KryptonIT Passwort Manager

Mobile Computing und Web Applications / Betreuer: Reto König, Dr. Bernhard Anrig
Experte: Dr. René Bach

Ein grosser Nachteil bestehender Passwort Manager ist, dass diese «challenging» sind. Dadurch sind sie angreifbar. Basierend auf einer neu entwickelten kryptographischen Methode wurden zwei Passwort Manager umgesetzt: Eine interaktive und grafische Lernkomponente, um die Grundlagen der Methode zu vermitteln, und eine benutzerorientierte Applikation, um die Verwendung der Methode in der Praxis zu erforschen.

Problemstellung

Diese Arbeit befasst sich mit der Umsetzung einer kryptographischen Methode mit dem Namen KryptonIT. Die Methode soll als Grundlage für einen Passwort Manager dienen. Der praktische Einsatz der Methode ist weitgehend unerforscht. Aus diesem Grund sollen zwei Umsetzungen («Proof of Concepts») erstellt werden: Eine Umsetzung, welche in der Lehre eingesetzt werden kann, um die Grundlagen und Funktionsweise grafisch zu vermitteln; eine weitere Umsetzung, mit welcher die Verwendung aus der Sicht eines Benutzers untersucht werden kann. Bei der «Benutzersicht» soll zusätzlich die Verwendung von Kontext-bezogenen Daten (z. B. ein Wifi-Netzwerk) als Eingaben betrachtet werden, welche in einem modernen Smartphone zur Verfügung stehen. Um einen Passwort-Speicher sowohl in der erklärenden Sicht, als auch in der Benutzersicht untersuchen zu können, soll ein Austausch eines Chiffrates zwischen den beiden Applikationen möglich sein.

Lösung

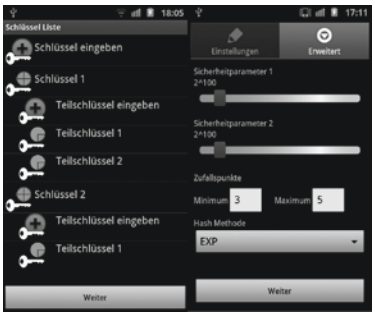
Es wurden zwei Applikationen umgesetzt. Eine Mobile Applikation auf der Basis von Android und eine Web Applikation mit Google Web Toolkit (GWT). Diese Technologien wurden gewählt, da die Umsetzung der KryptonIT Methode als Java Bibliothek bereits zur Verfügung stand.
Mit der Android Applikation können neue Chiffrate erstellt, gespeichert und abgefragt werden. Als Eingaben für die Abfrage wurden Text, der Inhalt eines QR-Barcodes, eine Wifi-Adresse und eine Kompass-Himmelsrichtung umgesetzt. Für den Austausch von Chiffraten wurden Import- und Export-Funktionen realisiert.
Mit der GWT Applikation können ebenfalls neue Chiffrate erstellt, gespeichert, und abgefragt werden. Als Eingaben für die Abfrage wurde ausschliesslich Text umgesetzt, da eine Web Applikation keine Sensoren zur Verfügung hat. Bei der Erstellung und beim Abfragen eines Chiffrates wird dem Benutzer zusätzlich eine grafische Visualisierung und ein Informationsbereich angezeigt. Diese beiden Bereiche zeigen dem Benutzer die Resultate der Berechnungen während der einzelnen Erstellungs- und Abfrage-Schritte eines Chiffrates auf. Des Weiteren hat man die Möglichkeit, ein Chiffrat zu importieren oder exportieren.

Schlussfolgerung

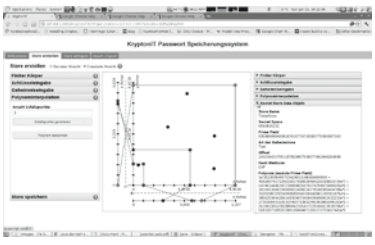
Durch grafische Untersuchungen mit der Web Applikation konnte gezeigt werden, dass die ursprünglich eingesetzten Hash-Methoden (z. B. SHA1) für die Verwendung ungeeignet sind. Deshalb musste die Umsetzung der KryptonIT Methode mit einer zusätzlichen Hash-Funktion erweitert werden.
Sowohl für die Android, sowie auch die GWT Applikation konnten wie gewünscht umgesetzt werden. Somit stehen die Resultate dieser Arbeit einerseits für die Lehre, andererseits für weitere Untersuchungen der Usability und Sicherheit der KryptonIT Methode zur Verfügung.

Louis Bernath

Jan Thomas Liechti



KryptonIT Android Passwort Manager



KryptonIT GWT Passwort Manager