Password and Key Safe

Fachgebiet: IT-Security
Betreuer: Prof. Dr. Emmanuel Benoist
Experte: Dr. Igor Metz (GLUE Software Engineering AG)

Ob im privaten Leben oder im beruflichen Umfeld verwenden wir tagtäglich unzählige Programme und Dienste bei welchen man sich mit einem Passwort anmelden muss. Wie kann man sich jedoch all diese verschiedenen Passwörter merken? Im Rahmen der Bachelor Thesis wurde eine Webanwendung realisiert, welche sowohl ein sicheres Speichern, wie auch ein unkompliziertes Teilen von Passwörtern erlaubt.

Ausgangslage

Heutzutage bestehen bereits verschiedene Lösungen für die Speicherung von Passwörtern in einem System. Dabei werden die Daten entweder lokal beim Benutzer in verschlüsselten Datenbankfiles oder beim Anbieter in der Cloud gespeichert. Beide Ansätze haben jedoch entscheidende Nachteile. Bei einer Cloud-basierten Anwendung werden sensitive Benutzerdaten einem externen Anbieter anvertraut. Bei der lokalen Speicherung bleiben die Daten beim Benutzer, jedoch wird dadurch ein effizientes Teilen von Passwörtern mit anderen Benutzern verunmöglicht.

Ziel

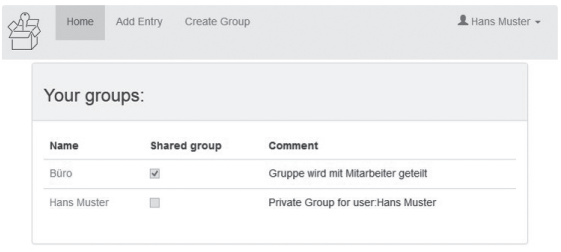
Das Ziel der Bachelor Thesis war es eine Webanwendung zur sicheren Verwaltung von Passwörtern zu realisieren. Die Anwendung soll auf einer LAMP Architektur aufgebaut sein. Neben der sicheren Verwaltung steht ein sicheres und unkompliziertes Teilen von Passwörtern im Zentrum.

Umsetzung

Das Resultat der Bachelor Thesis ist die Webanwendung «OpenKeyManager». Diese wurde grösstenteils mit PHP programmiert. Die Verschlüsselung wurde Client-seitig in JavaScript realisiert. Die Anwendung ist für den Einsatz in einer lokalen Umgebung wie zum Beispiel in einem kleineren Unternehmen vorgesehen. Dazu muss ein Administrator einen LAMP-Webserver entsprechend einrichten, auf welchen dann die einzelnen Benutzer zugreifen können und ihre Daten verwalten. Sämtliche Daten werden in einer MySQL Datenbank abgespeichert, wobei die sensitiven Informationen verschlüsselt werden.

Neue Benutzer können sich über die Webanmeldung registrieren und ihre Passwörter in Einträgen erfassen. Zur Verwaltung der Passwörter können verschiedene Gruppen erstellt werden. Bei Bedarf können diese mit anderen Benutzern geteilt werden und ihnen somit Zugriff auf die darin vorhandenen Einträge gewährt werden. Der Gruppenadministrator kann den Gruppenmitgliedern individuelle Rechte verteilen. Um das Teilen von Einträgen zu ermöglichen, ohne dass dafür ein Passwort ausgetauscht werden muss, wird asymmetrische Kryptographie verwendet. Für jeden Benutzer und jede Gruppe wird dafür bei der Erstellung ein Public / Private Key Schlüsselpaar generiert. Um eine Gruppe und deren Einträge mit einem bestimmten Benutzer zu teilen wird der Private Key der Gruppe so in der Datenbank gespeichert, dass nur derjenige Benutzer diese entschlüsseln kann, mit welchem die Gruppe geteilt werden soll.

Ein Benutzer muss nur beim Login sein Benutzerpasswort angeben und hat danach Zugriff auf alle Funktionen der Webanwendung. Sämtlich Verschlüsselungen und Entschlüsselungen, ob symmetrisch oder asymmetrisch, haben ihren Ursprung in diesem Passwort. Dank dieser Eigenschaft ist es möglich, die gesamte Kryptografie ohne erneutes Eingeben eines Passwortes durchzuführen, weder beim Erstellen von Einträgen, noch beim Teilen von Gruppen und deren Einträgen.



OpenKeyManager

Christoph Bruderer

Simon Thallinger