Fachhochschule Nordwestschweiz

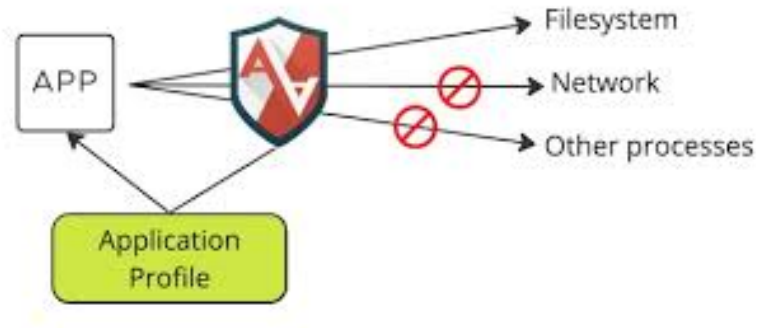
Sys Sec

25FS_IMVS14: Systems zur feingranularen Ressourcen-Zugriffskontrolle unter Linux

			Priorität 1	Priorität 2
Betreuer:	Christopher Scherb	**Arbeitsumfang:**	P6 (360h pro Student)	P5 oder P6
		Teamgrösse:	2er Team	1er oder 2er Team
Sprachen:	Deutsch oder Englisch			
Studiengang:	Informatik			

Ausgangslage

In der heutigen digitalen Welt werden Programme immer komplexer und haben Zugriff auf verschiedenste Systemressourcen wie Dateien, Netzwerkverbindungen, Kamera oder Mikrofon. Aktuelle Betriebssysteme bieten zwar grundlegende Sicherheitsmechanismen, diese sind jedoch oft zu grobgranular und für Endbenutzer schwer zu durchschauen. Linux-Systeme verfügen mit AppArmor, SELinux und eBPF über mächtige Werkzeuge zur Zugriffskontrolle, deren Potenzial für verbesserten Datenschutz und Sicherheit auf Anwendungsebene noch nicht ausgeschöpft ist.



Ziel der Arbeit

Das Ziel dieser Arbeit ist die Entwicklung eines benutzerfreundlichen Systems zur feingranularen Zugriffskontrolle von Programmen unter Linux. Benutzer sollen durch intuitive Dialoge über Ressourcenzugriffe informiert und um Erlaubnis gefragt werden. Dabei sollen sie die Möglichkeit haben, detaillierte Regeln zu definieren und diese für zukünftige Zugriffe zu speichern. Das System soll die vorhandenen Linux-Sicherheitsmechanismen (AppArmor, SELinux oder eBPF) nutzen und deren Komplexität vor dem Endbenutzer verbergen. Ein besonderer Fokus liegt auf der Benutzerfreundlichkeit und der Balance zwischen Sicherheit und Praktikabilität.

Problemstellung

Die Entwicklung eines benutzerfreundlichen Systems zur feingranularen Zugriffskontrolle erfordert die Lösung mehrerer komplexer Herausforderungen. Die technische Integration mit Linux-Sicherheitsmechanismen wie AppArmor, SELinux oder eBPF verlangt nicht nur tiefgreifendes Systemverständnis, sondern auch eine geschickte Abstraktion der komplexen Mechanismen für den Endbenutzer. Eine zentrale Herausforderung liegt in der Entwicklung einer intuitiven Benutzeroberfläche, die auch technisch weniger versierten Benutzern fundierte Sicherheitsentscheidungen ermöglicht. Dabei müssen sowohl die effiziente Verwaltung von Regeln als auch die Behandlung von Edge Cases wie verschachtelte Ressourcenzugriffe oder Systemupdates berücksichtigt werden. Zusätzlich muss das System performant arbeiten und Verzögerungen bei Ressourcenzugriffen minimieren, während gleichzeitig die Systemstabilität auch bei restriktiven Regelwerken gewährleistet bleiben muss.

Technologien/Fachliche Schwerpunkte/Referenzen

Linux Security Modules (LSM)

- AppArmor
- SELinux
- eBPF

Systemprogrammierung unter Linux