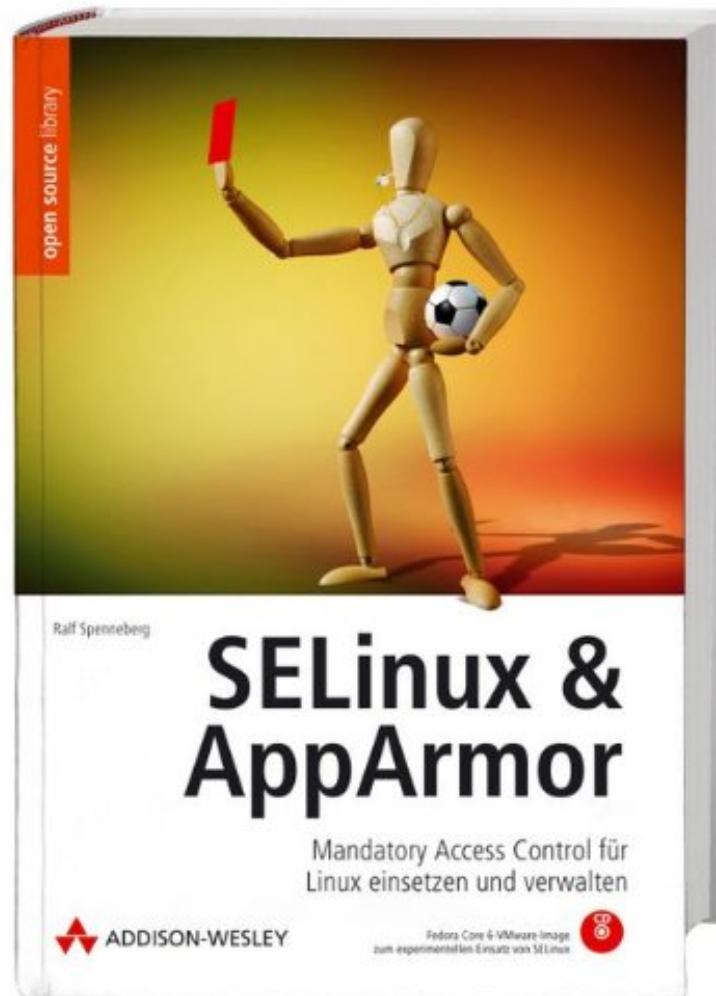


(Read free ebook) SELinux AppArmor: Mandatory Access Control fr Linux einsetzen und verwalten (Open Source Library)

## SELinux AppArmor: Mandatory Access Control fr Linux einsetzen und verwalten (Open Source Library)

Von Ralf Spenneberg  
audiobook / \*ebooks / Download PDF / ePub / DOC



[Download](#)

[Read Online](#)

Produktinformation - Verkaufsrang: #582218 in BcherVerffentlicht am: 2007-10-10Einband: Gebundene Ausgabe384 Seiten | File size: 50.Mb

**Von Ralf Spenneberg : SELinux AppArmor: Mandatory Access Control fr Linux einsetzen und verwalten (Open Source Library)** before purchasing it in order to gage whether or not it would be worth my time, and all praised SELinux AppArmor: Mandatory Access Control fr Linux einsetzen und verwalten (Open Source Library):

KundenrezensionenHilfreichste Kundenrezensionen1 von 4 Kunden fanden die folgende Rezension hilfreich. SELinuxVon LinuxTestbeide Themen gut behandelt, wobei der Schwerpunkt meines erachtens auf SELinux

liegt, nicht unbedingt ein Buch für Neulinge in diesem Bereich, gut für SELinux-Bevorzugte (so wie ich)

Kurzbeschreibung Zwei Mandatory Access Control-Systeme haben in die großen Linux-Distributionen Eingang gefunden: SELinux bei Red Hat, Fedora Core und Debian, AppArmor bei SUSE Linux. Damit gehört ihre wirksame Konfiguration und Anwendung zu den Pflichtaufgaben jedes Linux-Administrators. Ralf Spenneberg beschreibt beide MAC-Systeme detailliert, mit deutlichem Schwerpunkt auf SELinux. Er erlutert zunächst AppArmor, von der Installation über die Analyse der Überwachungsprotokolle und -berichte bis hin zu konkreten Szenarien wie der Überwachung von PHP-Anwendungen oder Shellscripts. Dann widmet er sich ausführlich SELinux und führt durch die Grundlagen, die Anwendung und erste Anpassungen, bevor er einzelne Policies und konkrete Anwendungsbeispiele wie z.B. die Absicherung eines Webservers mit SELinux vorstellt. Er zeigt außerdem, wie bestehende SELinux-Policies erweitert und eigene Policies entwickelt werden und stellt in einer Referenz die wichtigsten SELinux-Kommandos vor. Kapitel zur Installation von SELinux und AppArmor, ein Vergleich ihrer Performance sowie Kapitel über Tools zur SELinux-Policy-Erstellung und -Analyse runden das Buch zu einer Pflichtlektüre für sicherheitsbewusste Administratoren ab. SELinux (Security Enhanced Linux, u.a. von der NSA entwickelt) bietet zusätzlich zum klassischen Rechtssystem (Benutzer A aus Gruppe X darf eine Datei lesen schreiben, Benutzer B aus Gruppe Y nur lesen etc.) ein zusätzliches System, das nicht auf den UNIX-Benutzern oder Gruppen basiert, sondern abstrakte Rollen und Typen verwendet und so nicht über klassische Wege, wie die Erlangung von Superuser-Rechten o.. korrumpierbar ist. Mit SELinux und AppArmor stellt Security-Guru Ralf Spenneberg die zwei führenden Varianten MACL-basierter Linux-Systeme sicherheit vor. Nach einer Einführung in die gemeinsamen Grundlagen beschreibt er detailliert, wie gezielt oder allgemein vergebene SE-Richtlinien zur Systemüberwachung verwaltet werden oder wie AppArmor zum Schutz einzelner Anwendungen eingesetzt wird. Ralf Spenneberg hat für Addison-Wesley bereits den Bestseller VPN mit Linux sowie Intrusion Detection und Prevention mit Snort 2 Co. und Linux-Firewalls mit iptables Co. geschrieben. Er arbeitet als Sicherheitsberater und Dozent im eigenen Unternehmen, ist auf Fachkongressen als Redner und Mitorganisator anzutreffen und schreibt regelmäßig für IT-Zeitschriften. über den Autor und weitere Mitwirkende Ralf Spenneberg zählt zu Deutschlands führenden IT-Security-Experten. Mit seiner Firma Open Source Training bietet er Seminare und Consulting rund um das Thema "Sicherheit mit Open Source-Software" an. Für Addison-Wesley hat er bereits mehrere erfolgreiche Bücher geschrieben, darunter "Intrusion Detection Prevention mit Snort Co" und "SELinux AppArmor".