Container IMA using eBPF

Avery Blanchard and Lily Sturmann
Red Hat Emerging Technologies

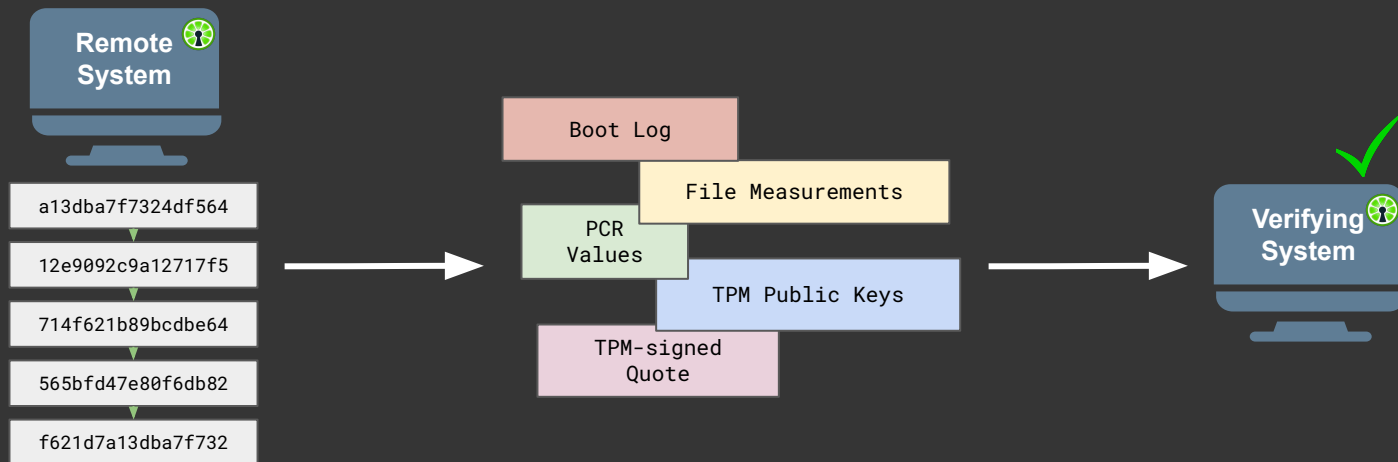March 22, 2023   Container Plumbing Days 2023

Overview

- Motivation

- Background

- Threat Model

- Implementation Details

- Future Work

Motivation

Extending Keylime remote attestation framework to individual containers

Using eBPF provides visibility for IMA while requiring no changes to the Linux kernel

Linux Integrity Measurement Architecture IMA

- Linux kernel's integrity subsystem

- IMA implementation

    - Measurement

    - Attestation

    - Appraisal

- Individual container integrity cannot be monitored by IMA as it

    measures the system as a whole

Zohar, M. An overview of the linux integrity subsystem. [LWN.net] . https://lwn.net/Articles/420001/
Red Hat on IMA: https://www.redhat.com/en/blog/how-use-linux-kernels-integrity-measurement-architecture

Red Hat

Trusted Platform Module TPM

- Microcontroller that can securely store artifacts used to authenticate the platform
- Components of a TPM
    - Non-volatile secure storage
    - Platform Configuration Registers PCR
    - Cryptographic functions (key generation, random number generation, hashing)
    - Platform Identity Keys
- Uses: remote attestation, secure boot, encrypted devices

Trusted platform module (TPM) summary. Trusted Computing Group. (2018, March 7). Retrieved October 27, 2022, from
https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary /

Red Hat

TPM: chain of trust

Each measurement in the chain incorporates the ones before it
to form an immutable record.

hash (event1) = h1

hash (h1 : hash(event2)) = h2

hash (h2 : hash(event3)) = h3

Measurements signed
by TPM's private key

Red Hat

eBPF

- Mechanism to provide a sandboxed runtime environment inside the kernel
- Programs can be attached in various places in the kernel including in system call and various kernel subsystems
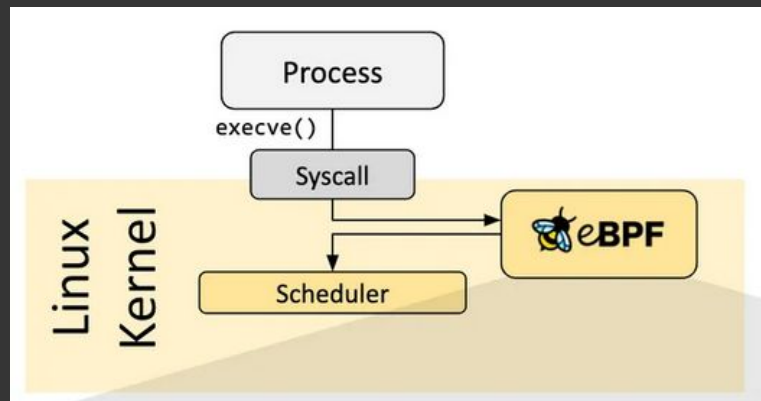

Image credit: https://ebpf.io/what-is-ebpf/

Threat Model

- Host is trusted and local attacker cannot gain ownership of the TPM
- Focus: local and remote adversaries
- Various attacks on file integrity, authenticity, confidentiality (ie. attempting to run malicious code, offline attacks)
- Detect if container integrity has been compromised, not protect against such compromise

Red Hat

Requirements

- Must provide the same functionality and interface for remote attestation as IMA
- Should not affect host IMA processes
- Architecture should not impeded the host's ability to scale
- Each container should be strongly associated with its IMA resources

Red Hat

Implementation

- Probe attests to the kernel module

- Kernel module is signed and signature is checked at boot by the OS

- Measurements are invoked by the probe

- IMA resources are namespaced

- Measurements are extended to a container's SWTPM

Architecture

- eBPF probe: **visibility** into a container's executable content **without changes to the kernel**
- Kernel Module: signed and included into a secure boot kernel to **extend trust**
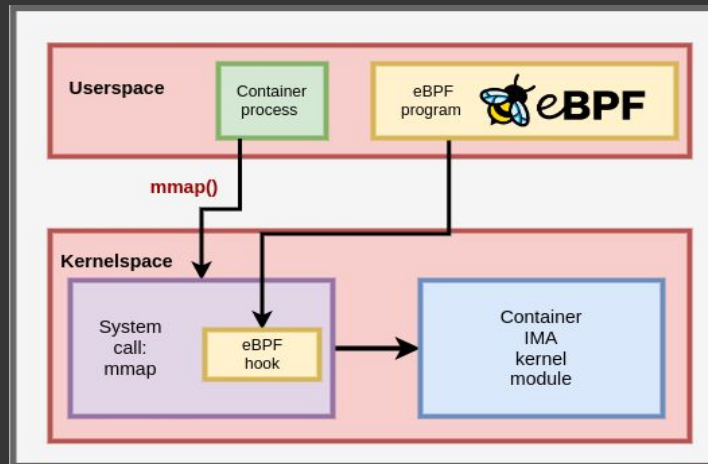
Probe Design

- eBPF program inserted into mmap system call implementation
- Invoke integrity measurement for executable content mapped by a container
- Parameters passed by probe to kernel module: namespace, address pointer, file descriptor, offset, flags, protocol

Red Hat

Kernel Module Design

- Measures and stores file integrity information

- Measurements are extend to PCR

- The value of the PCR is signed for per container attestation

- Container IMA data is separated by their namespace

- Signed to be included in a secure boot system

Red Hat

Demo

Interested in seeing a demo?

If you are a Red Hatter, join our Emerging Technologies group calls

- ▸ We're happy to have people join!
- ▸ 11am Eastern, 2nd Monday of each month

Red Hatter or not, send an email or gchat message to Lily to be included! lsturman@redhat.com

Red Hat

Future Work

- Allow for multiple policies (differing between container / host)

- Reduce complexity and overhead for scale

- Benchmarking

- Implement IMA appraisal

Red Hat

Thank you!

Keylime **https://keylime.dev/**

- Remote attestation and runtime integrity monitoring tool
- Utilizes IMA and TPM

agb2178@columbia.edu

lsturman@redhat.com

Red Hat