Key Management Service Integration mit FUSE

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Gerhard Hassenstein, Prof. Hansjürg Wenger
Experte: Dr. Igor Metz
Industriepartner: PostFinance AG, Bern

Was wäre, wenn keine Passwörter mehr auf den Servern persistiert wären? Sie würden nicht mehr auf Hard Disks geschrieben und damit zu einem forensischen Risiko werden, und ein Angreifer hätte nicht mehr allzu einfachen Zugriff darauf. Die in dieser Thesis entwickelte Software ermöglicht die sichere Persistierung der Passwörter in dafür vorgesehenen und sicheren Programmen auf einem eigenen System und gleichzeitig eine einfache und bekannte Schnittstelle für Applikationen.

Problemstellung

Passwörter sind kaum mehr aus der Informatik wegzudenken. In der Zeit der Digitalisierung und Automatisierung liegen sie oft im Klartext auf Dateisystemen von Servern, in der Regel nur durch Einschränkungen mittels Dateiberechtigungen vor Zugriff anderer Benutzer geschützt. Dies birgt Gefahren, da sie oft unüberlegt in Backups, Archiven, Logs oder gar in falsche Hände gelangen.

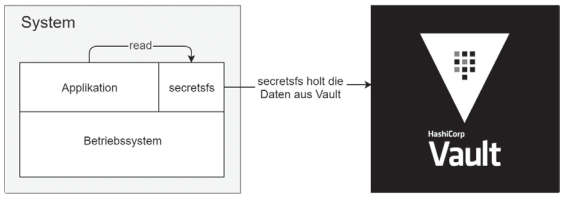
Technologien

Vault ist ein Key Management System, das Passwörter verschlüsselt in einer Datenbank ablegt. Der Zugriff auf die darin gespeicherten Daten ist nach einer erfolgreichen Authentisierung entweder mit dem Vault Client oder über die REST API sichergestellt.
FUSE steht für «Filesystem in Userspace» und ist ein Dateisystem, das selbst programmiert wird. Es ist im Linux Kernel mit einem Kernelmodul stark verankert und wird über die fuselib Library angesprochen.

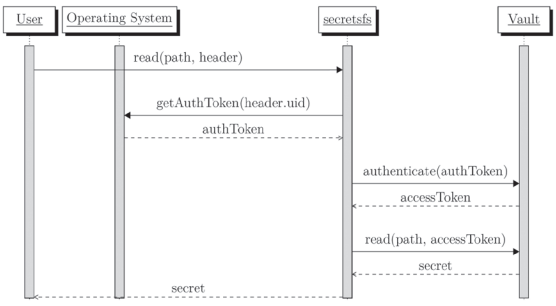
Umsetzung

Bei vielen eingekauften Applikationen ist es für Unternehmen oft nicht möglich, Wünsche an die Speicherung von Passwörtern anzubringen. Genau für diese Applikationen gibt es nun eine Lösung: Das **secretsfs** ist ein mit FUSE programmiertes Dateisystem, welches es lokalen Applikationen erlaubt, transparent auf benötigte Credentials (z. B. Startup-Passwörter) zugreifen zu können, ohne dass das Credential auf dem System einer Applikation persistiert werden muss. Das secretsfs lädt bei Bedarf das für eine Applikation autorisierte Credential vom Key Management System (Vault) und kann die Credentials in zwei Formaten der Applikation zur Verfügung stellen: Entweder direkt als Klartext-Passwort, oder in einer Konfigurationsdatei integriert und aufbereitet. Nebst dem deutlich einfacheren Erneuern von Passwörtern, bringt dieses Verfahren vorallem Vorteile bezüglich Sicherheit.

Natalie Sandra Fioretti



FUSE (Filesystem in Userspace) als einfache Passwort Schnittstelle



Authentisierung gegenüber Vault wird von secretsfs übernommen (vereinfachte Darstellung)