Evaluation of Mandatory Access Control for Database Management Systems on the Linux Platform

Felix Lange, Kim-Thomas Rehmann, Helge Deller
SAP SE, Walldorf, Germany
Felix.Lange01@sap.com, Kim-Thomas.Rehmann@sap.com, Helge.Deller@sap.com

ABSTRACT

The widespread adoption of cloud computing for enterprise software systems requires stringent access control. Mandatory Access Control (MAC) allows to implement security policies in a centralized and fine-grained manner, making it a popular choice to secure enterprise software in the cloud. However, suitable policies having low impact on functionality and performance are hard to construct.
This contribution characterizes and compares two popular MAC systems, SELinux and AppArmor, from security and performance point of view. The evaluation investigates the impact of MAC systems on the SAP HANA database management system with two Linux distributions in both non-virtualized and containerized environment.

ZUSAMMENFASSUNG

Mit einem zunehmenden Angebot sogenannter „cloud produkte“ steigt auch der Bedarf nach IT Security auf Betriebssystemebene in großen Unternehmen. Längst besteht diese nicht mehr nur aus dem Unterbinden externer Zugriffe, doch grade in Cloud-Umgebungen auch dem Absichern der Systeme gegen interne Angreifer, die Hosts aus einer Cloudinstanz heraus zu übernehmen versuchen.

Im Rahmen dessen hat die SAP Möglichkeiten der Absicherung durch alternative Verfahren der Zugriffskontrolle evaluiert, um etwa Zero-Day-Angriffe, Privilege Exploitation und Ausbrüche aus Containerumgebungen zu Verhindern.
Als Alternative zur herkömmlichen Steuerung der Zugriffskontrolle mittels Discretionary Access Control (DAC) wurde Mandatory Access Control (MAC) betrachtet. Während bei DAC Berechtigungen an Nutzer vergeben werden, werden diese bei MAC an Programme vergeben. Nutzer erhalten dann etwa über ein rollenbasiertes Berechtigungskonzept wie Role-Based Access Control (RBAC) Zugriff auf Anwendungen.

Die Evaluierung wurde anhand zweier MAC Implementierungen, SELinux und AppArmor, vorgenommen. Bei SELinux handelt es sich dabei um eine MAC Implementierung die unter anderem RBAC sowie sogenanntes Type-Enforcement in einer zentralen Policy verwendet. AppArmor hingegen verwendet textuelle Profile für einzelne Anwendungen und verknüpft diese mittels Dateipfade auf Applikationen. Dagegen bietet SELinux erweiterte Funktionen wie etwa Multi-Level Security (MLS) und Multi-Category Security (MCS), die bisher nicht in AppArmor implementiert wurden.

Betrachtet wurden unter anderem Faktoren wie der Ablauf der Berechtigungs-entwicklung, Auswirkungen der MAC Lösungen auf Applikationsperformance sowie die Sicherheit der generierten Berechtigungen. Dabei wurden die Lösungen einander gegenübergestellt und hinsichtlich dieser Metriken verglichen.

Zudem wurden im Rahmen der Evaluierung verschiedene Linux Distributionen, RedHat Enterprise Linux und SUSE Linux Enterprise Server, sowie die Containerumgebung Docker verwendet und hinsichtlich ihrer Kompatibilität mit den genannten Lösungen verglichen. Dabei wurden etwa Metriken wie Arbeitsaufwand und Support betrachtet.

Ziel der MAC Systeme war schließlich das SAP Datenbankmanagementsystem (DBMS) SAP HANA2, das es anhand weitreichender Regeln und Tests auf den genannten Plattformen abzusichern galt. Die Tests umfassten dabei weitreichende Funktionen der SAP HANA Plattform, die insbesondere eine realistische Anwendung im Betrieb reflektieren sollen. Da es sich bei SAP HANA um eine In-Memory Datenbank mit besonderem Fokus auf Performance handelt wurde insbesondere der Performanceeinfluss der MAC Lösungen betrachtet. Auf Grundlage dieser Metrik wurden erneut Rückschlüsse auf die generelle Anwendbarkeit der Lösungen im Zusammenhang mit SAP HANA gezogen.

Abschließend wurden die Anwendbarkeit beider Lösungen im Zusammenhang mit SAP HANA unter Einbezug aller genannten Metriken betrachtet und Defizite der Implementierungen aufgezeigt.