEE下载要点

- 使用linux dd命令
- 使用uboot mass storage功能
- 使用STM32CubeProgrammer

OP-TEE修改与调试要点

使用TRACE

- Wiki资源
 - https://wiki.st.com/stm32mpu/wiki/OP-TEE_-_How_to_debug
- 对于TA仅推荐使用TRACE
- 操作
 - 编辑./core/arch/arm/kernel/generic_boot.c
 - 使用IMSG打印调试信息

使用GDB

- Wiki资源
 - <https://wiki.st.com/stm32mpu/wiki/GDB>
- 操作
 - [Path_env.gdb](#)
 - [Setup.gdb](#)

系统安全的补充说明

- OP-TEE是安全组件选项
- 选择OP-TEE也应选择安全启动
- Wiki资源
 - https://wiki.st.com/stm32mpu/wiki/STM32MP15_microprocessor

系列	安全	主频
STM32MP15xA	Basic	650 MHz
STM32MP15xC	Secure boot + Cryptography (<u>CRYP</u>)	650 MHz
STM32MP15xD	Basic	800 MHz
STM32MP15xF	Secure boot + Cryptography (<u>CRYP</u>)	800 MHz

- OP-TEE是什么？
- OP-TEE可提供哪些服务？
- 如何编译OP-TEE内核？
- 如何利用本课程的知识来编译OP-TEE Example？

Thank you