Mechanismen für Containersicherheit unter Linux

Lorenz Kofler

SIB - Bachelorarbeit

Juli 07, 2021

Motivation

- Container werden immer beliebter (vs. hypervisorbasierte Virtualisierung)
- Container teilen den Kernel mit dem Hostsystem
- Container verwenden Isolationsmechanismen
- Linux Kernel Features & Linux Security Module

Fragestellung

Was sind der Stand der Technik und der Stand der Forschung von Mechanismen, die unter Linux zur Verfügung stehen, um einen Container zu isolieren und das Hostsystem vor diesem zu schützen?

- Linux Kernel Features
- Linux Security Modules

Linux Kernel Features

- Namespaces
  - Abstrahierung von globalen Systemressourcen
  - 8 verschiedene Typen:
    - Mount, Time, PID, UTS, Cgroup, User, IPC, Network
- Control Groups
  - Überwachen und limitieren des Ressourcenverbrauchs eines Containers
  - 13 verschiedene Subsysteme:
    - memory, pids, ...
- Seccomp-BPF
  - Limitieren von Systemcalls
  - somit wird die Angriffsoberfläche auf der Linux-Kernel verringert

Linux Security Modules (LSM)

- Sicherheitsmodule mittels dem LSM Framework
- Capabilities
  - Klassisch: unprivilegiert vs. privilegiert
  - Capabilities: aufteilen der Superuser-Rechte in kleine Einheiten
- AppArmor, SELinux
  - Möglichen Schaden reduzieren
  - MAC
    - Systemadministrator definiert systemweite Regeln
    - Feingranulierte Zugriffskontrolle

Linux Security Module: Probleme

- Problem: vorhandene LSMs sind nicht besonders für Container geeignet
  - Systemadministrator benötigt
  - Beeinflussen das gesamte System
- Lösungen:
  - AppArmor Namespace und benutzerdefinierte Richtlinien
  - Security Namespace
  - Landlock

Zusammenfassung

- **Namespaces**: Systemressourcen abstrahieren/isolieren
- **Cgroups**: Ressourcenverbrauch limitieren
- **Seccomp-BPF**: Systemcalls limitieren
- **Capabilities** (LSM): Aufteilen der Superuser-Rechte in kleine Einheiten
- **SELinux, AppArmor** (LSM): Feingranulierte Zugriffskontrolle