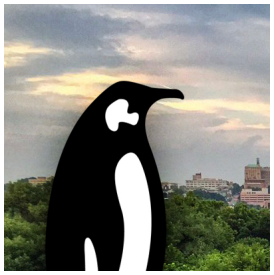

Contribution ID: **263** Type: **not specified**

BPF_LSM + fsverity for Binary Authorization

Monday, 13 November 2023 15:00 (30 minutes)

Overview

Binary authorization is a common security requirement for modern systems. Fundamentally, only securely authorized binaries are allowed to perform certain risky operations. For example, only an authenticated sshd binary is allowed to bind port 22, or only limited authorized binaries should write to raw block devices with critical data. Many proposals have sought to solve this problem, namely, fsverity, IMA, etc. However, existing solutions often fail to provide enough flexibility and fine granular control with reasonably low overhead. In this talk, we present a flexible and low overhead solution based on BPF_LSM and fsverity.

Design

In this solution, we use:

- fs-verity for file integrity checksums
- Secure binary signing service to compute and sign fs-verity hashes
- Xattrs to store fs-verity root hash signatures
- BPF_LSM to enforce access control
- User space daemon to manage keyrings and BPF_LSM programs

Kernel Work

We will need the following kfuncs to enable this work:
bpf_fsverity_get_digest() to get fsverity root hash;
bpf_vfs_getxattr() to get xattr, which contains the signature.

Note: We will have a patchset and/or a PoC for review before LPC 2023.

Primary authors: LIU, Song (Meta); BURKOV, Boris (Meta)

Presenters: LIU, Song (Meta); BURKOV, Boris (Meta)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track