euleros isula
Security Level:

容器安全

www.huawei.com

Author：张永
Email: zhangyong23@huawei.com

Date: 2017-06-14

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

背景介绍

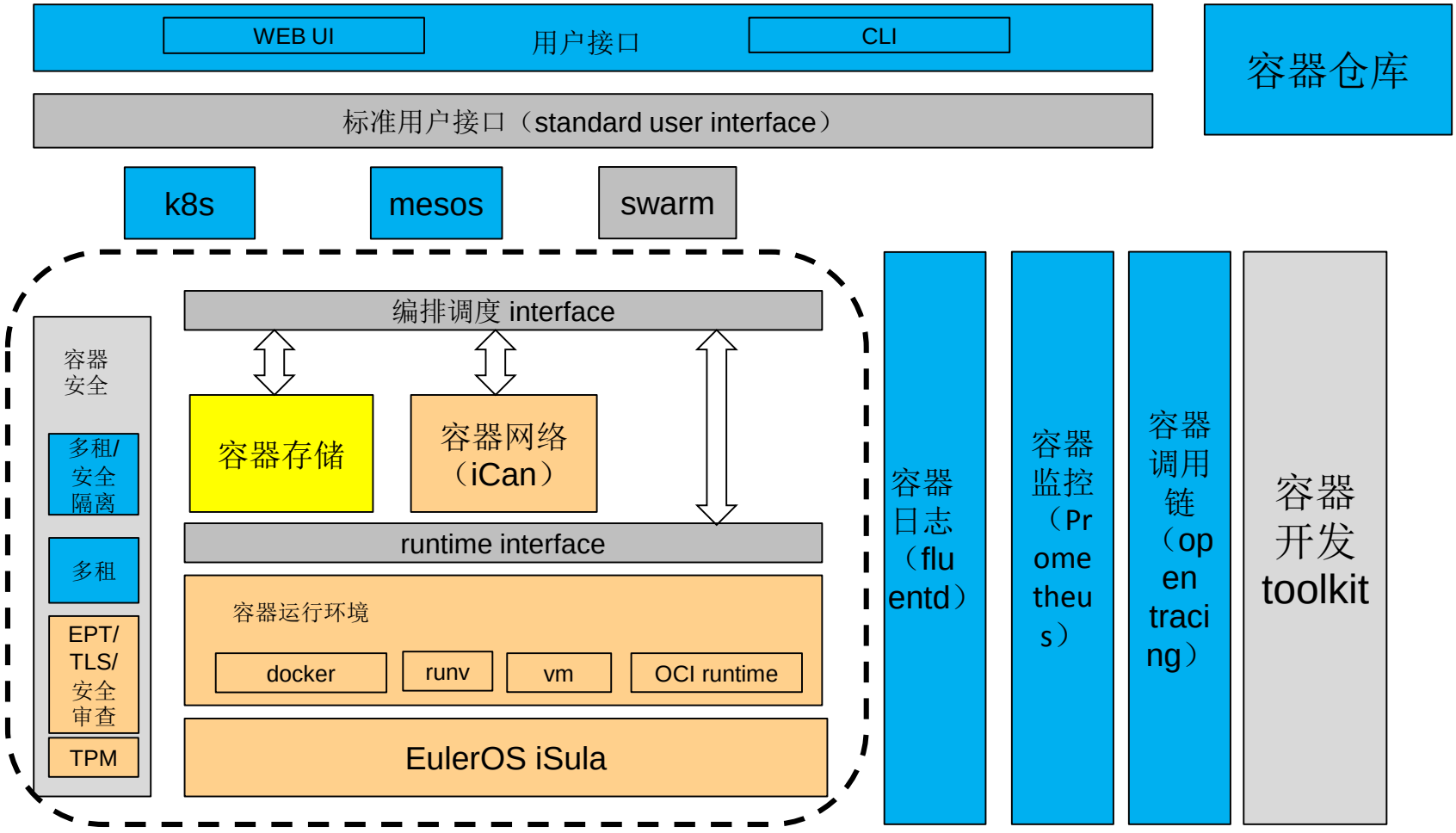
--我是谁？？

张永
Email：yong.zhang0@gmail.com； zhangyong23@huawei.com

- 2008 ~ 2015年：WindRiver Linux部门
- 2015.5 ~ Now：华为EulerOS系统部
- 长期从事linux系统开发，活跃于linux社区
- 在华为EulerOS部门主要负责容器项目的开发设计

背景介绍

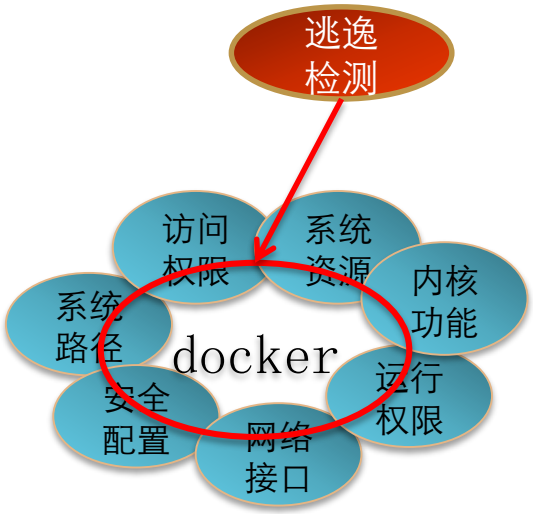
--EulerOS iSula

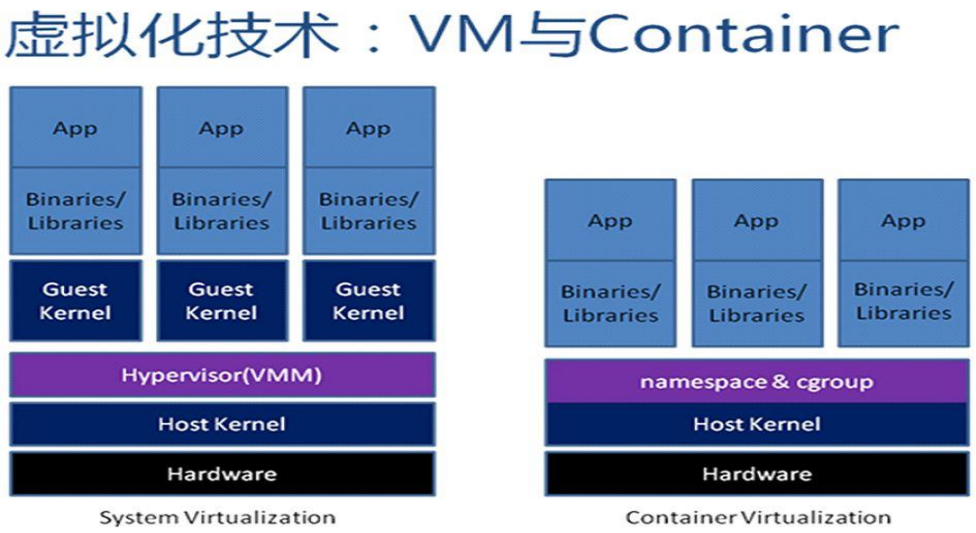


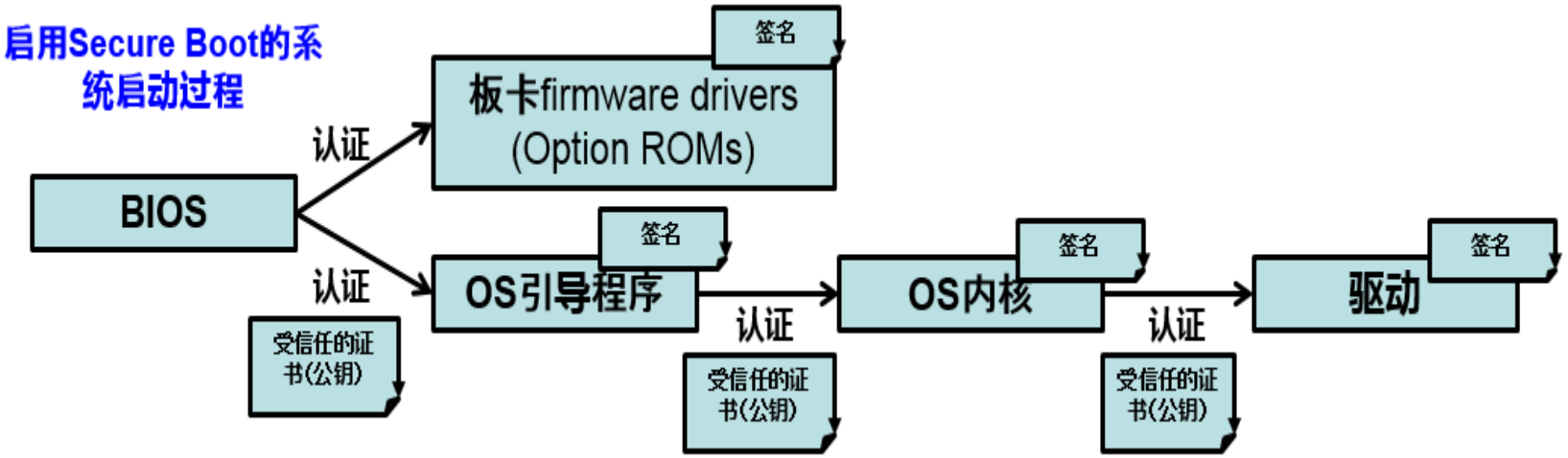
EulerOS iSula负责的范围

euleros isula

- 主机安全问题
  --
  --
  --
- 容器安全问题
  --
  --
  --



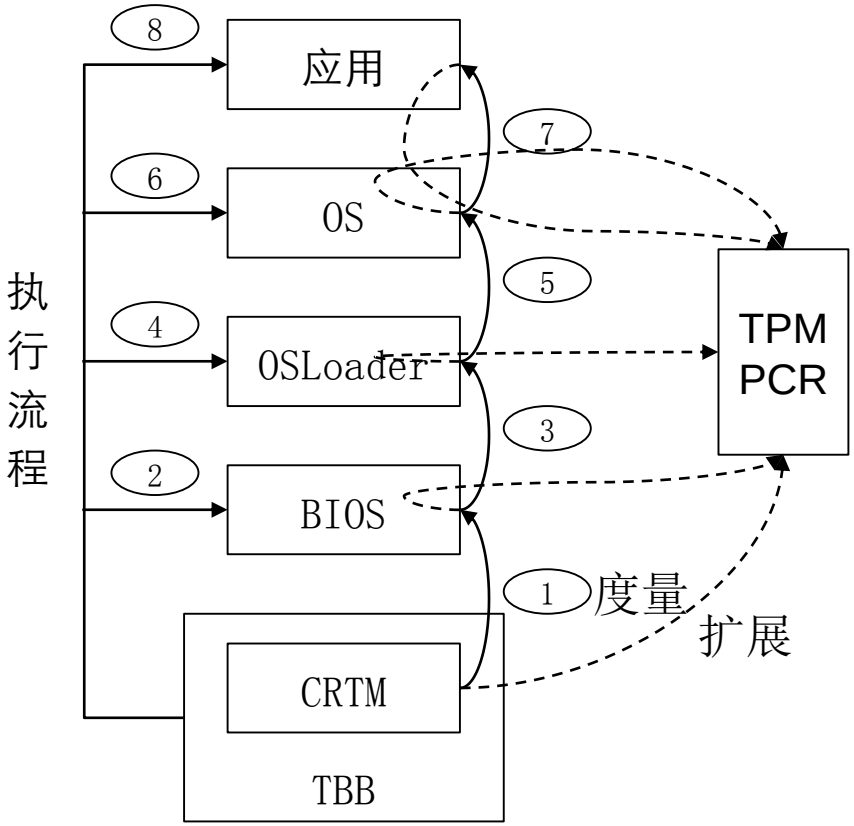


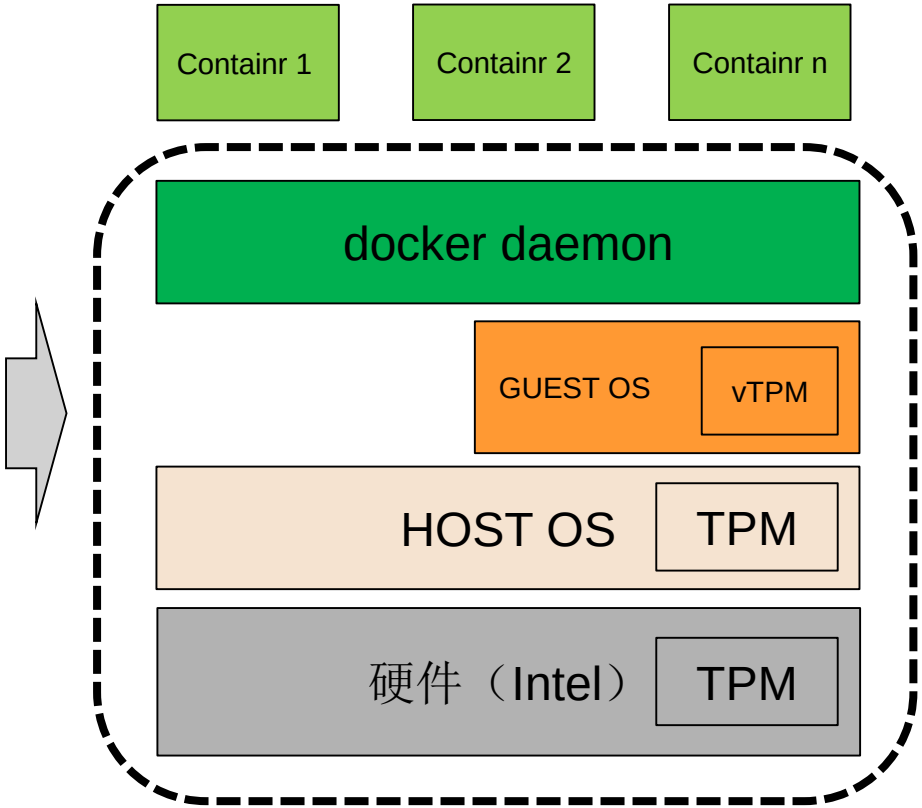


通过在启动过程中识别基础系统信任问题，确保主机安全

主机安全

--可信启动


8
应用
7
6
OS
5
执行流程
4
OSLoader
TPM
PCR
3
2
BIOS
1
度量
扩展
CRTM
TBB


Containr 1
Containr 2
Containr n
docker daemon
GUEST OS
vTPM
HOST OS
TPM
硬件（Intel）
TPM

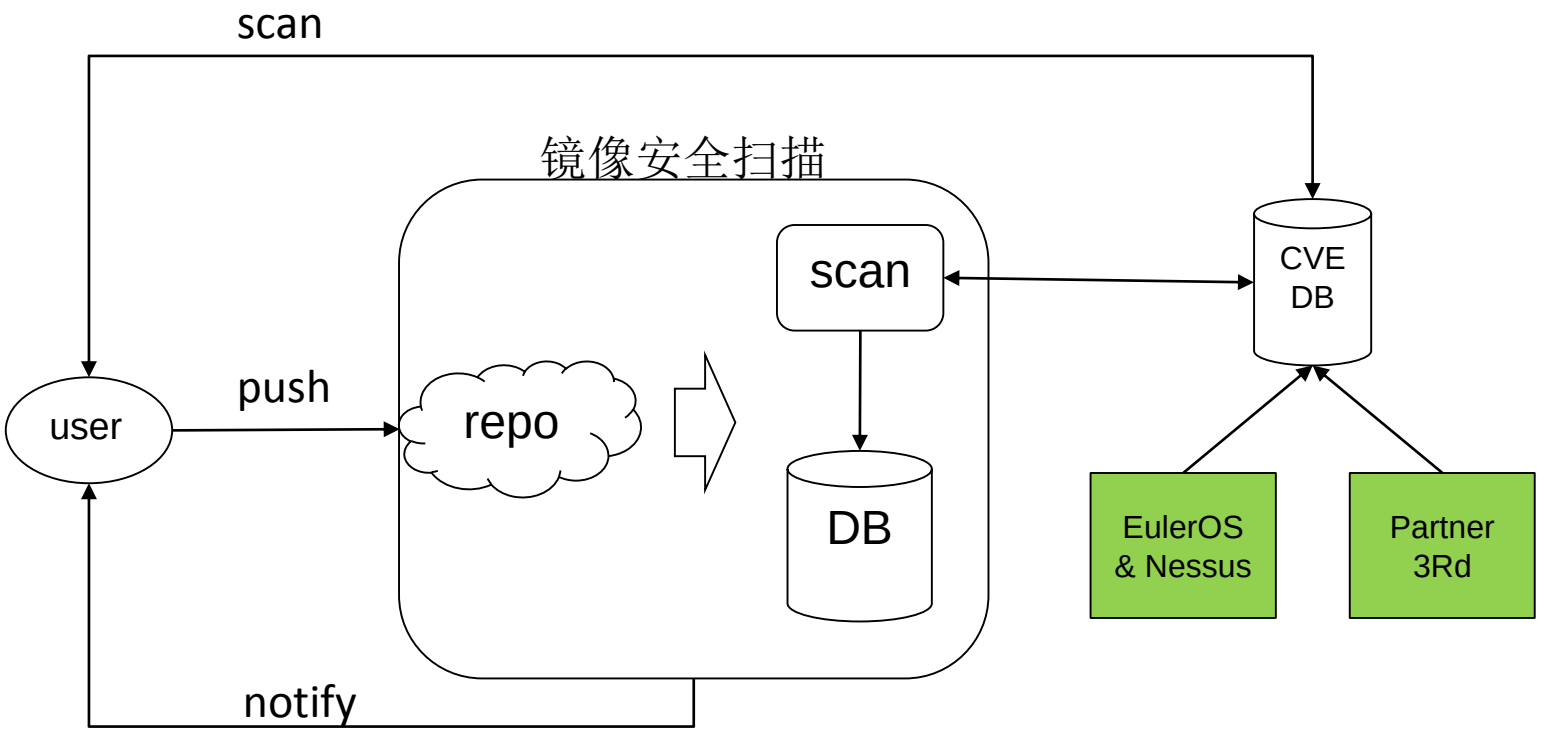
- Kernel
  - ACL
  - Capabilities
  - namespace
  - seccomp
  - iptables
  - audit
  - selinux
  - IMA
  - Address Space Layout Randomization (ASLR)

- OS
  - 不可变基础设施
  - 容器OS（Container OS）

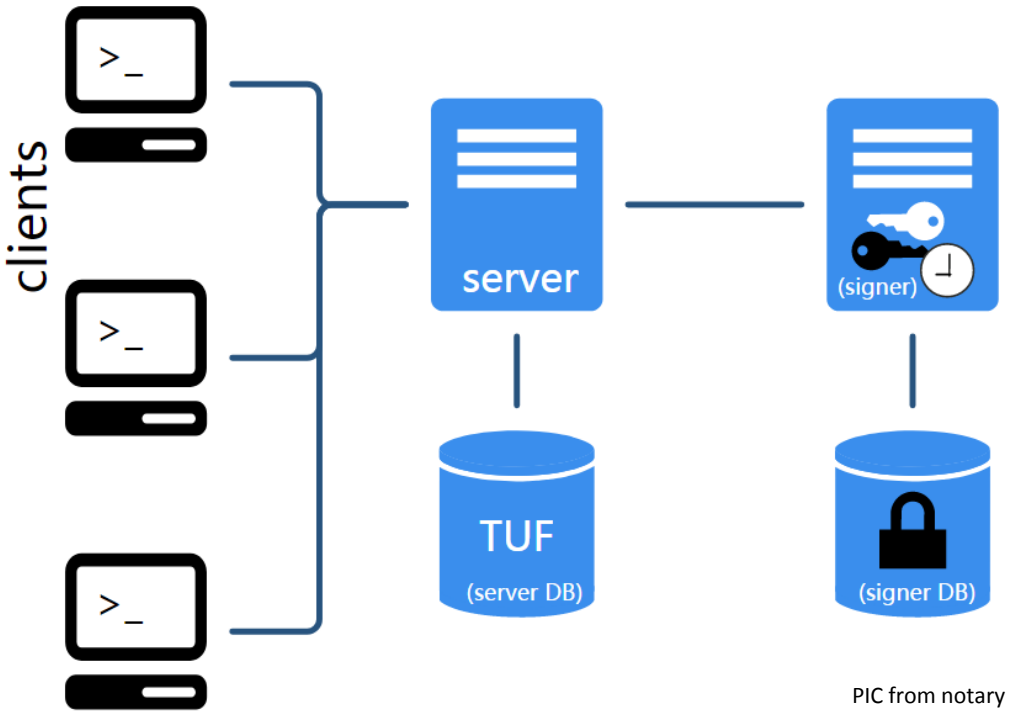
- Kernel
  - ACL
  - Capabilities
  - namespace
  - seccomp
  - iptables
  - audit
  - selinux
  - IMA（TPM）
  - Address Space Layout Randomization (ASLR)
  - cgroups

- OS
  - 不可变基础设施
  - 容器OS（Container OS）

针对Docker容器的漏洞扫描工具，解决容器镜像携带漏洞的问题，更进一步，发现带有恶意程序的镜像。



- DOCKER_CONTENT_TRUST
- Norary open source project



PIC from notary

容器安全

--运行时

- docker run --readonly
- No privilege
- no root in docker
- 镜像完整性检查

Join us at github.com/isula

Q&A