
GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
eBPF 专场
eBPF与私密计算的生态结合
郑振宇 2022年05月28日

About Me

郑振宇

openEuler社区Maintainer、布道师
OpenStack、Libvirt、Hadoop社区开发者

机密计算(Confidential Computing)

机密计算是由机密计算联盟 (CCC) 定义的一个行业术语：

通过在基于硬件的受信任执行环境 (TEE) 中执行计算来保护使用中的数据

机密计算(Confidential Computing)

云原生时代带来的安全挑战：将业务运行在云平台上意味着信任各类供应商

应用软件供应商

将业务运行在商业软件、开源软件、或就地部署软件上
意味着信任软件提供者

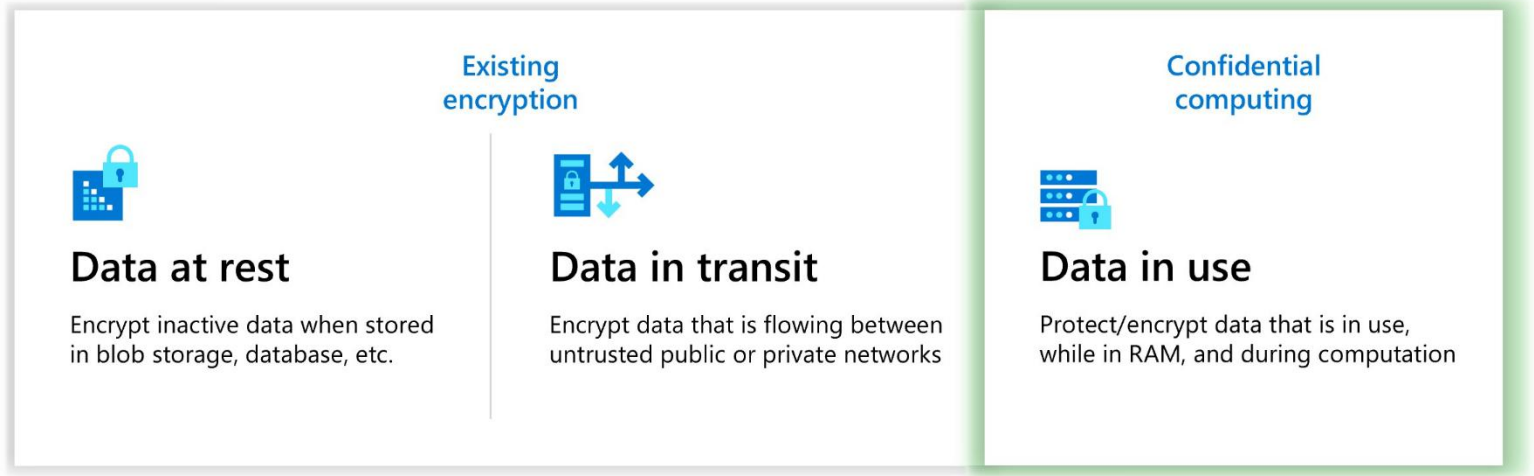
硬件供应商

业务最终会运行在硬件上，意味着信任硬件提供者

基础设施提供商

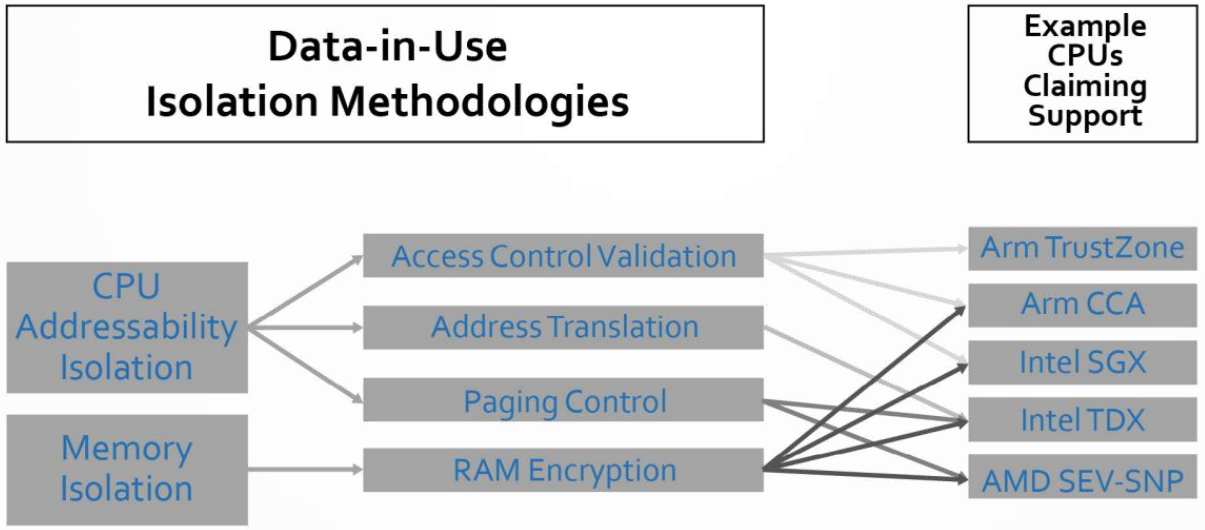
业务云基础设施提供商，意味着信任云基础设施提供者

机密计算(Confidential Computing)



- 与静态数据加密和传输中数据加密一起使用时，机密计算可以在安全的公有云平台中保护敏感或严格监管的数据集和应用程序工作负载，以此消除了加密的唯一最大难题 – 使用中数据的加密从而超越了常规数据保护
- TEE 还可用于保护专有业务逻辑、分析函数、机器学习算法或整个应用程序

机密计算(Confidential Computing)



- 访问控制验证：对内存区域的访问仅限于特定的进程/上下文。
- 地址转换：内存的分段区域不能直接从 TEE 的边界之外进行寻址。
- 分页控制：非 TEE 进程不会与 TEE 数据同时在 CPU 中活动。
- 内存加密：对内存中的数据进行加密，防止黑客或恶意软件窃取敏感信息

机密计算(Confidential Computing)

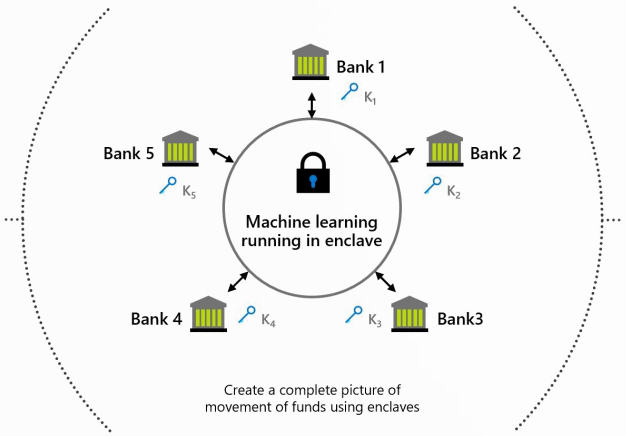
金融

Confidential computing allows

Run agreed upon analytics on the combined data

Insights without giving access

Meet confidentiality requirements



Outcomes

Increase detection rates

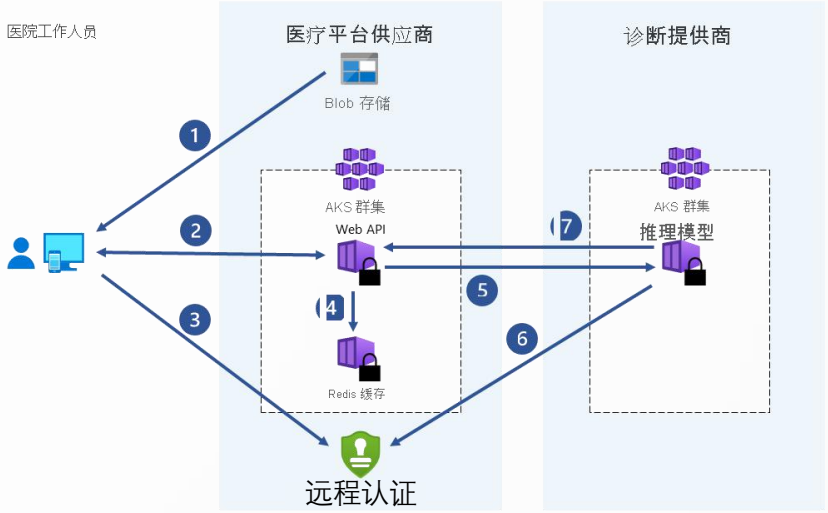
Reduce false positives

Iterative learnings

安全的多方计算：多个银行彼此共享数据，不会公开其客户的个人数据。 银行对合并的敏感数据集运行经过一致同意的分析。 对聚合数据集的分析可以检测一个用户在多个银行之间的资金流动，各银行之间不会互相访问数据。

通过机密计算，这些金融机构可以提高欺诈检测率，处理洗钱场景，减少误报，并持续从较大数据集中学习。

制造



联邦学习：相互合作的医疗保健机构提供专用医疗保健数据集来训练 ML 模型。 每个机构只能看到自己的数据集。 没有其他机构能够看到数据或训练模型，甚至云提供商也不能。 所有机构都可通过使用经过训练的模型获益。 通过使用更多数据创建模型，模型变得更准确。 参与训练模型的每个机构都可以使用该模型并收到有用的结果。

机密计算(Confidential Computing)

GOTC

Premier Members

accenture 蚂蚁集团 ANT GROUP arm facebook Google HUAWEI intel Microsoft Red Hat

General Members

AMD AMPERE. anjuna Anqlave appliedblockchain ByteDance cisco cosmian

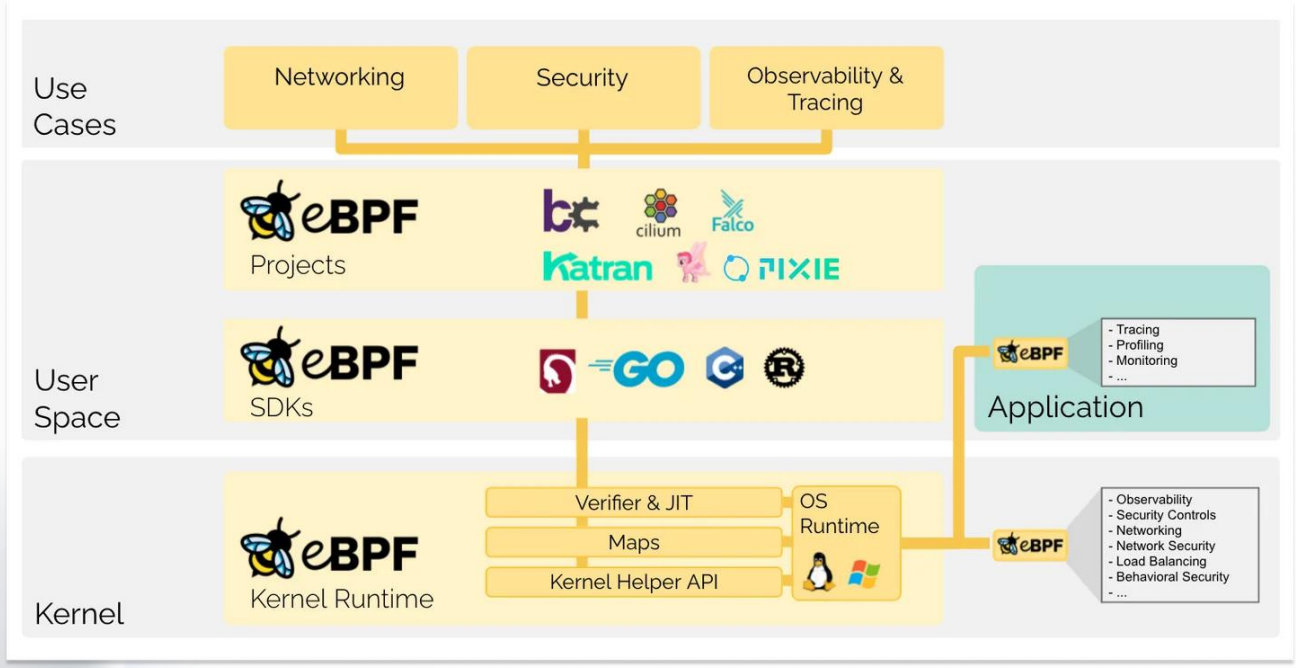
CRUST CYSEC DECENTRIQ EDGELESS SYSTEMS ENVEIL Ethernity CLOUD Fortanix

iExec MADANA NVIDIA. PHALA NETWORK Profian r3. swisscom vmware

Western Digital. XILINX

eBPF + Confidential Computing

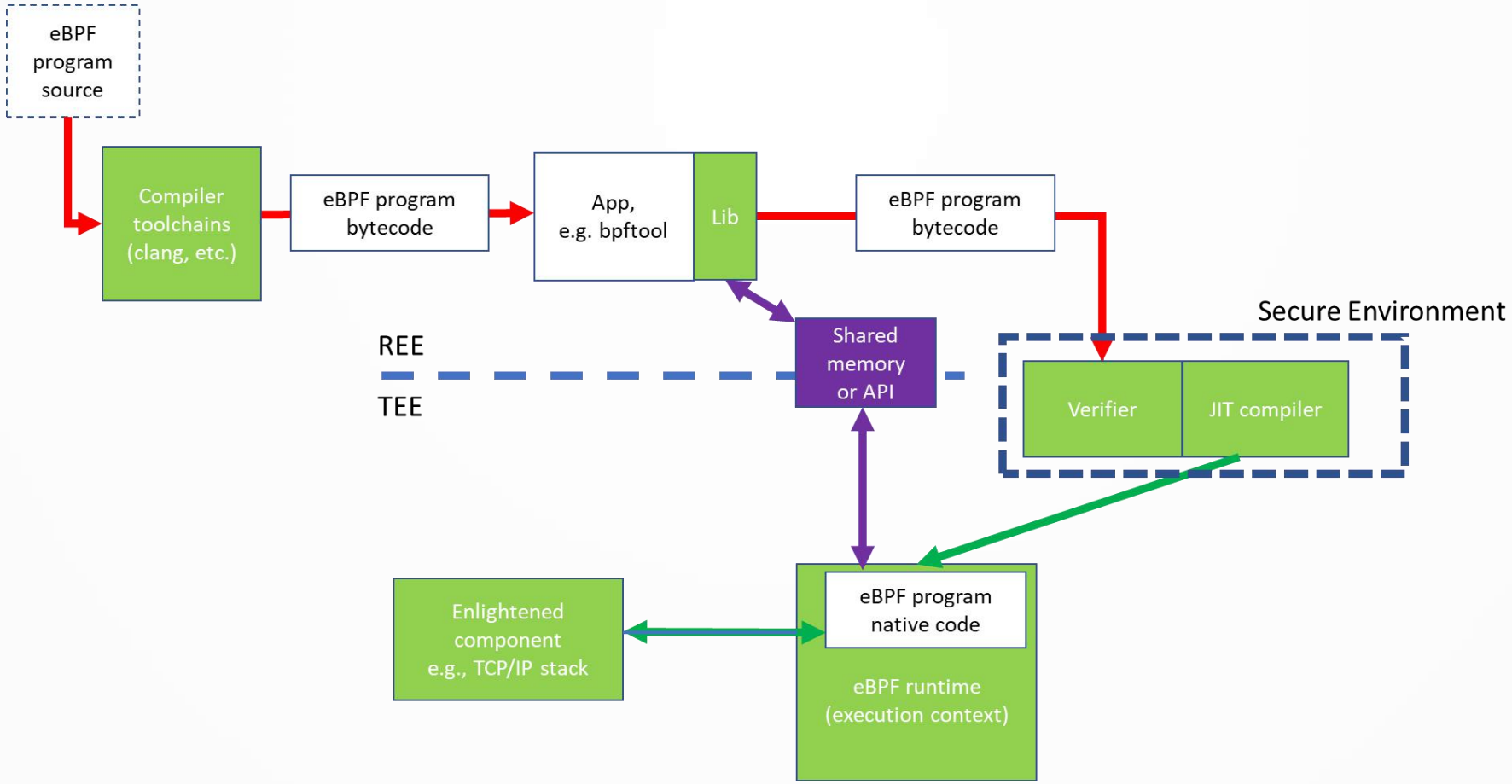
eBPF + Confidential Computing



“eBPF是一种跨平台技术，可以运行沙盒程序来扩展特权系统组件”

- 在可信执行环境（TEE）中的代码是特权系统组件
- 设计时场景：设计一个扩展程序，将其部署到现有的保密虚拟机/容器/进程/库中；
- 运行时场景：根据管理员输入即时创建一个扩展程序，以在现有的保密虚拟机/容器/进程/库中运行。

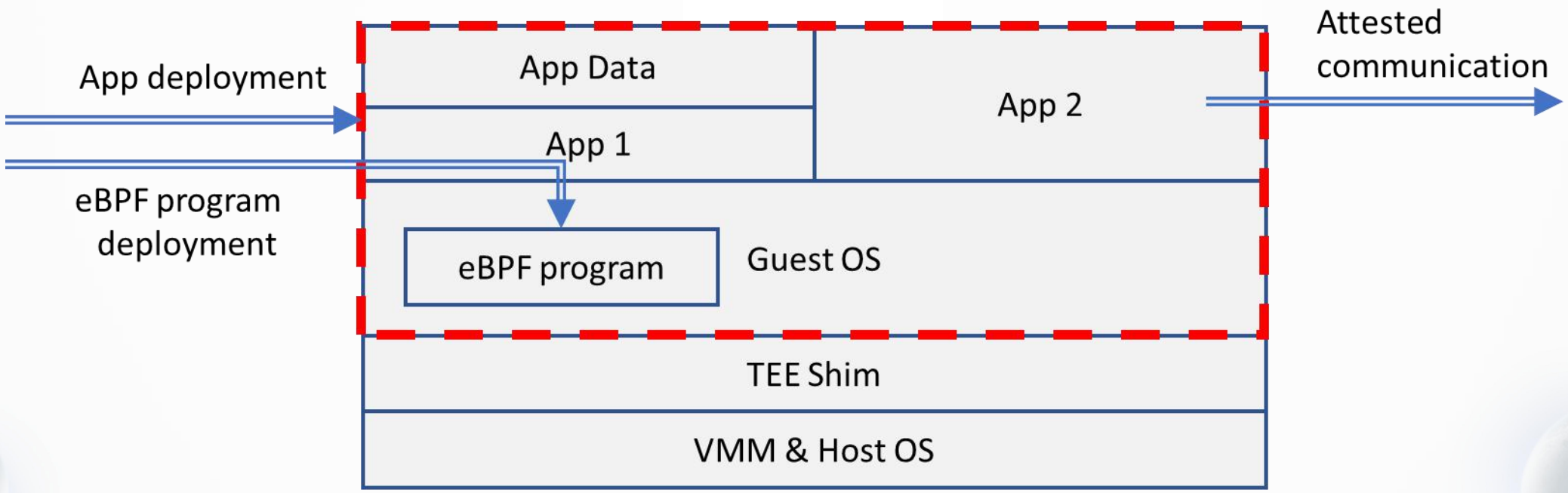
eBPF + Confidential Computing



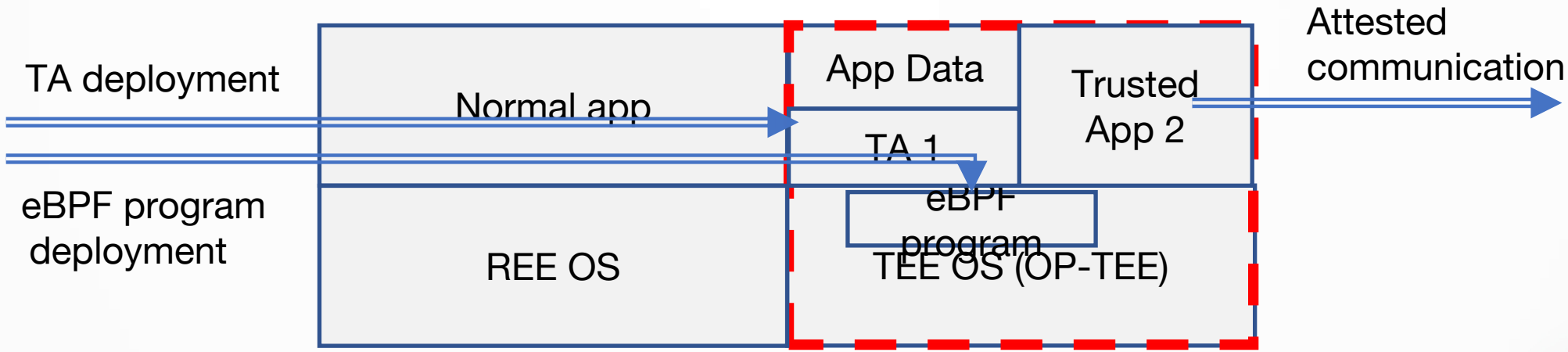
Why eBPF?

- 可能已经存在于TEE中（例如，在TEE中的Linux虚拟机中）。
- 硬件卸载已经存在，更多的硬件正在出现。
- 已经存在工具和知识的生态系统。与Linux的可扩展趋势相一致。
- 与WASM相比，可以在内核模式下工作，支持更多语言类型（例如Rust）。
- 验证器提供了比许多其他方法更强的安全性和可靠性（例如，代码在有限时间内终止）。

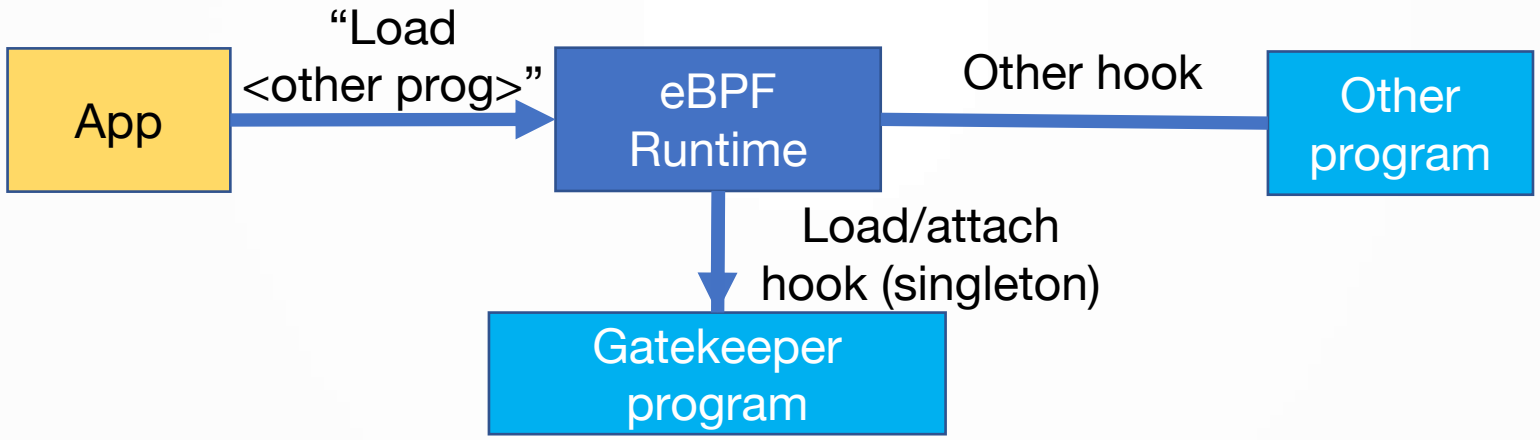
示例1：CVM(Confidential Virtual Machine)



示例2：OP-TEE


TA deployment
eBPF program
deployment
Normal app
REE OS
App Data
TA 1
eBPF
program
TEE OS (OP-TEE)
Trusted
App 2
Attested
communication

eBPF GateKeeper：2nd gate after verifier



- 对eBPF程序进行签名校验，仅允许授信程序执行
- 灵活的授信模式：按应用程序、按来源、按发行商等
- 按需配置默认行为

eBPF + Confidential Computing 证明

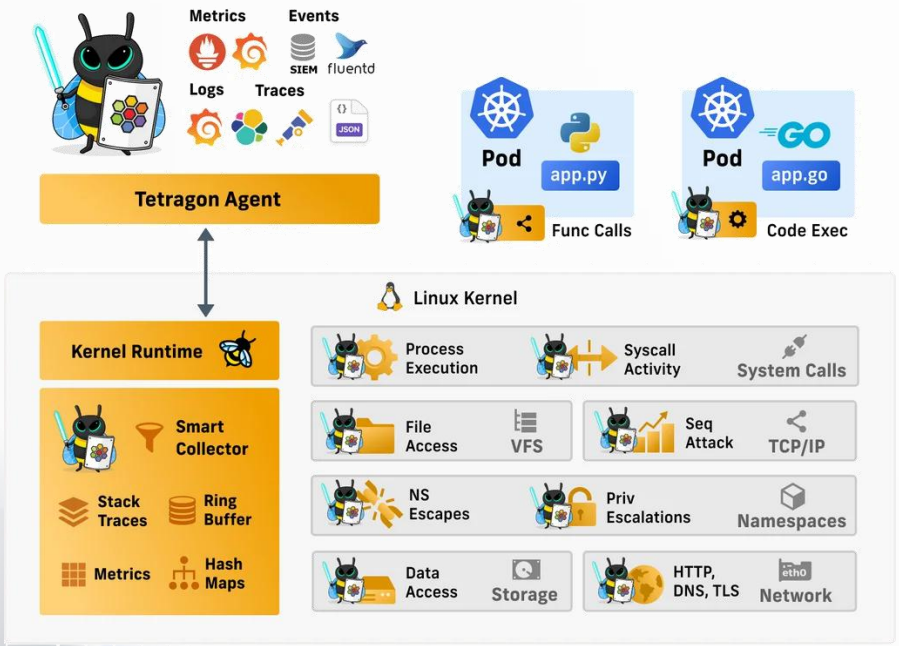
Many potential scenarios exist

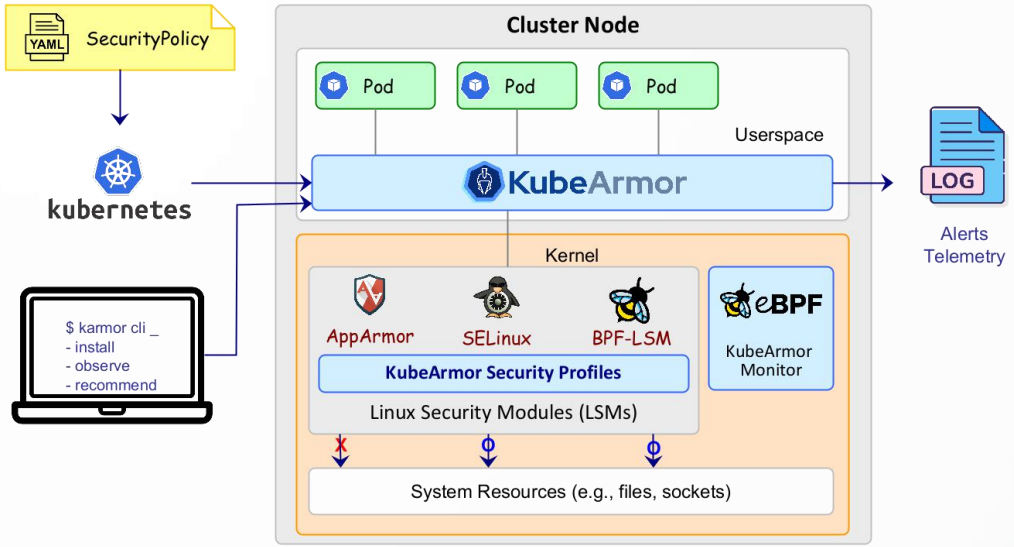
1. eBPF应用部署证明:
   A. 仅在可靠的TEE上部署可靠的eBPF应用
   B. TEE 仅接受来自可靠源的eBPF应用

2. eBPF 扩展实现可信通信:
   A. 将数据或代码部署到可信 TEE (可被eBPF扩展)
   B. 仅接受来自可靠TEE的数据请求 (可被eBPF扩展)

3. eBPF 应用通过API访问:
   A. eBPF 在数据流量中校验
   B. eBPF 在API调用时校验
   C. 使用eBPF程序作为校验工具

开源方案

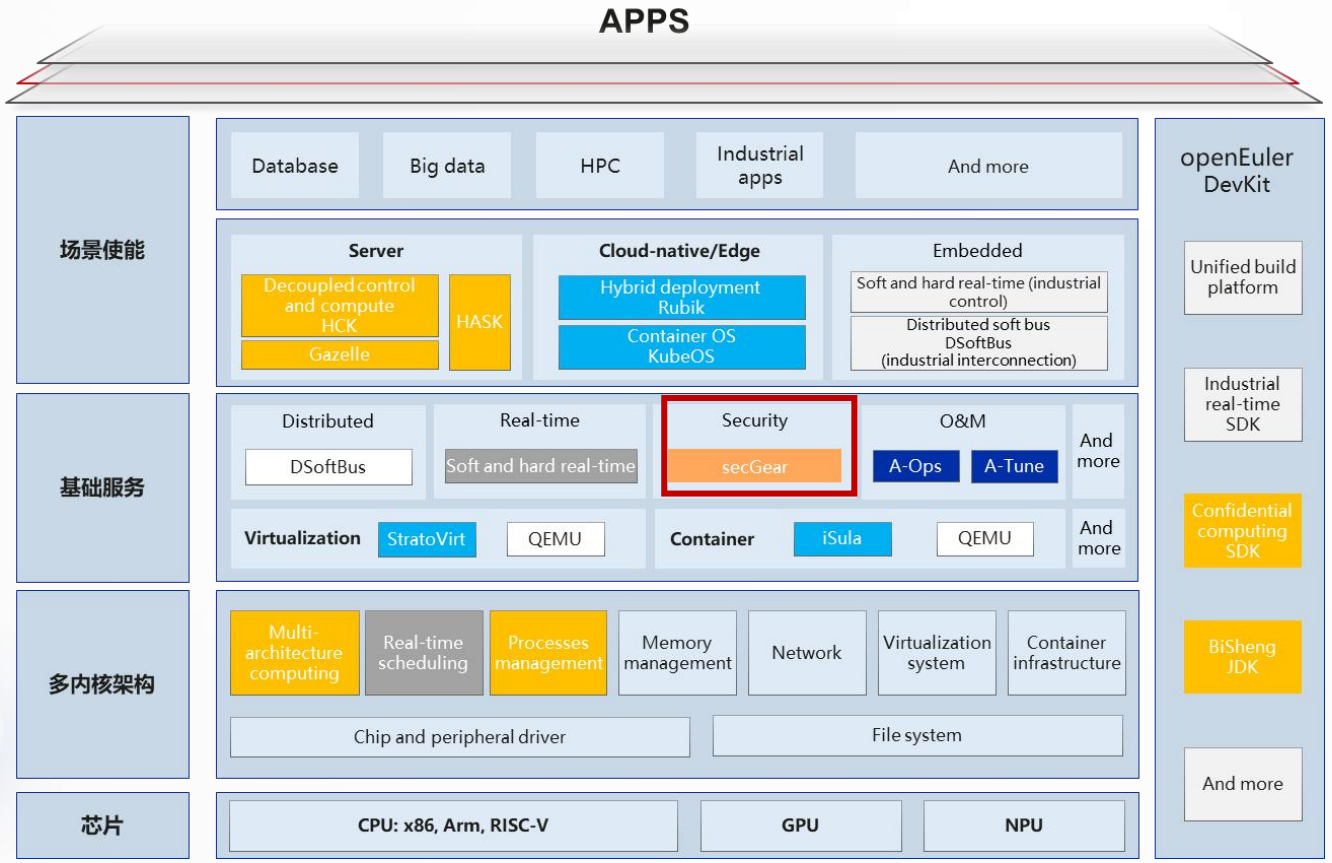




CONFIDENTIAL CONTAINERS

eBPF/Confidential & openEuler

openEuler: 高性能、高安全、易运维数字基础设施开源操作系统



多样性算力支持

内核架构优化、用户模式协议栈 Gazelle 和 HCK 解耦控制和计算架构可实现最佳性能（提升 5% 至 20%）；混合存储加速套件 HASK 显着提高了 Ceph 存储的 IOPS。

云原生全栈

引擎、容器OS、安全容器混合部署，夯实云原生基础，资源利用率提升15%~40%

嵌入式场景

硬实时解决方案满足工控领域多层时延要求（中断/调度时延<0.5μs）

高效 O&M

A-OPS智能运维，A-tune智能调优效率倍级提升

高安全、高可靠

机密计算框架secGear：软硬件协同打造安全优势

openEuler SecGear

1、服务层：提供完整的基于机密计算的安全服务，用户直接使用相关服务，享受机密计算带来的安全性。

2、中间件层：提供常见的安全协议组件以及各种安全函数库，用户可以直接在安全及非安全侧调用相关接口，不必从头造轮子。

3、基础层：提供丰富的 enclave 开发接口或工具，包含代码生成工具和enclave声明周期管理等接口，并且在安全侧支持POSIX APIs 和标准 OpenSSL 接口，用户基于这些接口可以自由开发安全应用程序 。

openEuler Kmesh

代理架构 数据面引入额外时延开销，无法满足时延敏感应用诉求

Kmesh

基于可编程内核，OS中完成流量治理，服务访问3跳变1跳

高性能网络：

流量治理下沉，服务访问通信性能提升5倍

关键技术：

- 治理运行时：基于伪建链、应用协议四层寻址等技术，在OS中构筑L4~L7治理运行时
- 动态可编程：基于ebpf实现灵活、可靠的治理能力，随流完成治理，不引入额外开销z

eBPF as Service

将内核能力、硬件加速能力服务化、集市化，惠及更多的社区用户

- eBPF runtime：负责提供具备可移植性的软件安装能力，软件热升级能力，包管理等能力。
- eBPF Development Kit：负责提供一站式开发、调试、编译工具，提供具备跨体系、平台移植能力的软件包发布能力。
- eBPF Service HUB：负责提供 eBPF Service 集市化管理，提供 eBPF Service 推送、分发等能力。

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE