

# [月报] 蓬莱TEE更新-2023-09

## 1. 蓬莱TEE Roadmap

蓬莱TEE是上海交通大学IPADS实验室推出的RISC-V架构上的开源可信执行环境。为了更好的发展RISC-V的可信计算的开源生态，以及让用户更好的了解蓬莱TEE的未来的发展规划，我们将对蓬莱开源仓库的每月更新进行汇总，以月报和季报的方式，分享给大家。蓬莱现阶段包含三个主要仓库：

### 1. Penglai-TVM



Penglai-Enclave/**Penglai-Enclave-TVM**  
The main repo of Penglai Enclave based on RISC-V Trapped Virtual Memory (TVM).


4 Contributors 2 Issues 32 Stars 7 Forks



<https://github.com/Penglai-Enclave/Penglai-Enclave-TVM>  
**GitHub - Penglai-Enclave/Penglai-Enclave-TVM: The main repo of Penglai Enclave based on RISC-V Trapp**  
The main repo of Penglai Enclave based on RISC-V Trapped Virtual Memory...

Penglai-TVM版本是OSDI'21论文[[www.usenix.org](http://www.usenix.org)]论文的纯软件实现支持细粒度内存隔离，enclave的shadow fork，server enclave等更加丰富了功能。该版本主要用于学术上的前沿研究。

### 2. Penglai-PMP/sPMP



<https://github.com/Penglai-Enclave/Penglai-Enclave-sPMP>  
**GitHub - Penglai-Enclave/Penglai-Enclave-sPMP: Penglai Enclave is an open-sourced, secure and scalab**  
Penglai Enclave is an open-sourced, secure and scalable TEE system for RISC...

Penglai-PMP/sPMP版本是基于RISC-V PMP保护的用户态Enclave，类似于Intel的SGX。我们通过提供Enclave libruntime支持用户态enclave的各种函数功能（受保护的系统调用以及用户自定义的函数功能）。接下来，我们将进一步完善Penglai-PMP/sPMP的生态共建，具体计划如下：

- a. 支持Secgear[[secGear](#)]+openEuler 23.09：Secgear提供了不同TEE架构的统一接口（Intel SGX，Arm TrustZone以及RISC-V Penglai），基于Secgear的框架，能够实现sealing，TLS server，attestation等Enclave的基本功能，也允许用户实现自定义的ecall和ocall的函数。

#### 开源计划：

- i. openEuler 23.09+opensbi 1.3：预计2023年9月开源（已开源）
- ii. Secgear-v0.2.0支持：预计在2023年十月份开源支持所有secgear demo的蓬莱实现
- iii. Enclave libruntime的完善（类似SGX scone的实现）：预计在2024第一季度
- b. 支持RISC-V OpenHarmony：OpenHarmony/开源鸿蒙[[www.openharmony.cn](http://www.openharmony.cn)]致力于实现下一代操作系统。RISC-V OpenHarmony是开源鸿蒙社区对RISC-V的支持，而蓬莱将作为RISC-V开源鸿蒙的可信基石。

## 开源计划：

- i. 对OpenHarmony QEMU+DAYU800硬件平台的支持：预计2023年第四季度开源
- ii. TEE SDK包含基础通信计算能力：预计2023年第四季度开源
- iii. 对于主流加密签名算法的支持（包含国密SM2, SM3, SM4等）：预计2023年第四季度开源
- iv. 实现端侧可信存储：预计2024年第一季度开源
- v. 支持PSA/GP可信计算框架：预计2024年第二季度开源
- vi. 支持分布式TEE实现（基于机密软总线实现）：预计2024年第一季度

## 3. PenglaiZone

Penglai-Enclave/  
**PenglaiZone**

PenglaiZone is a project that aims to support the privileged zone in Trusted Execution Environment (TEE), such as TEEOS, standaloneMM...

6

Contributors

0


Issues

4

Stars

0

Forks



<https://github.com/Penglai-Enclave/PenglaiZone>

**GitHub - Penglai-Enclave/PenglaiZone: PenglaiZone is a project that aims to support the privileged z**

PenglaiZone is a project that aims to support the privileged zone in Trusted...

PenglaiZone是对标Arm TrustZone的可信计算架构实现，能够支持运行多个TEE OS，远程验证、安全启动等相关功能。PenglaiZone提供了static domain以及dynamic domain两种隔离机制，实现了硬件物理资源的强隔离。

## 开源计划：

- a. 基于opensbi domain机制的裸金属机密计算架构
  - i. 基于Starfive Versionfive 1代开发板的Normal Linux + Secure Linux的双系统裸金属可信计算架构方案：已完成
  - ii. 基于QEMU的裸金属计算架构PoC验证：2024年第一季度
- b. 基于UEFI standaloneMM的安全启动（Intel, starfive）：
  - i. 在QEMU平台上UEFI standaloneMM的PoC实现：已完成
  - ii. 实现符合RPMI标准的SPM（secure partition manager）：预计2023年10月完成
  - iii. 基于Starfive Versionfive 2开发板的完整的安全启动流程：预计2023年11月完成
- c. RISC-V Secure partition manager + TEEOS
  - i. 扩展opensbi中的domain机制，增加上下文的切换与中断隔离：预计2023年第四季度完成+逐步更新到opensbi主线
  - ii. 支持Chcore（IPADS实验室可信操作系统）作为TEEOS运行在penglaiZone架构中：预计2024年第二季度完成
  - iii. 纯软件版本IOPMP防御机制实现：预计2024年第一季度

## 2. 蓬莱TEE九月仓库更新汇总

### Penglai-PMP/sPMP

#### 1. opensbi版本支持更新至opensbi1.2

截止2023年9月，[Penglai-Enclave-sPMP](#)完成了Penglai Enclave support针对opensbi 0.9/1.0/1.2 的适配。

#### 2. openEuler版本支持升级至23.03

[Penglai-Enclave-sPMP](#)新增了对Enclave Driver的修改，实现Penglai Enclaved对基于kernel-6.X的openEuler23.03版本的支持。

最新的修改和运行说明文档已经更新到Penglai-Enclave-sPMP仓库中。

<https://github.com/Penglai-Enclave/Penglai-Enclave-sPMP>

### Penglai-Zone

#### 1. PenglaiZone 的[双系统裸金属可信计算架构方案](#)已完成。采用静态domain机制，实现在Starfive Visionfive1开发板上同时启动Normal Linux + Secure Linux，支持Secure Linux镜像的安全启动、远程验证。

#### 2. 基于UEFI standaloneMM的安全启动

- a. 以OpenSBI domain为基础，实现动态domain，包括上下文切换及domain切换，完成了Qemu平台上和Visionfive2上的开发和测试，目前[文档](#)只包含Qemu部分。
- b. 与Intel共同确定了UEFI standaloneMm所需的接口修改，与基于CoVE的修改保持一致，代码已进入edk2-staging分支，[整体进展同步到RISE社区](#)。
- c. 完成了符合RPMI 标准的SPM (secure partition manager) 的[PoC code](#)，将PenglaiZone的动态domain机制面向RPMI标准重构，形式上与ATF SPM类似，以支持RISC-V上的MM services (即standaloneMm)。完成多轮code clean up，目前正提交OpenSBI 社区讨论。