

操作系统实验二

本实验包含四个实验，即《自制 OS 实验》、《openEuler 实验》、《OpenHarmony 操作系统实验》和开源安全奖励计划或其他项目/竞赛（单独联系老师），大家任选其一完成即可。

《自制 OS 实验》主要面向底层，从零开始写一个通用型的操作系统，可以帮助同学们从底层深刻理解操作系统的底层工作原理。此实验的资料比较丰富，同学们可以参考提供的链接。

《openEuler 实验》主要是面向国产操作系统 openEuler 的实验，考察同学们对操作系统框架的整体理解以及实操能力。该实验要求同学们能够从零安装 openEuler 操作系统，采用重新编译源码的方式将内核更新至最新版，并且完成一些基础的实验。

《OpenHarmony 实验》主要是面向国产操作系统 OpenHarmony 的实验，因为 OpenHarmony 较为复杂，所以本实验手册附录部分该系统做了简要的介绍，同学们也可以自行到官方网站上搜索相应的材料。本实验考察同学们对操作系统框架的整体理解以及实操能力，要求同学们能够对 OpenHarmony 操作系统有基本的理解，并且可以编译 OpenHarmony 系统源码，最后在 QEMU 硬件模拟器中模拟 OpenHarmony 操作系统的运行。

如果有同学对对开源安全奖励计划或其他项目/竞赛感兴趣，可以单独联系老师，我们讨论细节后，报名并完成相应的项目/竞赛可以免除该实验。

考核标准

1. 该实验满分 12 分。
2. 《自制 OS 实验》中，能用 U 盘或在虚拟机上完成开机启动，并实现任意一个功能，并提交完整输出成果，即可得到合格成绩，即 $12 \times 60\%$ ；在此基础上，每多完成一个功能，可获 $12 \times 20\%$ 成绩。
3. 《openEuler 实验》中，完成 openEuler 操作系统的安装和内核更新（源代码更新方式）得 $12 \times 60\%$ ；在此基础上，每多完成一个功能，可获 $12 \times 10\%$ 成绩。此外，如果可以修复一个 CVE 漏洞，并提交到开源官方，直接满分。
4. 《OpenHarmony 实验》中，完成 OpenHarmony 操作系统的编译（得到 OHOS image 镜像文件）得合格成绩，即 $12 \times 60\%$ ；采用 QEMU 成功运行 OHOS 得 $12 \times 100\%$ ；
5. 实验可由 1~3 人组队完成，得分成绩按照文档和 PPT 中每个成员的分工百分比分配，所以同学们在提交的文档中，一定要说明自己的工作量。例如：
姓名：xxx 班级：xxx 学号：xxx 分工：60%
姓名：xxx 班级：xxx 学号：xxx 分工：40%

自制 OS 实验

- 1. **实验说明：**通过查找资料，小组完成一个自制 OS，要求能够用 U 盘或在虚拟机上完成启动，并实现一个（含）以上自行拟定的功能，例如：启动后输出显示预先设定的字符串；读出硬盘数据；开启内存分页机制；内存管理操作；进程操作；线程操作；锁。
- 2. **输出成果：**设计文档、测试文档、源代码、小组实验报告；实验介绍 PPT。
- 3. **注意事项：**必须在文档和 PPT 中写出每个成员的分工、实验过程（时间和对应的成果）、问题及解决方案。
- 4. **参考资料：**
[1] 自制 os 极简教程 1：写一个操作系统有多难，
<https://www.cnblogs.com/flashsun/p/13969254.html>

该仓库未指定开源许可证，未经作者的许可，此代码仅用于学习，不能用于其他用途。

代码参考：<https://gitee.com/sunym1993/flash-4th-os.git>

[2] 自己制作一个简单的操作系统，
<https://www.cnblogs.com/Cherrison-Time/p/11590693.html>

openEuler 实验

- 1. **实验说明：**
 - a) 采用虚拟机 Vmware 完成 openEuler 操作系统的安装，安装版本为 20.03-TLS，iso 镜像从 https://mirror.iscas.ac.cn/openeuler/openEuler-20.03-LTS/ISO/x86_64/openEuler-20.03-LTS-x86_64-dvd.iso 镜像源下载；安装操作系统后，（1）请创建一个可以彰显自己小组信息的用户名（可以选择一位同学的姓名和学号组合，例如图 1 中的 bupt-os-zhangsan20108021234），否则只能获得该实验步骤的一半分数；（2）请执行 `uname -a` 指令，并将截图放到实验报告中；（3）请执行 `getconf PAGESIZE` 指令，查看 openEuler 的分页大小。

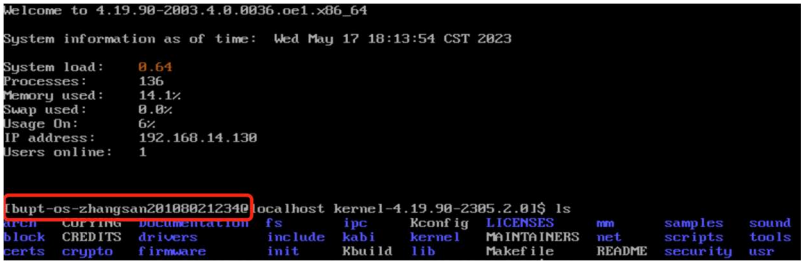


图 1.用户名示例

- b) 采用重新编译源代码的方式将内核更新至最新版。具体而言，下载最新版本的 openEuler 内核源码，见 <https://gitee.com/openeuler/kernel/releases> 页面中提交 ID 为 5dac66def453ae9578ba2d64d820fedbe7ac2181 的内核源码 zip 包或者 tar.gz 包，

详见图 2。

4.19.90-2405.5.0

2024-05-29 09:29

最新

5d6c6dd

对比

openEuler 20.03 update 4.19.90-2405.5.0

zhangchangzhong

1TASK

4.19.90-2405.4.0~1...4.19.90-2405.5.0

TASK	COMMIT
bugzilla: #19RFET:CVE-2023-52818	48dbe0ca04ac drm/amd: Fix UBSAN array-index-out-of-bounds for SMU7
bugzilla: #19RE4X:CVE-2023-52817	181a46bb998e drm/amdgpu/bugs: fix error code when smc register accessors are NULL 1365c38a021d drm/amdgpu: Fix a null pointer access when the smc_rreg pointer is NULL
bugzilla: #19R4C8:CVE-2021-47269	14ed5f93fbb0 usb: dwc3: ep0: fix NULL pointer exception
bugzilla: #19Q970:CVE-2024-35806	d2ded74ea35b soc: fsl: qbman: Always disable interrupts when taking cgr_lock
bugzilla: #19RE1F:CVE-2023-52835	9181cc5daf25 perf/core: Bail out early if the request AUX area is out of bound

图 2. 内核源码

- c) 重新编译后，安装内核，然后执行 `uname -a` 指令，并将截图放到实验报告
- d) 更新内核至最新后，参考 https://blog.csdn.net/gq_46744173/article/details/122199462，完成基础操作系统实验，例如内核模块编程、内存管理、进程管理、中断实验、设备管理等。
- e) 尝试解决系统里的 bug 或者 CVE 漏洞

开源项目 > 其他开源 > 操作系统

G.P

openEuler/kernel

Watch 427

Star 1.5K

Fork 1.6K

</> 代码

Issues 1370

Pull Requests 3140

Wiki

统计

流水线

服务

全部

搜索 Issue

看板

里程碑

+ 新建 Issue

全部

开启的 1307

进行中 59

已完成 5197

已关闭 132

创建者

负责人

标签

项目

里程碑

优先级

排序

scsi building errors, BLIST_IGN_MEDIA_CHANGE/BLIST_NO_VPD_SIZE undeclared

sig/Kernel

DEFECT/UNFIXED

#IBUHY9

qeliangtanq

2

负责人: CTC-Xibo.Wang

24分钟前

网络CVE合作共享

sig/Kernel

#IBUFEE

zhangshuqi

2

13小时前

Some trivial cleanups for shmem

sig/Kernel

#IBUAH1

王栋

1

19小时前

[olk 6.6] 支持 hibmcge驱动一组特性patch

sig/Kernel

#IBU56J

陈浩

1

1天前

百虚拟机开发，基础性能线性度>80%需求未达标

sig/Kernel

DEFECT/UNFIXED

#IBUZY1

Tenqu

2

负责人: zhaolichang

1天前

[OLK-6.6] add support TLBI in HIP12

sig/Kernel

#IBTXV2

yiq

1

2天前

[OLK 5.10] X2AVIC feature backport

sig/Kernel

#IBTVRA

mohanav

1

2天前

Minimize xa_node allocation during xarry split

sig/Kernel

#IBTUCE

王栋

1

2天前

OLK-6.6 6.11 sched/psi 优化补丁回合

sig/Kernel

#IBTTV4

koishimind

1

2天前

OLK-6.6 6.13 idle task 优化补丁回合

sig/Kernel

#IBTTFS

koishimind

1

2天前

OLK6.6补丁回合: pv spinlock特性

sig/Kernel

#IBTO64

李树森

1

3天前

CVE-2025-21859: USB: gadget: f_midi: f_midi_complete to call queue_work

sig/Kernel

DEFECT/UNFIXED

图 3. 开放问题

开源项目 > 其他开源 > 操作系统

src-openEuler/kernel

Watch 108 Star 69 Fork 291

代码 Issues 111 Pull Requests Wiki 统计 流水线 服务

Issues / 详情

CVE-2024-35806

已完成 #190970 CVE和安全问题 openeuler-ci-bot 待检查 创建于 2024-05-17 22:38

一、漏洞信息

漏洞编号: CVE-2024-35806

漏洞归属组件: kernel

漏洞归属的版本: 4.19.140.4,19.194.4,19.90.5,10.0.6.1,0.6.1,14.6.1,19.6.1,5.6.1,6.6.1,8.6.4,0.6.6.0

CVSS V3.0分值:

BaseScore: 0.0 None

Vector: CVSS: 3.0/

漏洞简述:

In the Linux kernel, the following vulnerability has been resolved:soc: qbman: Always disable interrupts when taking cgr_locksmp_call_function_single disables IRQs when executing the callback. Toprevent deadlocks, we must disable IRQs when taking cgr_lock elsewhere.This is already done by qman_update_cgr and qman_delete_cgr; fix theother lockers.

漏洞公开时间: 2024-05-17 22:15:14

漏洞创建时间: 2024-05-17 14:38:31

漏洞详情参考链接: <https://nvd.nist.gov/vuln/detail/CVE-2024-35806>

更多参考(点击展开)

漏洞分析指导链接: <https://gitee.com/openeuler/cve-manager/blob/master/cve-vulner-manager/doc/md/manual.md>

漏洞数据来源:

openBrain开源漏洞感知系统

漏洞补丁信息:

详情(点击展开)

二、漏洞分析结构反馈

影响性分析说明:

In the Linux kernel, the following vulnerability has been resolved:fs: qbman: Always disable interrupts when taking cgr_locksmp_call_function_single disables IRQs when executing the callback. Toprevent deadlocks, we must disable IRQs when taking cgr_lock elsewhere.This is already done by qman_update_cgr and qman_delete_cgr; fix theother lockers.

openEuler评分: 5.5

Vector: CVSS: 3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

受影响版本排查(受影响/不受影响):

- 1.openEuler-20.03-LTS-SP4(4.19.90):受影响
- 2.openEuler-22.03-LTS-SP1(5.10.0):受影响
- 3.openEuler-22.03-LTS-SP3(5.10.0):受影响
- 4.openEuler-22.03-LTS-SP4(5.10.0):受影响
- 5.master(6.6.0):不受影响

状态

已完成

负责人

sanglipeng

项目

未立项任务

Pull Requests

- soc: fs: qbman: Always disable interrupts when taking cgr_lock
- soc: fs: qbman: Always disable interrupts when taking cgr_lock
- [sync] PR-8060: soc: fs: qbman: Always disable interrupts when taking cgr_lock
- [sync] PR-8060: soc: fs: qbman: Always disable interrupts when taking cgr_lock
- [sync] PR-8060: soc: fs: qbman: Always disable interrupts when taking cgr_lock
- release 4.19.90-2405.5.0
- release 4.19.90-2405.5.0
- release 5.10.0-2010.0
- release 5.10.0-2010.0
- release 5.10.0-2010.0
- release 5.10.0-153.56.0
- release 5.10.0-136.77.0
- release 5.10.0-60.139.0

关联的 Pull Requests 被合并后可能会关闭此 issue

预计工期 (小时)

0

开始日期 - 截止日期

2024-05-17 - 2024-06-16

置顶选项

不置顶

优先级

次要

图 4. 已解决的漏洞信息

2. **输出成果:** (1) 小组实验报告: 实验报告中必须包含上述实验的细致步骤(实现步骤越详细越好)以及必要的截图;(2) 小组实验介绍 PPT: 实验中遇到各种问题, 以及最终小组成员是如何解决的(最好将对应的资料和网页链接写出来);。
3. **注意事项:** 必须在文档和 PPT 中写出每个成员的分工、实验过程(时间和对应的结果)、问题及解决方案。
4. **参考资料:**

[1] <https://blog.csdn.net/hiascend/article/details/128579458>

[2]

https://blog.csdn.net/m0_56602092/article/details/118604262?utm_medium=distribute.pc_relevant.none-task-blog-2~default~baidujs_baidulandingword~default-0-118604262-blog-128579458.235^v36^pc_relevant_anti_vip&spm=1001.2101.3001.4242.1&utm_relevant_in_dex=3

[3] <http://mirrors.aliyun.com/openeuler/openEuler-20.03LTS/?spm=a2c6h.25603864.0.0.e5ae71a8Fexn4l>

[4] <https://www.openeuler.org/zh/mirror/list/>

[5] <https://zhuanlan.zhihu.com/p/423624818>

[6] <https://blog.csdn.net/xuyuefei1988/article/details/8635539>

[7] <https://blog.csdn.net/alwaysbefine/article/details/123363999>

[8] https://blog.csdn.net/weixin_56483756/article/details/124185212

[9] <https://blog.csdn.net/xcyjxy2021/article/details/123341308>

- [10] https://blog.csdn.net/qq_45945548/article/details/120557041
- [11] https://blog.csdn.net/weixin_45467056/article/details/112930163
- [12] https://blog.csdn.net/qq_36393978/article/details/117816425

OpenHarmony 操作系统实验

实验内容

使用 QEMU 硬件模拟器运行开源鸿蒙 OpenHarmony4.x 操作系统

实验步骤提示

(1) 安装 VMware WorkStation 的安装

(2) 在 Vmware 中安装 ubuntu 20.04 系统

推荐使用华为镜像的 ubuntu 操作系统，即 ubuntu-20.04.6-desktop-amd64.iso 文件地址为：repo.huaweicloud.com/ubuntu-releases/20.04/

由于操作系统源码较大，请预留足够的空间，建议给 `ubuntu` 分配 100G 以上的磁盘空间。文档参考：

[zh-cn/device-dev/quick-start/quickstart-ide-env-ubuntu.md](https://gitee.com/openharmony/docs/blob/master/zh-cn/device-dev/quick-start/quickstart-ide-env-ubuntu.md) · [OpenHarmony/docs](https://gitee.com/openharmony/docs) - Gitee.com

(3) 安装鸿蒙 QEMU 硬件模拟器

鸿蒙 QEMU 的下载地址为 [device_qemu: Hardware platforms emulation by QEMU | QEMU 模拟不同的硬件单板 \(gitee.com\)](#)。当然一些厂商也为自己的硬件设备开发了相应的 QEMU，相应的地址为 [OpenHarmony/vendor_ohemu - 码云 - 开源中国 \(gitee.com\)](#)，同学们可以按需采用。

(4) 下载编译鸿蒙系统源码，并生成操作系统镜像

a) 下载源码

下载方式 1: 完整版本的 openHarmony 系统较大 (30G 左右), 请安装 ubuntu 操作系统时预留足够的空间。最新版的操作系统源码如下:
<https://repo.huaweicloud.com/harmonyos/os/4.1-Release/code-v4.1-Release.tar.gz>。下载完成会, 解压到相应的目录下, 进行编译

下载方式 2 (建议采用): 使用 repo+ssh 直接从 gitee 下载, 具体步骤详见 [zh-cn/device-dev/get-code/sourcecode-acquire.md · OpenHarmony/docs - Gitee.com](#)

注意：repo 在 python2 运行不了，请改为 python3 就解决

如果采用方式 2 下载，在 Ubuntu 系统下，下载完整代码，采用 repo 进行初始化时，可以用

```
repo init -u git@github.com:openharmony/manifest.git -b master --no-repo-verify
```

如果采用方式 2 下载，可以选择下载部分代码，例如，采用的 chipset 时 qemu，并且只针对轻量系统（mini 系统），则可以用

```
repo init -u https://gitee.com/openharmony/manifest -b master -m chipsets/qemu.xml -g ohos:mini
```

具体指令请参考：<https://blog.csdn.net/qq582880551/article/details/136330246>

b) 编译源码

根据文档，搭建 docker 编译环境

[zh-cn/device-dev/get-code/gettools-acquire.md · OpenHarmony/docs - Gitee.com](https://gitee.com/openharmony/docs/zh-cn/device-dev/get-code/gettools-acquire.md)

根据系统类型，执行行营的编译指令。

- 轻型系统

```
python3 build.py -p qemu_mini_system_demo@ohemu
```

- 小型系统

```
python3 build.py -p qemu_small_system_demo@ohemu
```

注意：编译工具和开发板都分为轻型、小型、标准，必须属于同一种类型，否则编译时各种报错

编译完成后会生成操作系统镜像 OHOS_Image，供 QEMU 加载使用。

（5）使用 QEMU 加载并运行生成的操作系统镜像

例如，如果选择 x86_64_virt 平台，使用 QEMU 启动操作系统的过程请参考：

https://gitee.com/openharmony/device_qemu/tree/master/x86_64_virt/linux

注意事项：

（1）因为运行 openHarmony 操作系统需要相应的硬件设备，因此，本实验采用 QEMU 硬件模拟器模拟硬件设备，并将自己手动编译好的 openHarmony 操作系统 image“安装到”QEMU 所模拟出的硬件设备上运行。鸿蒙 QEMU 的下载地址为：

[device_qemu: Hardware platforms emulation by QEMU | QEMU 模拟不同的硬件单板 \(gitee.com\)](https://gitee.com/openharmony/device_qemu)

目前 QEMU 模拟器支持 arm_mps2_an386、arm_virt、esp32、riscv32_virt、x86_64_virt、SmartL_E802 等开发板的模拟，因此同学们可以选择上述任意一款开发版对应的 QEMU 作为操作系统的硬件使用，详见下图。

编译形态整体说明

在编译过程中，需要根据实际需求选择不同的编译形态。单击下表中的链接可获取具体产品配置，从而了解

表1 编译构建支持的产品列表

编译形态	开发板	主芯片	内核	系统类型
neptune100	neptune100	winnermicro	liteos_m	mini
rk3568	rk3568	rockchip	linux	standard
rk3568_mini_system	rk3568	rockchip	linux	standard
bearpi_hm_micro	bearpi_hm_micro	stm32mp1xx	liteos_a	small
bearpi_hm_nano	bearpi_hm_nano	hi3861v100	liteos_m	mini
wifiot_hispark_pegasus	hispark_pegasus	hi3861v100	liteos_m	mini
ipcamera_hispark_aries	hispark_aries	hi3518ev300	liteos_a	small
ipcamera_hispark_taurus	hispark_taurus	hi3516dv300	liteos_a	small
ipcamera_hispark_taurus_linux	hispark_taurus	hi3516dv300	linux	small
hispark_taurus_standard	hispark_taurus	hi3516dv300	linux	standard
watchos	hispark_taurus	hi3516dv300	linux	standard
hispark_phoenix	hispark_phoenix	hi3751v350	linux	standard
hispark_taurus_mini_system	hispark_taurus	hi3516dv300	liteos_a	mini
hispark_pegasus_mini_system	hispark_pegasus	hi3861v100	liteos_m	mini
gr5515_sk_iotlink_demo	gr5515_sk	gr551x	liteos_m	mini
gr5515_sk_xts_demo	gr5515_sk	gr551x	liteos_m	mini
wifi_demo	dev_wifi_a	asr582x	liteos_m	mini
xts_demo	dev_wifi_a	asr582x	liteos_m	mini
display_demo	v200zr	bes2600	liteos_m	mini
xts_demo	v200zr	bes2600	liteos_m	mini
iotlink_demo	v200zr	bes2600	liteos_m	mini
mini_distributed_music_player	v200zr	bes2600	liteos_m	mini
niobe407	niobe407	stm32f4xx	liteos_m	mini
qemu_mini_system_demo	arm_mps2_an386	qemu	liteos_m	mini
qemu_csky_mini_system_demo	SmartL_E802	qemu	liteos_m	mini
qemu_cm55_mini_system_demo	arm_mps3_an547	qemu	liteos_m	mini
qemu_xtensa_mini_system_demo	esp32	qemu	liteos_m	mini
qemu_riscv_mini_system_demo	riscv32_virt	qemu	liteos_m	mini
qemu_ca7_mini_system_demo	arm_virt	qemu	liteos_a	small
qemu_small_system_demo	arm_virt	qemu	liteos_a	small
qemu_arm_linux_min	qemu-arm-linux	qemu	linux	standard
qemu_arm_linux_headless	qemu-arm-linux	qemu	linux	standard
iotlink_demo	cst85_wblink	chipsea	liteos_m	mini
dsoftbus_demo	cst85_wblink	chipsea	liteos_m	mini
xts_demo	cst85_wblink	chipsea	liteos_m	mini

(2) 请同学们不要在自己的物理主机上做实验（为了保护同学们的电脑），同学们可以下载 VMware 虚拟机，然后安装 ubuntu 20.04 操作系统，所有的实验都在 ubuntu 20.04 中完成。

1. 实验说明：

- a) 采用虚拟机 VMware 完成 Ubuntu 操作系统的安装，安装操作系统后，（1）请创建一个可以彰显自己小组信息的用户名（可以选择一位同学的姓名和学号组合，例如图 1 中的 bupt-os-zhangsan20108021234），否则只能获得该实验步骤的一半分数；


```
Welcome to 4.19.90-2003.4.0.0036.oc1.x86_64
System information as of time: Wed May 17 18:13:54 CST 2023
System load: 0.64
Processes: 136
Memory used: 14.1%
Swap used: 0.0%
Usage On: 6%
IP address: 192.168.14.130
Users online: 1

bupt-os-zhangsan201808212340 localhost kernel-4.19.90-2385.2.01$ ls
arch  corring  documentation  fs  ipc  kconfig  LICENSES  mm  samples  sound
block  CREDITS  drivers  include  kabi  kernel  MAINTAINERS  net  scripts  tools
certs  crypto  firmware  init  Kbuild  lib  Makefile  README  security  usr
```

图 1. 用户名示例

- b) 本实验全部采用 QEMU，因此无需指定特定的硬件系统，但需要在实验报告中指明（1）所采用 QEMU 版本；（2）所要编译的系统是轻型、小型或标准系统
- c) 鸿蒙操作系统有多种编译方式，可以不采用 docker 的方式进行编译。无论采用哪种编译方式，都要进写一下详细的实验步骤。

2. **输出成果：**（1）小组实验报告：实验报告中必须包含上述实验的细致步骤（实现步骤越详细越好）及其相应的指令，关键步骤的截图也请写到实验报告中；（2）小组实验介绍 PPT：实验中遇到各种问题，以及最终小组成员是如何解决的（最好将对应的资料和网页链接写出来）；。

3. **注意事项：**必须在文档和 PPT 中写出每个成员的分工、实验过程（时间和对应的结果果）、问题及解决方案。

4. 参考资料：

[1] [OpenAtom OpenHarmony 教育资源仓: OpenAtom OpenHarmony 项目教育资源仓是可自由访问的，开放许可的培训课程、技术手册、解决方案、成功案例等的集合，可用于 OpenHarmony 教学，学习和评估以及研究目的。\(gitee.com\)](#)

[2] [基于 Ubuntu20.04 搭建 OpenHarmony v3.0.6 的 qemu 仿真环境 openharmony qemu-CSDN 博客](#)

[3] [Openharmony 鸿蒙内核编译及 qemu 运行过程问题记录 openharmony 编译内核-CSDN 博客](#)

[4] [3 开源鸿蒙 OpenHarmony4.1 源码下载、编译，生成 OHOS Image 可执行文件的最简易流程 openharmony-4.1-release 下载-CSDN 博客](#)

[5] [运行在 Qemu 上的鸿蒙内核 Liteos-m - 哔哩哔哩 \(bilibili.com\)](#)

[6] [在 qemu 上体验芯来 RISC-V 处理器运行鸿蒙 LiteOS-M 内核 专栏 RISC-V MCU 中文社区 \(riscv-mcu.com\)](#)

[7] [arm_virt/liteos_a/README_zh.md · OpenHarmony/device qemu - Gitee.com](#)

[8] [华为开源镜像站 软件开发服务 华为云 \(huaweicloud.com\)](#)

[9] [zh-cn/device-dev/kernel/kernel-overview.md · OpenHarmony/docs - Gitee.com](#)

附录

鸿蒙操作系统基本介绍

OpenHarmony 整体遵从分层设计，从下向上依次为：内核层、系统服务层、框架层和应用层。系统功能按照“系统 > 子系统 > 组件”逐级展开，在多设备部署场景下，支持根据实际需求裁剪某些非必要的组件。OpenHarmony 技术架构如下所示：



docs.openharmony.cn/pages/v4.0/zh-cn/OpenHarmony-Overview_zh.md/

内核层

- **内核子系统**：采用多内核（Linux 内核或者 LiteOS）设计，支持针对不同资源受限设备选用适合的 OS 内核。内核抽象层（KAL，Kernel Abstract Layer）通过屏蔽多内核差异，对上层提供基础的内核能力，包括进程/线程管理、内存管理、文件系统、网络管理和外设管理等。
- **驱动子系统**：驱动框架（HDF）是系统硬件生态开放的基础，提供统一外设访问能力和驱动开发、管理框架。

一次开发，多端部署

OpenHarmony 提供用户程序框架、Ability 框架以及 UI 框架，能够保证开发的应用在多终端运行时保证一致性。一次开发、多端部署。

多终端软件平台 API 具备一致性，确保用户程序的运行兼容性。

- 支持在开发过程中预览终端的能力适配情况（CPU/内存/外设/软件资源等）。
- 支持根据用户程序与软件平台的兼容性来调度用户呈现。

统一 OS，弹性部署

OpenHarmony 通过组件化和组件弹性化等设计方法，做到硬件资源的可大可小，在多种终端设备间，按需弹性部署，全面覆盖了 ARM、RISC-V、x86 等各种 CPU，从百 KiB 到 GiB 级别的 RAM。

内核概述

内核简介

用户最常见到并与之交互的操作系统界面，其实只是操作系统最外面的一层。操作系统最重要的任务，包括管理硬件设备，分配系统资源等，我们称之为操作系统内在最重要的核心功能。而实现这些核心功能的操作系统模块，业界一般称之为操作系统“内核”。

实现原理

操作系统是位于应用和硬件之间的系统软件，向上提供易用的程序接口和运行环境，向下管理硬件资源。内核位于操作系统的下层，为操作系统上层的程序框架提供硬件资源的并发管理。

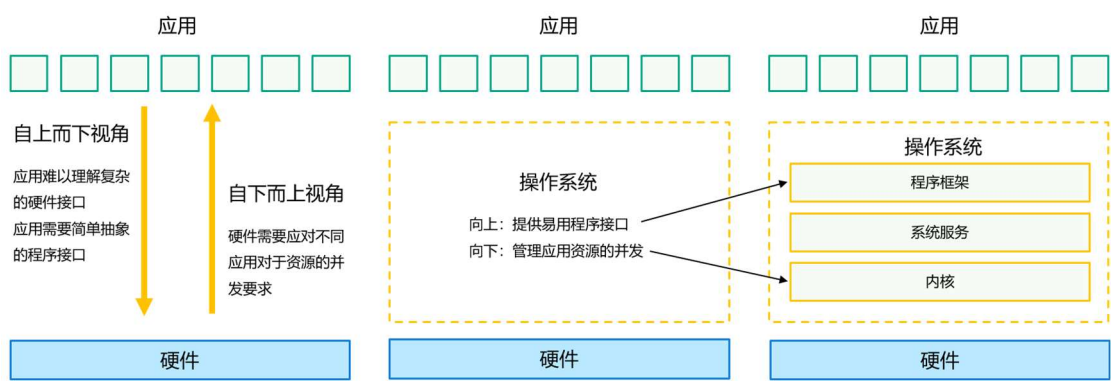


图 1 操作系统架构

多内核架构和基本组成

业界的内核有很多，但无论是什么内核，基本上有几个最重要的组成单元是每个内核均要具备的，分别是：

- 负责持久化数据，并让应用程序能够方便的访问持久化数据的“文件系统”。
- 负责管理进程地址空间的“内存管理”。
- 负责管理多个进程的“进程管理”或者“任务管理”。
- 负责本机操作系统和另外一个设备上操作系统通信的“网络”。

OpenHarmony 采用了多内核结构，支持 Linux 和 LiteOS，开发者可按不同产品规格进行选择使用。Linux 和 LiteOS 均具备上述组成单元，只是实现方式有所不同。多个内核通过 KAL（Kernel Abstraction Layer）模块，向上提供统一的标准接口。

内核子系统位于 OpenHarmony 下层。需要特别注意的是，由于 OpenHarmony 面向多种设备类型，这些设备有着不同的 CPU 能力，存储大小等。为了更好的适配这些不同的设备类型，内核子系统支持针对不同资源等级的设备选用适合的 OS 内核，内核抽象层（KAL，Kernel Abstract Layer）通过屏蔽内核间差异，对上层提供基础的内核能力。



图 2 OpenHarmony 架构图

不同内核适配的系统及设备类型

OpenHarmony 按照支持的设备可分为如下几种系统类型：

- 轻量系统（mini system） 面向 MCU 类处理器例如 Arm Cortex-M、RISC-V 32 位的设备，硬件资源极其有限，支持的设备最小内存为 128KiB，可以提供多种轻量级网络协议，轻量级的图形框架，以及丰富的 IOT 总线读写部件等。可支撑的产品如智能家居领域的连接类模组、传感器设备、穿戴类设备等。
- 小型系统（small system） 面向应用处理器例如 Arm Cortex-A 的设备，支持的设备最小内存为 1MiB，可以提供更高的安全能力、标准的图形框架、视频编解码的多媒体能力。可支撑的产品如智能家居领域的 IP Camera、电子猫眼、路由器以及智慧出行域的行车记录仪等。
- 标准系统（standard system） 面向应用处理器例如 Arm Cortex-A 的设备，支持的设备最小内存为 128MiB，可以提供增强的交互能力、3D GPU 以及硬件合成能力、更多控件以及动效更丰富的图形能力、完整的应用框架。可支撑的产品如高端的冰箱显示屏。
- OpenHarmony 针对不同量级的系统，使用了不同形态的内核。轻量系统、小型系统可以选用 LiteOS；小型系统和标准系统可以选用 Linux。其对应关系如下表：

表 1 系统关系对应表

系统级别	轻量系统	小型系统	标准系统
LiteOS-M	√	×	×
LiteOS-A	×	√	√
Linux	×	√	√

LiteOS-M

内核架构

OpenHarmony LiteOS-M 内核是面向 IoT 领域构建的轻量级物联网操作系统内核，具有小体积、低功耗、高性能的特点，其代码结构简单，主要包括内核最小功能集、内核抽象层、可选组件以及工程目录等，分为硬件相关层以及硬件无关层，硬件相关层提供统一的 HAL（Hardware Abstraction Layer）接口，提升硬件易适配性，不同编译工具链和芯片架构的组合分类，满足 AIoT 类型丰富的硬件和编译工具链的拓展。

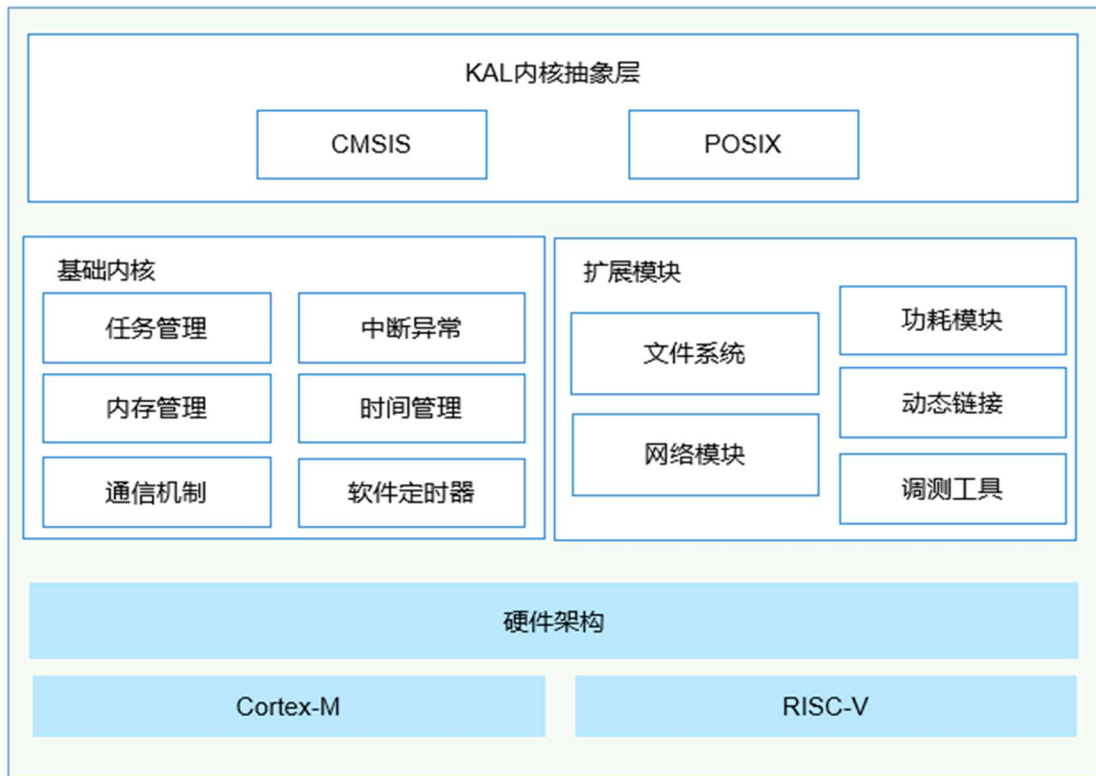


图 3 LiteOS-M 架构图

使用指导

LiteOS-M 使用指导请参见 LiteOS-M [内核概述](#)的“使用说明”章节。

LiteOS-A

内核架构

OpenHarmony 轻量级内核是基于 IoT 领域轻量级物联网操作系统 Huawei LiteOS 内核演进发展的新一代内核，包含 LiteOS-M 和 LiteOS-A 两类内核。LiteOS-M 内核主要应用于轻量系统，面向的 MCU（Microprocessor Unit）一般是百 K 级内存，可支持 MPU（Memory Protection Unit）隔离，业界类似的内核有 FreeRTOS 或 ThreadX 等；LiteOS-A 内核主要应用于小型系统，面向设备一般是 M 级内存，可支持 MMU（Memory Management Unit）隔离，业界类似的内核有 Zircon 或 Darwin 等。

为适应 IoT 产业的高速发展，OpenHarmony 轻量级内核不断优化和扩展，能够带给开发者友好的开发体验和统一开放的生态系统能力。轻量级内核 LiteOS-A 重要的新特性如下：

- 新增了丰富的内核机制：
 - 新增虚拟内存、系统调用、多核、轻量级 IPC（Inter-Process Communication，进程间通信）、DAC（Discretionary Access Control，自主访问控制）等机制，丰富了内核能力；
 - 为了更好的兼容软件和开发者体验，新增支持多进程，使得应用之间内存隔离、相互不影响，提升系统的健壮性。

- 引入统一驱动框架 HDF（Hardware Driver Foundation）

引入统一驱动框架 HDF，统一驱动标准，为设备厂商提供了更统一的接入方式，使驱动更加容易移植，力求做到一次开发，多系统部署。

- 支持 1200+标准 POSIX 接口

更加全面的支持 POSIX 标准接口，使得应用软件易于开发和移植，给应用开发者提供了更友好的开发体验。

- 内核和硬件高解耦

轻量级内核与硬件高度解耦，新增单板，内核代码不用修改。

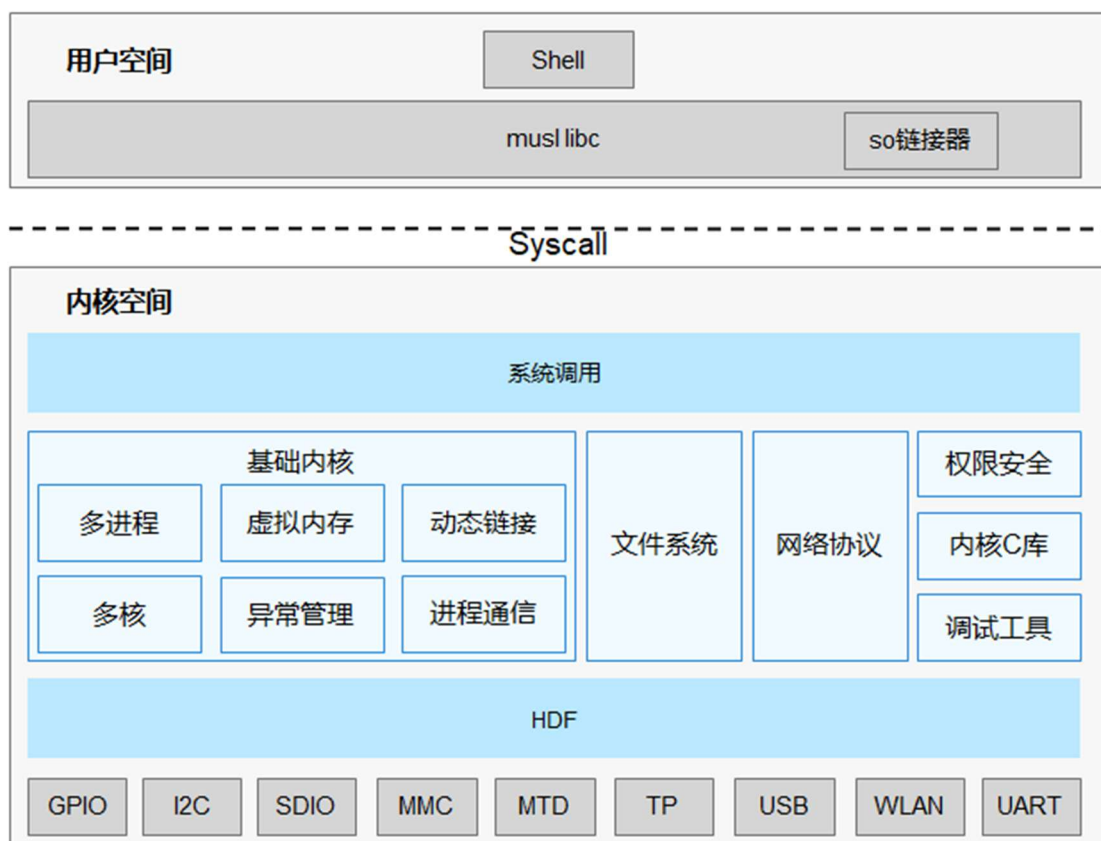


图 4 OpenHarmony LiteOS-A 内核架构图

使用指导

LiteOS-A 使用指导请参见 LiteOS-A [内核概述](#)的“使用说明”章节。

Linux

linux 内核概述

OpenHarmony 的 Linux 内核基于开源 Linux 内核 LTS 4.19.y / 5.10.y 分支演进，在此基线基础上，回合 CVE 补丁及 OpenHarmony 特性，作为 OpenHarmony Common Kernel 基线。针对不同的芯片，各厂商合入对应的板级驱动补丁，完成对 OpenHarmony 的基线适配。

Linux 社区 LTS 4.19.y 分支信息请查看 [kernel 官网](#)。

Linux 社区 LTS 5.10.y 分支信息请查看 [kernel 官网](#)。

内核的 Patch 组成模块，在编译构建流程中，针对具体芯片平台，合入对应的架构驱动代码，进行编译对应的内核镜像。所有补丁来源均遵守 GPL-2.0 协议。

内核增强特性

OpenHarmony 针对 linux 内核在 ESwap(Enhanced Swap)、关联线程组调度和 CPU 轻量级隔离做了增强。

Enhanced SWAP 特性

ESwap 提供了自定义新增存储分区作为内存交换分区的能力，并创建了一个常驻进程 zswapd 将 ZRAM 压缩后的匿名页加密换出到 ESwap 存储分区，从而能完全的空出一块可用内存，以此来达到维持 Memavailable 水线的目标。同时，配合这个回收机制，在整个内存框架上进行改进，优化匿名页和文件页的回收效率，并且使两者的回收比例更加合理以避免过度回收导致的 refault 问题造成卡顿现象。

关联线程组调度

关联线程组(related thread group)提供了对一组关键线程调度优化的能力，支持对关键线程组单独进行负载统计和预测，并且设置优选 CPU cluster 功能，从而达到为组内线程选择最优 CPU 运行并且根据分组负载选择合适的 CPU 调频点运行。

CPU 轻量级隔离

CPU 轻量级隔离特性提供了根据系统负载和用户配置来选择合适的 CPU 进行动态隔离的能力。内核会将隔离 CPU 上的任务和中断迁移到其他合适的 CPU 上执行，被隔离的 CPU 会进入 idle 状态，以此来达到功耗优化的目标。同时提供用户态的配置和查询接口来实现更好的系统调优。

使用指导

1. 合入 HDF 补丁 在 kernel/linux/build 仓中，按照 kernel.mk 中 HDF 的补丁合入方法，合入不同内核版本对应的 HDF 内核补丁：

```
$(OHOS_BUILD_HOME)/drivers/hdf_core/adapters/khdf/linux/patch_hdf.sh  
$(OHOS_BUILD_HOME) $(KERNEL_SRC_TMP_PATH) $(KERNEL_PATCH_PATH)  
$(DEVICE_NAME)
```

2. 合入芯片平台驱动补丁 以 Hi3516DV300 为例：

在 kernel/linux/build 仓中，按照 kernel.mk 中的芯片组件所对应的 patch 路径规则及命名规则，将对应的芯片组件 patch 放到对应路径下：

```
DEVICE_PATCH_DIR :=  
$(OHOS_BUILD_HOME)/kernel/linux/patches/${KERNEL_VERSION}/${DEVICE_NAME}_patch  
DEVICE_PATCH_FILE := $(DEVICE_PATCH_DIR)/$(DEVICE_NAME).patch
```

3. 修改自己所需要编译的 config 在 kernel/linux/build 仓中，按照 kernel.mk 中的芯片组件所对应的 patch 路径规则及命名规则，将对应的芯片组件 config 放到对应路径下：

```
KERNEL_CONFIG_PATH :=  
$(OHOS_BUILD_HOME)/kernel/linux/config/${KERNEL_VERSION}DEFCONFIG_FILE  
FILE := $(DEVICE_NAME)_$(BUILD_TYPE)_defconfig
```



须知： 由于 OpenHarmony 工程的编译构建流程中会拷贝 kernel/linux/linux-*. * 的代码环境后进行打补丁动作，在使用 OpenHarmony 的版本级编译命令前，需要 kernel/linux/linux-*. * 源代码环境。

根据不同系统工程，编译完成后会在 out 目录下的 kernel 目录中生成对应实际编译的内核，基于此目录的内核，进行对应的 config 修改，将最后生成的.config 文件 cp 到 config 仓对应的路径文件里，即可生效。