openEuler系列直播

可信计算：内核完整性度量

openEuler公众号

openEuler

课程目标

- 了解可信计算的前世今生
- 了解原生社区与openEuler中的内核完整性度量（IMA）
- 掌握在openEuler环境下部署IMA的方法

目录

01 可信计算的前世今生

- 什么是可信计算?
- 可信计算基本原理与技术族

什么是可信计算

什么是可信?

- **Trusted System**: 系统行为符合设计预期. System operates as **expected**, according to design and policy, doing what is required and not doing other things. [RFC4949]

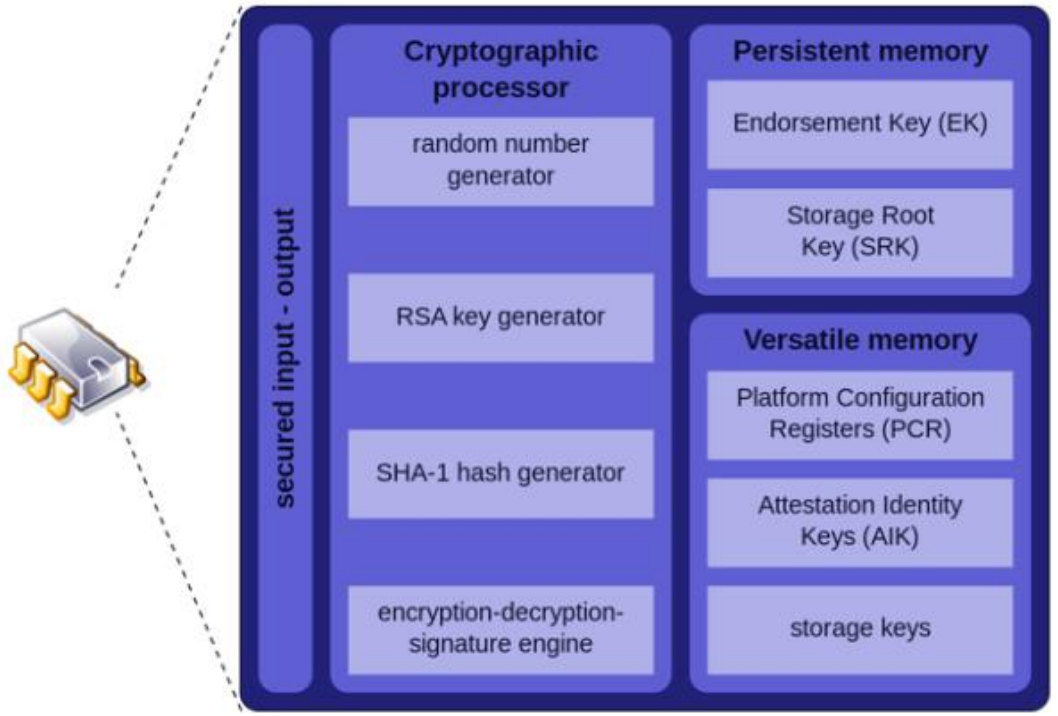
什么是可信计算?

- **Trusted Computing (广义)**：系统行为总是符合预期，并且**有硬件和软件提供保障**. the computer will consistently behave in expected ways, and those behaviors will be enforced by computer hardware and software[Chris Mitchell (2005). *Trusted Computing*].
- **Trusted Computing (TCG)**：**基于可信平台模块 (TPM)**，保护系统行为和完整性. TCG created the Trusted Platform Module cryptographic capability, which enforces specific behaviors and protects the system against unauthorized changes and attacks such as malware and root kits[TCG].

可信计算基本原理

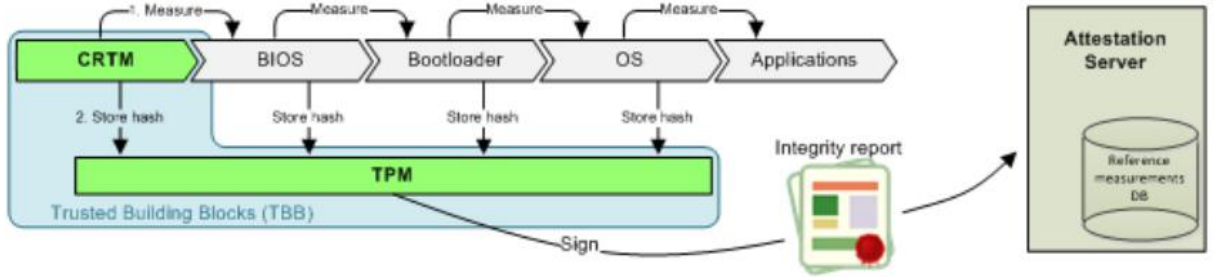
TPM：可信平台模块

- TPM 是可信计算平台的**信任根（TCB）**，是可信计算的核心模块。
- 通过将密钥和加解密引擎集成到 TPM 芯片中，为实现系统安全功能提供了安全的可信基点。
- PCR 存储方式是扩展递加存储，具有**单向性**，即根据 PCR 中的值反推消息和之前的任何信息是不可能的。



信任链与可信计算的实现

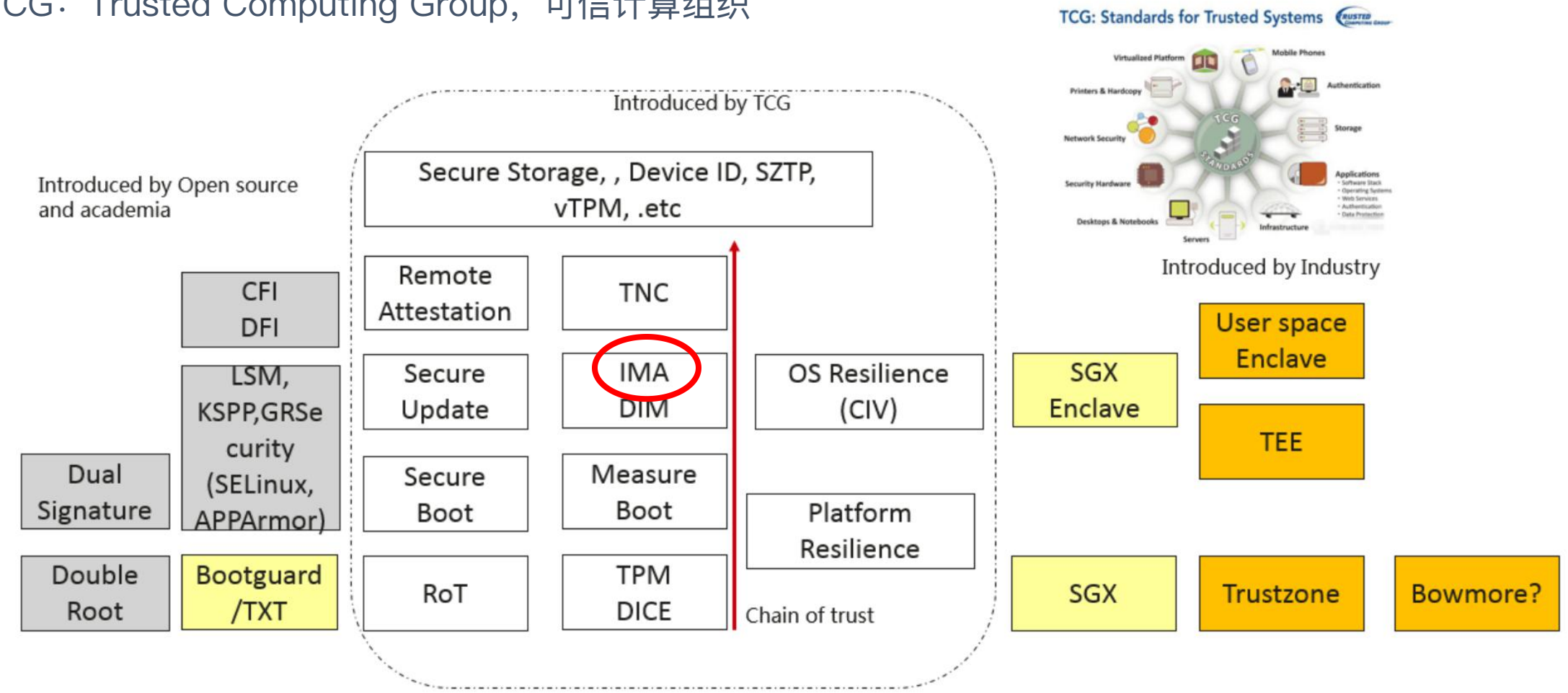
1. **建立信任链**：从信任根开始到硬件平台、操作系统，再到应用，一级信任一级，把信任扩展到整个计算机系统。
2. **标识身份**：模块内置 EK 身份证书，通过权威认证平台签发，证明芯片和系统的身份。
3. **保护密钥**：模块内置 SRK 存储根密钥，不能被外部访问，从而建立起一棵密钥保护树。



openEuler

可信计算技术族

TCG：Trusted Computing Group，可信计算组织



参考< TCG Guidance for Securing Network Equipment Using TCG Technology >

openEuler

快问快答赢T恤

下列哪项技术不属于可信计算的范畴?

A.IMA

B.Trustzone

C.SELinux

D.iSulad

02 走近内核完整性度量

- 内核完整性度量
- openEuler提供的IMA摘要列表扩展
- 总结：对比原生IMA特性与IMA摘要列表特性

openEuler

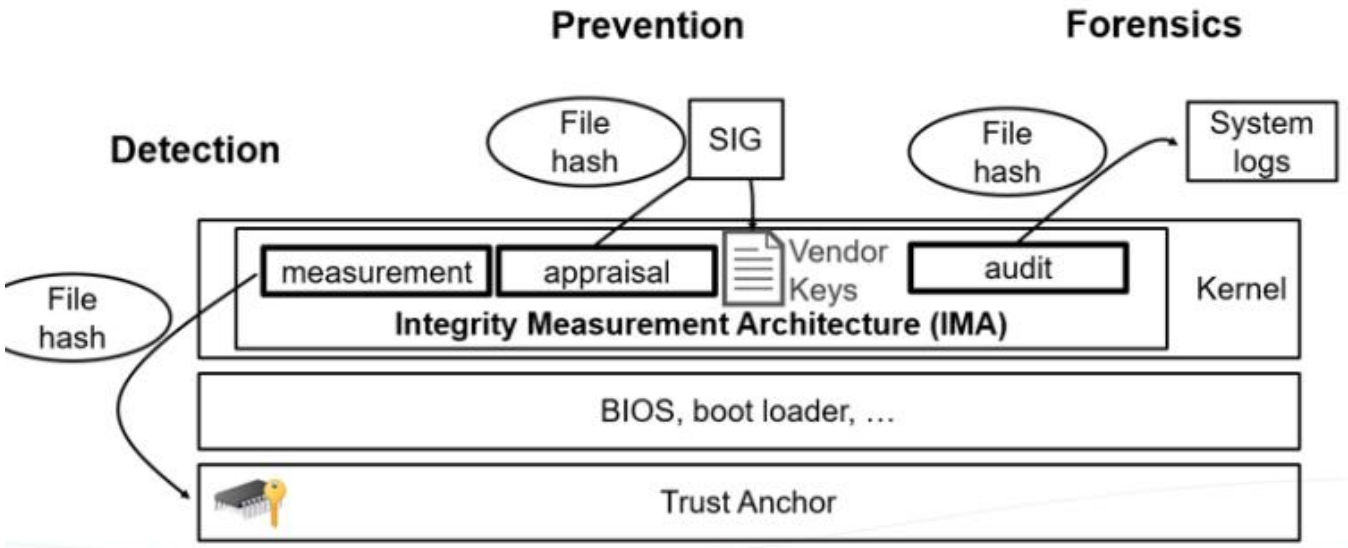
内核完整性度量（IMA）

IMA (Integrity Measurement Architecture)

- IBM 研究院于 2004 年提出完整性度量架构（IMA），基于 TPM 进行系统完整性度量。
- **IMA-measurement**：通过在内核中增加 IMA 模块，当应用程序/动态库/内核模块被加载时，度量文件和关键数据并扩展到 PCR10。
- **IMA-appraisal**：对 IMA 基础功能的扩展，将被评估文件内容的度量基准值存储在安全扩展属性 **security.ima** 中，在打开文件时将度量值与扩展属性中的基准值进行对比，如果不匹配，则拒绝该加载文件。
- **IMA-audit**：提供审计功能的日志模块。

EVM (Extended Verification Module)

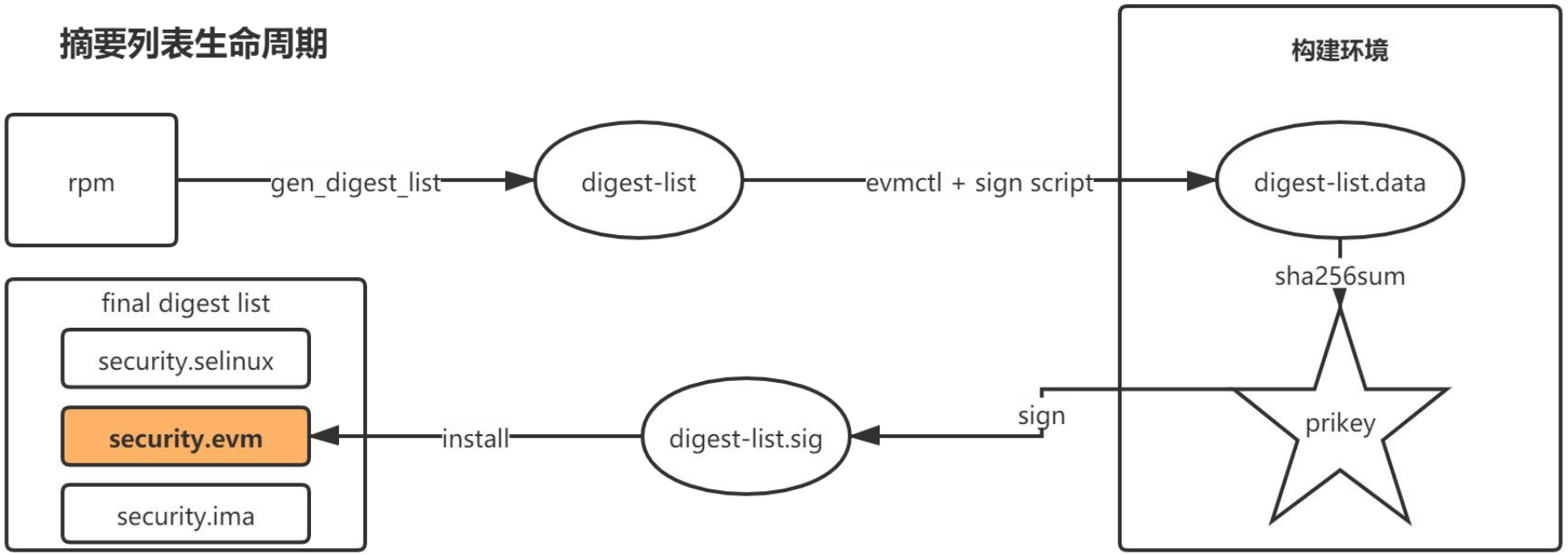
- 通过对安全扩展属性计算 HMAC 值，然后存储在 **security.evm** 中，提供对安装扩展属性的离线保护。



IMA摘要列表扩展：openEuler的思考（1/3）

Feature 1：构建时发布的参考值

- 为解决原生内核 IMA 初次部署操作复杂且信任链不完整的问题，openEuler 内核将参考值的生成统一放到**构建阶段**。
- **“摘要列表”（digest lists）**是一种特殊格式的二进制数据文件，它与 rpm 包一一对应，在构建过程中自动生成并打包到 rpm 包中（在 /etc/ima/digest_lists 目录下），记录了 rpm 包中受保护文件（即可执行文件和动态库文件）的哈希值列表。
- 构建环境下，摘要列表文件会被私钥签名，以保护其完整性。

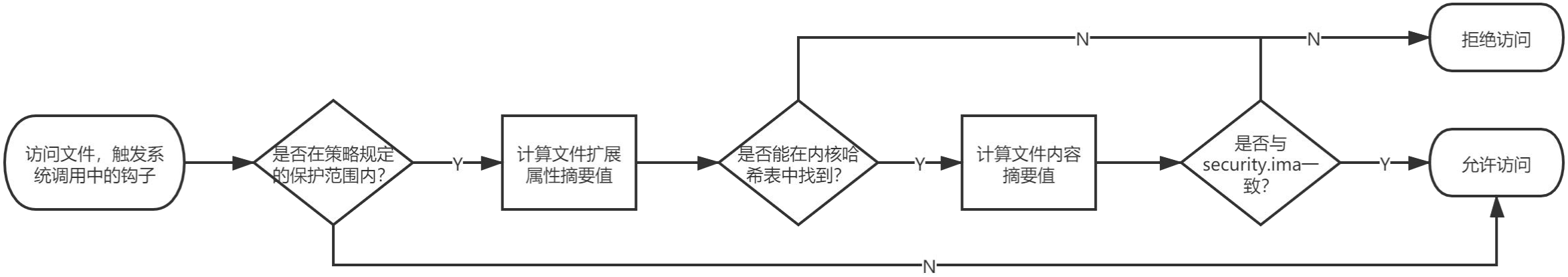


openEuler

IMA摘要列表扩展：openEuler的思考（2/3）

Feature 2：启动阶段验签导入所有参考值，并支持开箱即用

- 在 initramfs 阶段就完成所有摘要列表的导入，确保 systemd 起的每个进程都经过 IMA 校验 。
- 摘要列表在导入时需由内核中的公钥进行签名校验。
- 如果 ISO 中的内核启动参数默认配置打开了 IMA 开关，那么完成安装时所有摘要列表已被导入，无需重启。
- enforce 模式下，访问文件时发生了什么?



IMA摘要列表扩展：openEuler的思考（3/3）

Feature 3：随时随地更新参考值

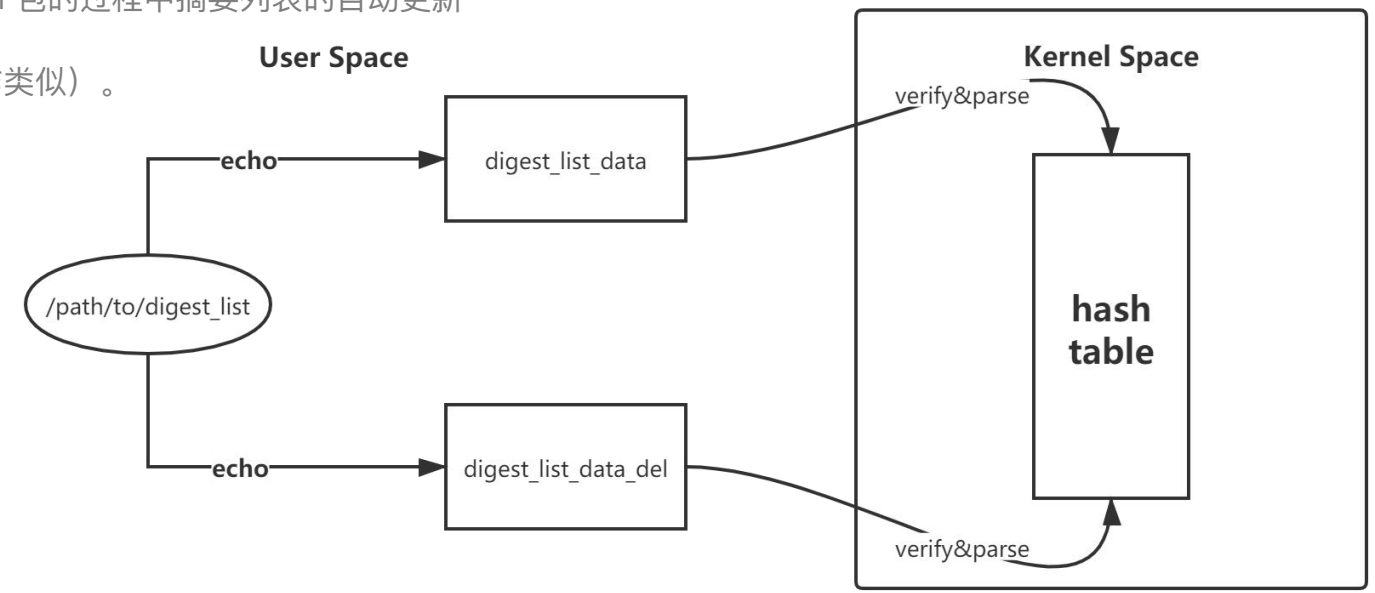
进入运行阶段后，您可以随时在内核空间中更新 IMA 度量和评估所需的参考值，而无需像原生 IMA 那样重启后进入 fix 模式：

方法一（手动更新）：使用 echo 命令将摘要列表文件的绝对路径写到 securityfs 提供的接口中。

- 导入列表：echo [/path/to/digest_list] > /sys/kernel/security/ima/digest_list_data
- 删除列表：echo [/path/to/digest_list] > /sys/kernel/security/ima/digest_list_data_del
- 优点在于灵活自由，只要摘要列表事先经过签名（签名存放在 security.ima 属性中），就能完成内核中参考值的更新。

方法二（自动更新）：安装、卸载、升级 rpm 包的过程中摘要列表的自动更新

- 更新操作由插件自动完成（原理与手动操作类似）。



openEuler

总结：原生内核IMA特性 vs openEuler内核IMA特性

	原生内核IMA特性	openEuler内核IMA特性
安全性	原生 IMA 机制要求在现网环境下预生成并标记文件扩展属性，访问文件时使用扩展属性作为参考值，信任链不完整。	将文件参考摘要值保存在内核空间，构建阶段通过摘要列表形式携带在发布的 rpm 包中，安装 rpm 包时导入摘要列表并执行验签，确保参考值来自于软件发行商，**实现了完整的信任链**。
易用性	原生 IMA 机制在初次部署或每次更新软件包时，都需要切换到 fix 模式手动标记文件扩展属性后再重启进入 enforce 模式，才能正常访问安装的程序。	摘要列表扩展可实现安装完成后开箱即用，且允许直接在 enforce 模式下安装或升级 rpm 包，无需重启和手动标记即可使用，实现了用户感知最小化，适合**现网环境下快速批量部署**。
性能	IMA 度量场景下，每次触发度量，都会进行TPM PCR扩展。 IMA 评估场景下，每次访问文件都会执行文件验签。	IMA 度量场景下，减少不必要的 PCR 扩展，开启度量时性能损失小于 5%，**相比原生 IMA 度量性能提升高达 50%**。 IMA 评估场景下，将签名验证统一移动到启动阶段进行，避免每次访问文件时都执行验签，**相比原生 IMA 提升运行阶段文件访问的性能约20%**，但增加启动时长约5%。

注：以上性能数据均为实验室环境下测试所得，实际环境下可能存在一定偏差。

快问快答赢T恤

下列哪个安全扩展属性用于存储受保护文件内容的摘要值?

A.security.selinux

B.security.ima

C.security.evm

D.security.capability

03 在openEuler上部署IMA

- 配置环境前的准备工作
- 配置环境进入IMA enforce模式
- 实际环境演示

配置环境前的准备工作

Step 1：从官方镜像源下载安装 openEuler-20.09 ISO

- **openEuler 官方镜像站**： https://mirrors.huaweicloud.com/openeuler/
- 镜像还在准备过程中，预计在 9 月底的正式版本中与大家见面！
- 对于安装环境而言，虚拟机和物理机都可行，且 TPM 芯片不是必需的，具体步骤请参考第三期直播“安装openEuler”：

https://www.bilibili.com/video/BV1vK4y1s7QG?from=search&seid=2139240105137620883

Step 2：配置 IMA 前的环境准备

- 使用 openEuler 官方镜像源配置 yum 仓库。
- 确认工具包 digest-list-tools 和 ima-evm-utils 是否已安装：rpm -qa | grep [package]
- 检查系统的 initramfs 公钥是否正确：evmctl ima_verify /etc/keys/x509_evm.der
- 编辑 /etc/dracut.conf 文件，加入一行：install_items+=" /etc/keys/x509_ima.der /etc/keys/x509_evm.der"

配置环境进入 IMA enforce 模式

Step 3：为受保护文件标记 security.ima 和 security.evm 扩展属性

- $ upload_digest_lists –p add–ima–xattr –d /etc/ima/digest_lists.tlv
- $ upload_digest_lists –p add–evm–xattr –d /etc/ima/digest_lists.tlv

Step 4：为摘要列表文件标记 security.ima 和 security.evm 扩展属性

- $ sh /usr/bin/restore_xattr.sh # 恢复脚本的内容在文档中提供
- $ find /etc/ima/digest_lists –type f –exec evmctl verify –o –a sha256 \{} \; # 检查摘要列表扩展属性是否已正确标记

Step 5：重新生成 initramfs

- 重新生成 initramfs：dracut –f –e xattr

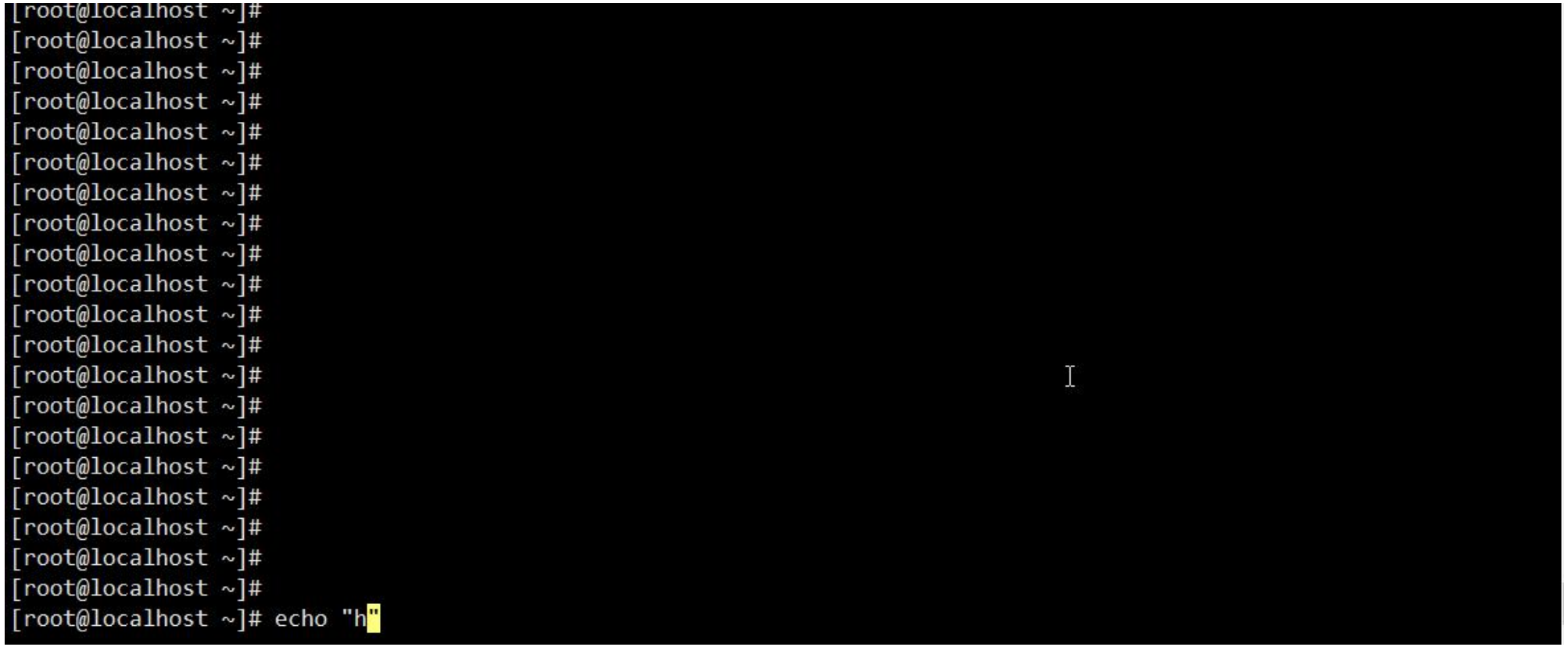
Step 6：设置启动参数并重启

- 添加 grub 启动参数：ima_appraise=enforce–evm evm=ignore ima_appraise_digest_list=digest ima_digest_list_pcr=+11 ima_template=ima–sig ima_policy="tcb_exec|secure_boot_exec|secure_boot_immutable" initramtmpfs integrity=1
- reboot

实际环境演示：x86_64

场景一：攻防场景

- 修改文件内容，查看文件是否能够继续执行？如果修改文件扩展属性呢？
- 执行一条未知的命令，是否可以成功？



openEuler

实际环境演示：x86_64

场景一：攻防场景

- 摘要列表会保护文件的哪些内容?

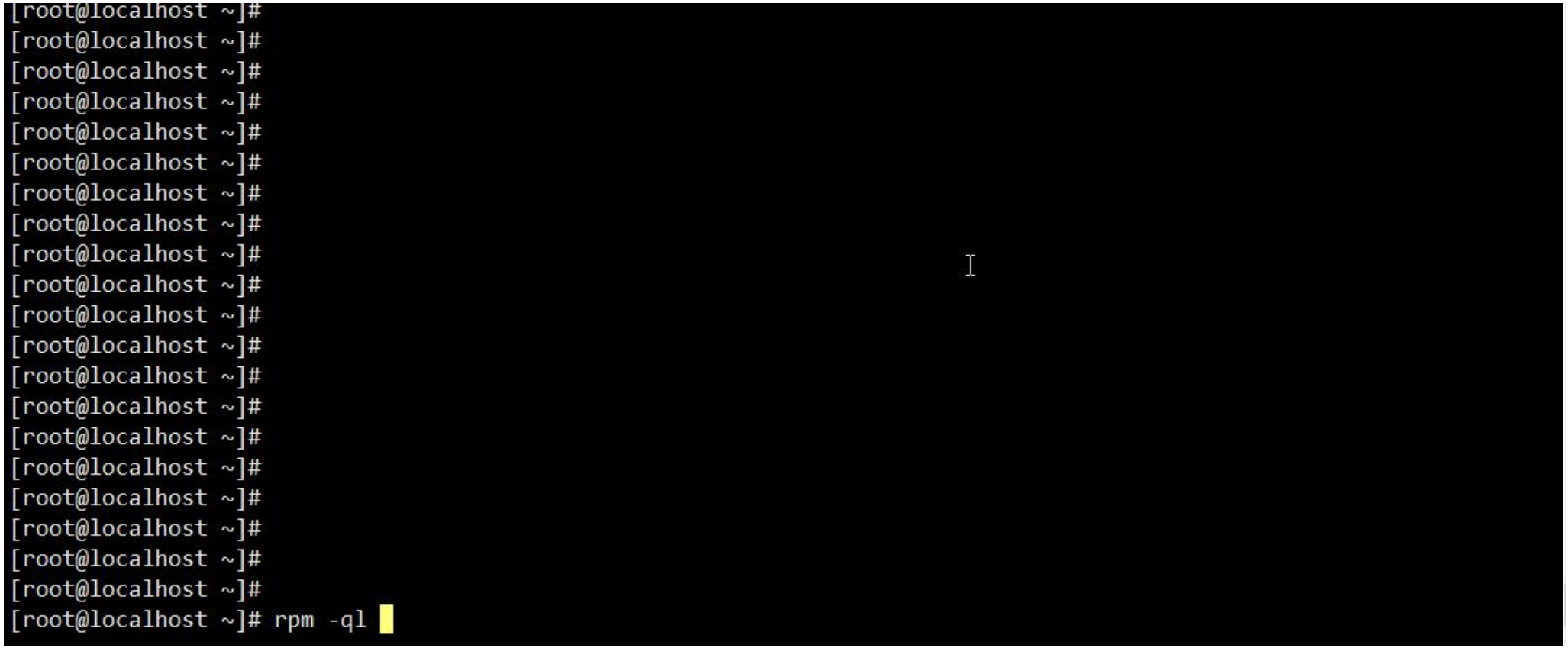
答：uid、gid、权限、security.selinux、security.ima、security.evm、security.capability

openEuler

实际环境演示：x86_64

场景二：升级场景

- 安装、卸载软件包过程中digests_count数量的变化。



实际环境演示：x86_64

场景二：升级场景

- 尝试通过 securityfs 接口手动更新内核哈希表，更新后命令是否能够正确执行?

04 one more thing…

- 展望未来：IMA是否能做得更多?
- 如何在openEuler上参与对安全基础设施的贡献?
- 更多学习资源

展望未来

Topic A：如何将度量范围从可执行文件延伸到非可执行文件?

从**主体（可执行文件/动态库文件）**的可信，扩展到被它读取的**客体（配置文件/数据文件）**的可信。

- 引入新的IMA策略关键字check_evm和don_check_evm。
- 根据业务场景，为需要保护客体完整性的主体设置特殊的SELinux标签，被此类主体访问的客体都会触发IMA度量。
- 需要在运行环境下手动调整的配置文件，不会触发IMA度量，而是通过信任链的其它环节保护。

Topic B：如何导入第三方应用的摘要列表?

在内核中加入新公钥，重新构建内核，从而支持导入第三方软件摘要列表。

使第三方应用在系统中运行的步骤：

1. 使用digest-list-tools和ima-evm-utils为第三方应用rpm包或tar包生成摘要列表。
2. 在可信的构建环境中用第三方公钥对应的私钥对摘要列表签名。
3. 安装部署过程对摘要列表验签。

如何贡献

openeuler内核邮件列表：kernel@openeuler.org

如果您想要参与到内核中IMA特性的开发，可以发送补丁到openEuler内核邮件列表，详见第9期直播“如何参与openEuler内核开发”。

openEuler自维护源码仓

https://gitee.com/openeuler/kernel

https://gitee.com/openeuler/digest-list-tools

https://gitee.com/openeuler/attest-tools

提issue或者PR，甚至申请加入security facility SIG成为maintainer，你说了算！

openEuler第三方软件仓

https://gitee.com/src-openeuler/tss2

https://gitee.com/src-openeuler/ima-evm-utils

心动不如行动，加入openEuler大家庭，现在就加入openEuler的大家庭吧！

更多学习资源

openEuler文档资源

openEuler 官方博客：https://openeuler.org/zh/blog.html

项目仓库：https://gitee.com/digest-list-tools

开源社区资源

内核完整性度量（IMA）官方 wiki：http://sourceforge.net/p/linux-ima/wiki/Home

可信软件栈（TSS）：https://github.com/tpm2-software/tpm2-tss

IBM Software TPM：http://ibmswtpm.sourceforge.net/

学术资源

推荐阅读 CMU 学者的综述论文“Bootstrapping Trust in Commodity Computers”，发表在信息安全顶会 IEEE S&P 2010，对可信计算理解比较到位。

中文书籍推荐冯登国教授的“可信计算理论与实践”，对可信计算的研究历史、现状和技术有比较全面和深入的探讨。

欢迎关注

官方网站

代码托管平台

openEuler已全面开源， 欢迎关注、使用openEuler并参与社区贡献。

欢迎关注

官方微信交流群

添加小助手微信备注openEuler，拉你进群

微信公众号： openEuler

新浪微博： openEuler社区

Twitter： openEuler

openEuler