Monthly Research

SELinux in Virtualization and Containers

F F R I , Inc
http://www.ffri.jp

Ver 1.00.02

SELinux in Virtualization and Containers

- Virtualization security with SELinux
  - Threat model of operating system virtualization
  - libvirt(svirt)
  - An isolation between host OS and guest OS with Type Enforcement*1
  - An isolation between guests with Multi Category Security*2

- Docker security with SELinux
  - About Docker
  - Threat model of Docker
  - Isolation using libcontainer with SELinux

- Conclusion

*1, *2: We already shows SELinux Basics. See also:
http://www.ffri.jp/assets/files/monthly_research/MR201406_A%20Re-introduction%20to%20SELinux_ENG.pdf

Introduction

- In virtualization environment, isolation is an important security factor
  - Container is also the same
- Unfortunately, almost virtualization instances and containers require root privilege
  - If possible, host OS confines guest OS and container “in the virtual”
- In this research, we show isolation using SELinux in Linux virtualization system and Docker

VIRTUALIZATION SECURITY WITH SELINUX

Threat model of operating system virtualization

- Case1: Infecting host from malicious guest
  - If vulnerabilities exist in virtualization system, an attacker may gain privileges because almost Guest OS runs with root privileges in Linux virtualization system
- Case2: Malicious guest attacks to the other guest
  - DoS attack, information stealing and more

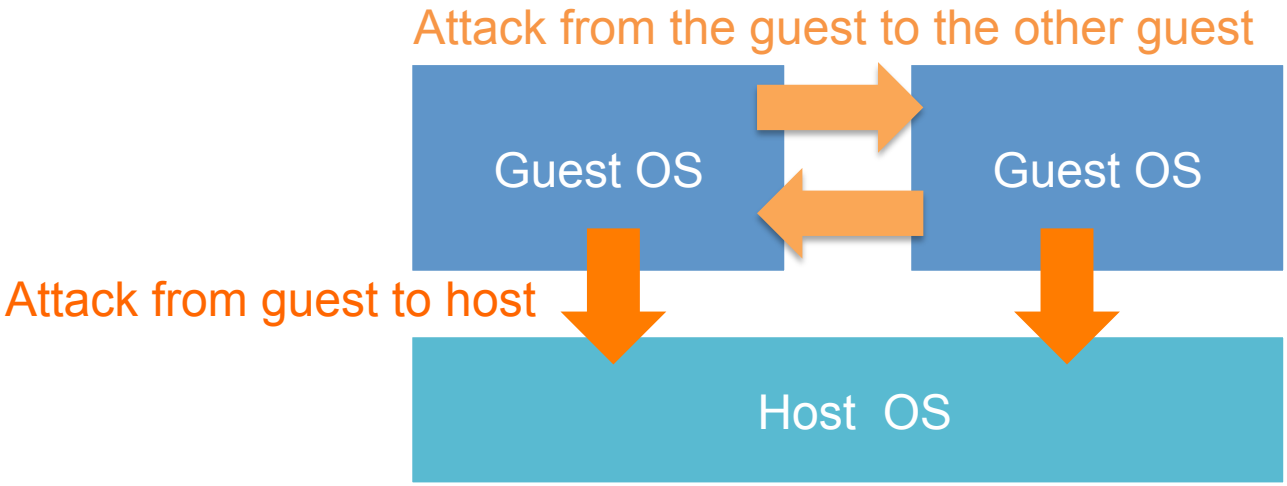


Fig 1. Threat model of virtualization system

libvirt(with svirt)

- libvirt is well-integrated VM management framework
  - virsh is sophisticated component in libvirt which is usable tools for administrator

- sVirt(secure Virtualization) integrated into libvirt for each virtualization software and containers with SELinux and AppArmor
  - Virtualization: KVM, Xen, QEMU, VirtualBox, VMwaare, Hyper-V etc.
  - Containers: LXC, OpenVZ etc.
  - If use SELinux, security policies are managed by reference policy

An isolation between host OS and guest OS with Type Enforcement

- A Security manager of libvirt isolates the guest using integrated Linux access controls
  - selinux, apparmor, Unix DAC

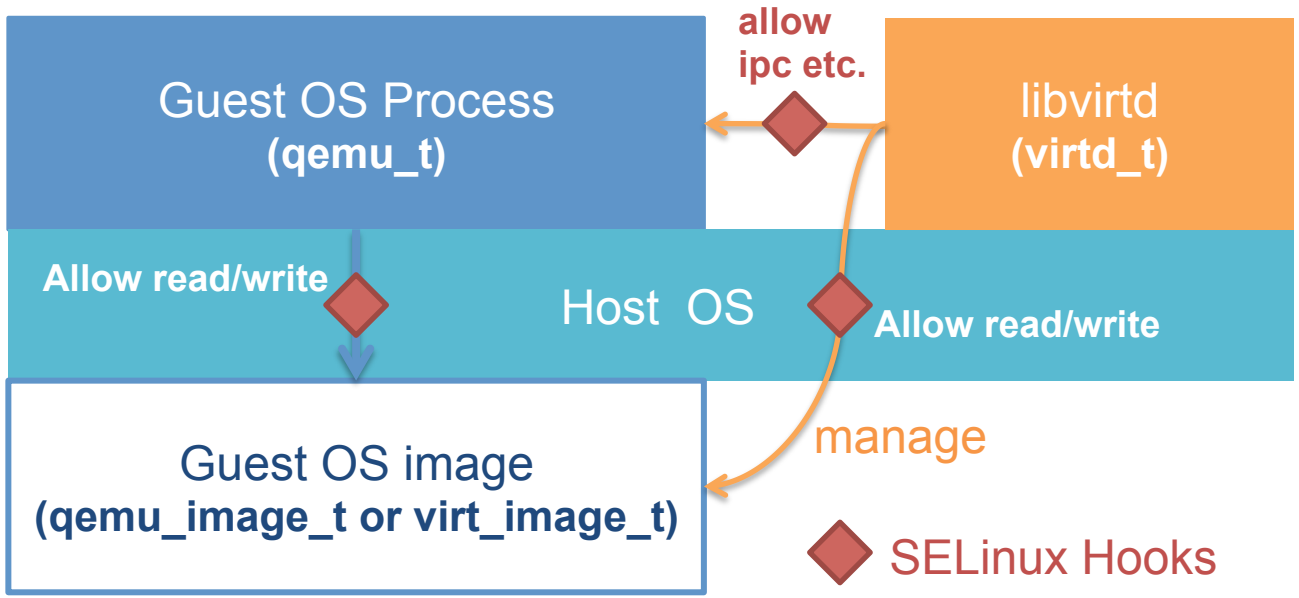


Fig 2. Host-Guest Isolation using SELinux

An isolation between guests with Multi Category Security

- A Security manager of libvirt assigns unique MCS context to guest process and guest disk images dynamically
- MCS access controls denies access from another categories

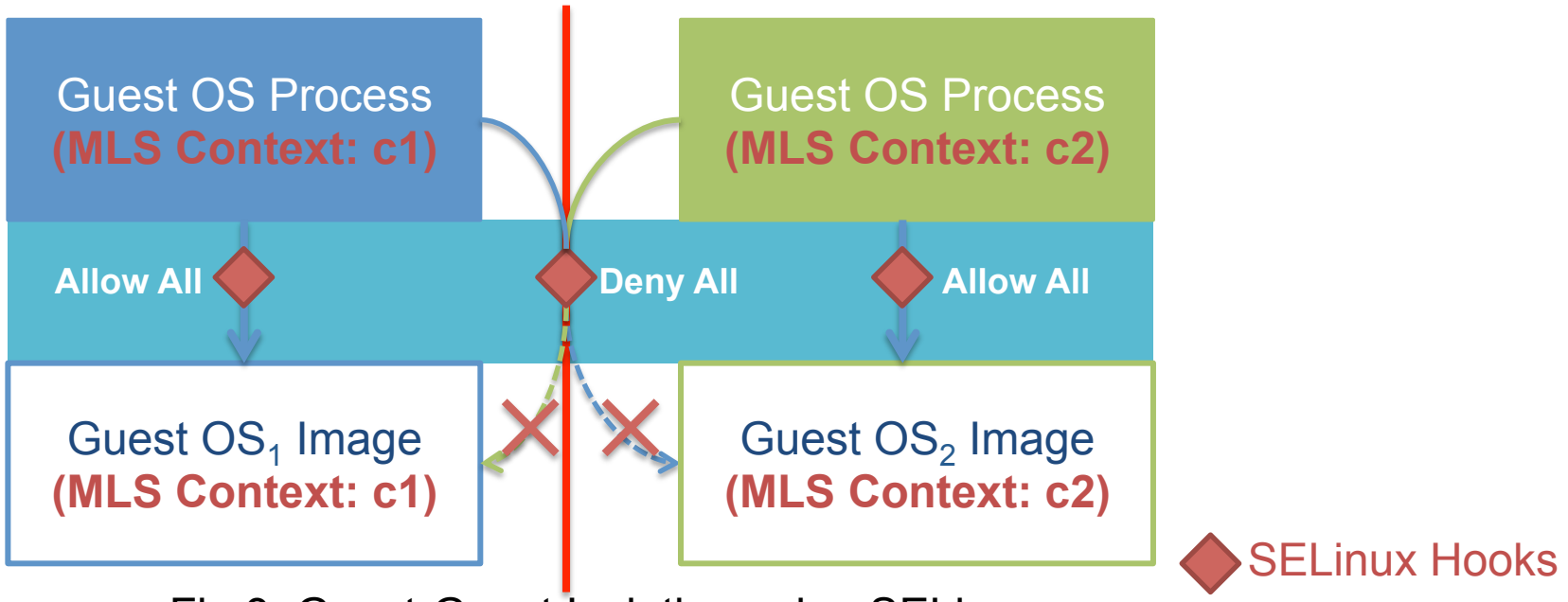


Fig 3. Guest-Guest Isolation using SELinux

DOCKER SECURITY WITH SELINUX

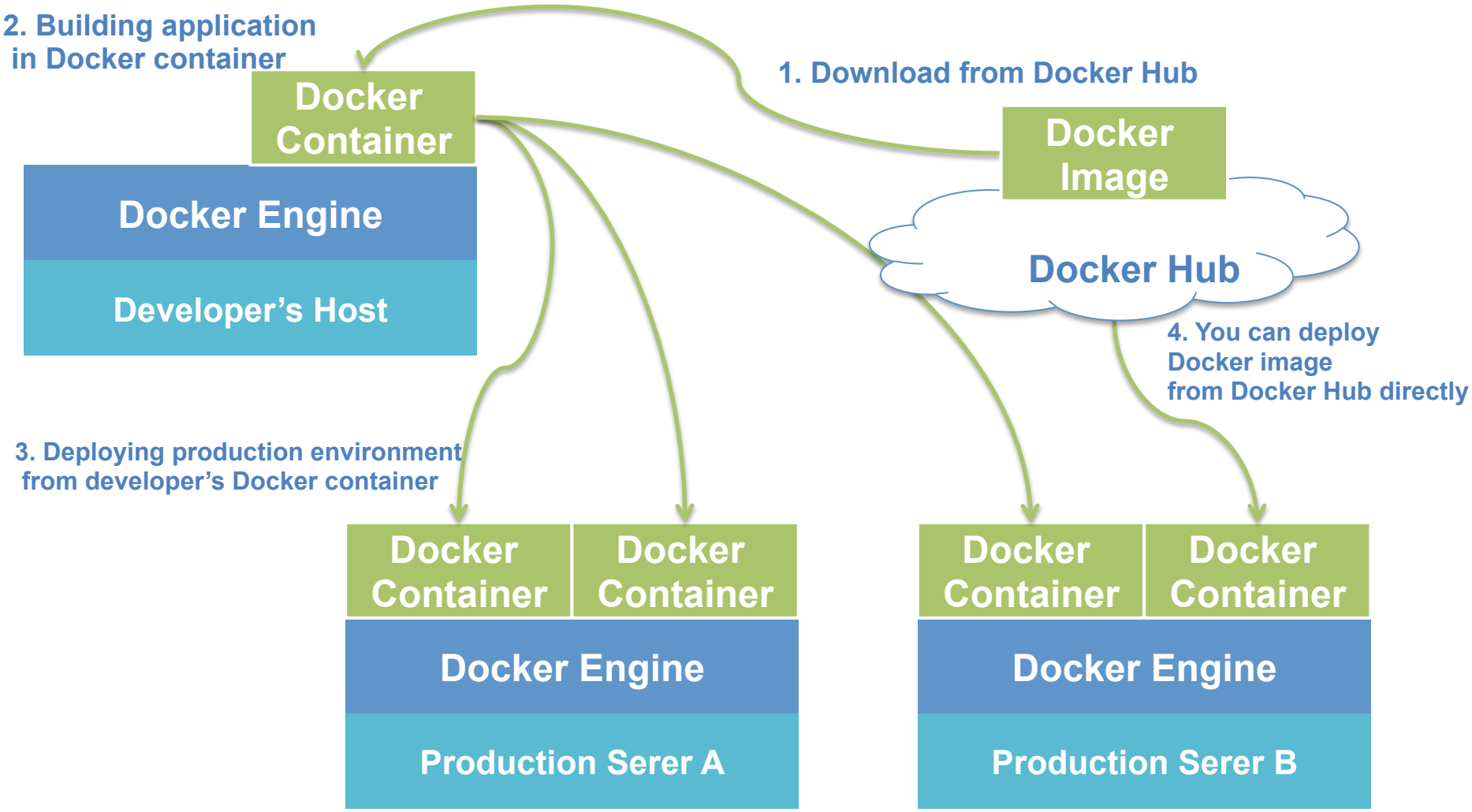
About Docker

- Docker is application deployment framework using containers and OS image version control system
  - Docker Engine
    - Including containers manager, disk controller and CLI etc.
  - Docker Hub
    - Image distribution and management platform like github

- Docker developed by DotCloud for PaaS
  - DotCloud has renamed itself Docker, Inc.

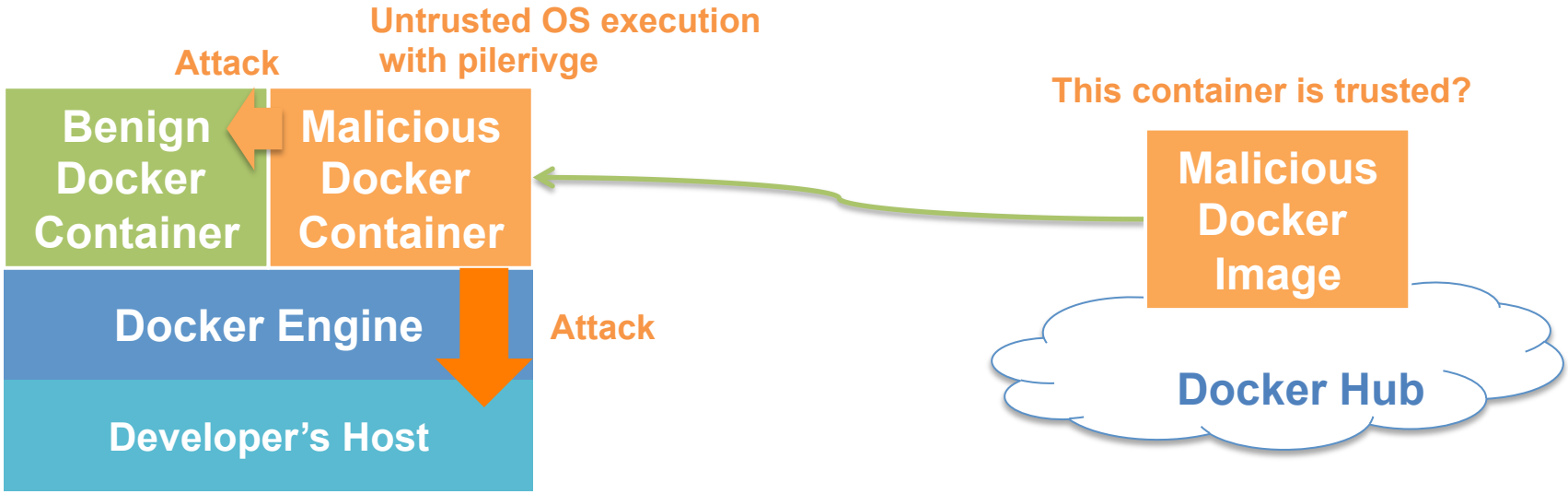
- Docker is hot topic in PaaS provider
  - Microsoft, Google and Amazon establish relations with Docker in 2014.

Scalable Deployment Cycle with Docker



Threat model of Docker

- Docker container requires root privilege
- Docker Hub is hosting service, do not guarantee images safety
  - Do you trust public docker image?



Isolation using libcontainer with SELinux

- libcontainer was integrated into Docker after version 0.9
  - In the past, lxc and libvirt used
- libcontainer isolates container using Linux capabilities, cgroup, MAC(SELinux, AppArmor)
  - In case of SELinux; libcontainer assigns MCS context dynamically

Conclusion

- To achieve secure environment requires two surfaces for isolation in virtualization and containers
  - An isolation between host OS and guest OS
  - An isolation between guests
- libvirt is sophisticated VM management framework, it has already integrated isolation with SELinux and AppArmor
- Docker is familiar to developers, but it includes security risks like execution of untrusted programs
  - We absolutely need SELinux for secure development with Docker

References

- Section 3: sVirt
  https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/6/html/Virtualization_Administration_Guide/chap-sVirt.html
- Docker and SELinux
  http://www.projectatomic.io/docs/docker-and-selinux/
- DOCKER 0.9: INTRODUCING EXECUTION DRIVERS AND LIBCONTAINER
  https://blog.docker.com/2014/03/docker-0-9-introducing-execution-drivers-and-libcontainer/
- Introducing a *Super* Privileged Container Concept
  http://developerblog.redhat.com/2014/11/06/introducing-a-super-privileged-container-concept/

Contact Information

E-Mail : research—feedback@ffri.jp
Twitter : @FFRI_Research