MASTER OF SCIENCE IN ENGINEERING

Forschungsprojektarbeit des Profils Information and Cyber Security

AccessSentry: Proaktive Sicherheit durch transparente Ressourcenkontrolle

Ausgangslage

Moderne Betriebssysteme, insbesondere Linux-Distributionen, verfügen oft nicht über feingranulare, benutzerfreundliche Sicherheitskontrollen auf Anwendungsebene. Während Linux robuste Sicherheitsmechanismen durch traditionelle Benutzerberechtigungen und SELinux/AppArmor bietet, sind diese Systeme komplex in der Konfiguration und Überwachung. Anwendungen, die nicht durch SELinux/AppArmor verwaltet werden, können auf alle Benutzerdaten zugreifen, was potenziell die Systemsicherheit und Privatsphäre der Benutzer gefährdet. Aktuell installieren und verwenden Benutzer häufig Anwendungen, ohne deren Ressourcenzugriffsmuster zu verstehen, was zu potenziellen Sicherheitslücken und Datenschutzverletzungen führen kann. Im Gegensatz zu mobilen Betriebssystemen, die über ausgefeilte Berechtigungssysteme verfügen, fehlt es Desktop-Linux-Umgebungen an umfassenden, benutzerfreundlichen Mechanismen zur Sicherheitsabfrage.

Zielsetzung / Methodik / Vorgehen

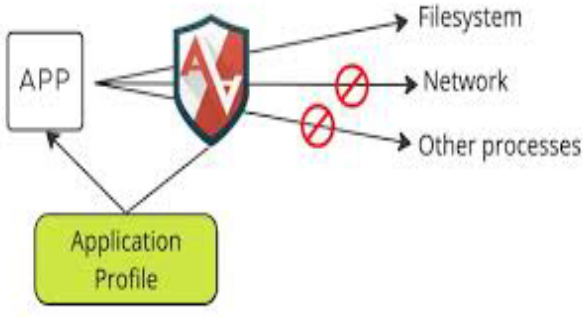
Dieses Masterprojekt zielt darauf ab, ein dynamisches Sicherheitsabfragesystem für Linux zu entwickeln, das den Anwendungszugriff auf Systemressourcen verwaltet und kontrolliert. Das System implementiert eine Sicherheitsschicht, die Zugriffsversuche auf kritische Systemressourcen wie Dateisystemoperationen, Netzwerkverbindungen und Hardware-Geräte (Kamera, Mikrofon, etc.) abfängt und verwaltet. Der Ansatz umfasst:

- Ein Überwachungssystems zum Abfangen von Ressourcenzugriffsversuchen
- Entwicklung eines regelbasierten Berechtigungssystems, das akzeptable Zugriffsmuster für Anwendungen definiert
- Eine benutzerfreundlichen Abfrageschnittstelle, die Benutzer über Zugriffsversuche informiert und Berechtigungen verwaltet
- Ein persistenten Konfigurationssystems, das Benutzerentscheidungen speichert und gleichzeitig Richtlinienaktualisierungen ermöglicht
- Sicherheitsprofile für gängige Anwendungstypen zur Empfehlung angemessener Standardberechtigungen

Das System soll mit minimalem Performance-Einfluss entwickelt werden und dabei umfassende Sicherheitskontrollen bieten. Besondere Aufmerksamkeit wird der Verhinderung von Privilege-Escalation-Angriffen und der Sicherstellung gewidmet, dass Anwendungen das Sicherheitssystem nicht umgehen können. Das Projekt wird auch die Integration mit bestehenden Linux-Sicherheitsframeworks wie SELinux und AppArmor untersuchen.

Teilaufgaben

Das Projekt kann in drei Phasen durchgeführt werden: P7: Analyse bestehender Sicherheitsframeworks, Design der Systemarchitektur und Implementierung der grundlegenden Ressourcenzugriffsüberwachung, P8: Entwicklung des Abfragesystems, der Benutzeroberfläche und initialer Sicherheitsprofile, P9: Integration mit bestehenden Sicherheitsframeworks, Performanceoptimierung und Sicherheitsevaluation.



Studienart: [x] Vollzeitstudium
[x] Teilzeitstudium 50%

Projektorganisation: Einzelarbeit

Projektfinanzierung: -

Arbeitsort: Windisch

Advisor: Prof. Dr. Christopher Scherb