Smartcard-OTP 2FA

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Annett Laube
Experte: Dr. Andreas Spichiger (Eidg. Finanzdepartement Informatiksteuerungsorgan des Bundes ISB IKT Planung und -Steuerung)
Industriepartner: SBB AG, Bern

Artikel über bemerkenswerte Datenschutzverletzungen, welche von Cyberkriminellen ausgeführt werden, sind in den Medien omnipräsent. Durch eine Zwei-Faktor-Authentifizierung, 2FA, gewinnt man eine Extraschicht an Sicherheit. In dieser Arbeit wurde eine 2FA-Methode, mit grossem Wert auf Benutzerfreundlichkeit und Sicherheit, implementiert.

Einleitung

Falls eine Zwei-Faktor-Authentisierung vorliegt, können die Kriminellen nicht mehr nur mit deinem Benutzername und Passwort Zugang gewinnen. Wenn ein gutes Protokoll und Hardware-basierter Authentifizierungs-Faktor vorliegt, ist es mit heutigen Mitteln unmöglich die Authentifizierung zu knacken. Ziel dieser Arbeit ist es, aufgrund einer Studie einen Prototypen, welcher eine 2FA-Methode benutzt, zu erstellen. Implementiert wurde der Registrierungs- wie Anmeldeprozess. Da vom Auftraggeber so kommuniziert, wurde grossen Wert auf die Benutzerfreundlichkeit und Sicherheit gelegt. Der zweite Faktor ist in dieser Arbeit ein „one time password", OTP. Dieses Passwort wird, wie der Name schon sagt, nur einmal verwendet und darf danach in keinem Fall mehr gültig sein.

Methode

Bei der 2FA-Methode interagieren 4 Komponenten:

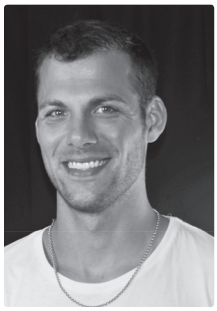
- Die NFC-fähige Smartcard ist für die Generierung des OTP zuständig. Da die Karte vom Hersteller noch nicht zur Verfügung stand, wurden die OTP auf einem anderen Gerät erstellt und auf mehreren NFC-Tags gespeichert.
- Die Authentisierungs-App auf dem NFC-fähigen Smartphone liest das OTP aus und gibt es an dem IdP weiter.
- Der „identity provider" (IdP) validiert das OTP bei der Anmeldung und ist bei der Registrierung für die Übertragung der Identifikationsdaten an das Backend des Kartenherausgebers zuständig.
- Das Backend prüft bei der Registrierung der Smartkarte, ob diese im System vorhanden und gültig ist.

Die 2FA-Methode kann entweder auf dem gleichen oder einem zweiten Gerät (z.B. Laptop) verwendet werden. Der Benutzer authentifiziert sich zunächst mit dem ersten Authentifizierungsfaktor (Benutzername und Passwort) auf dem IdP. Dieser schickt eine Nachricht an das registrierte Smartphone und holt so den zweiten Authentifizierungsfaktor, das OTP, ab. Wenn Registrierung und Anmeldung auf dem gleichen Gerät erfolgen (Smartphone) können die unterschiedlichen Nachrichten mittels Inter-App-Kommunikation ausgetauscht werden. In dieser Arbeit wurde nur die Anwendung mit zwei unterschiedlichen Geräten implementiert, da diese den allgemeineren Fall abdeckt.

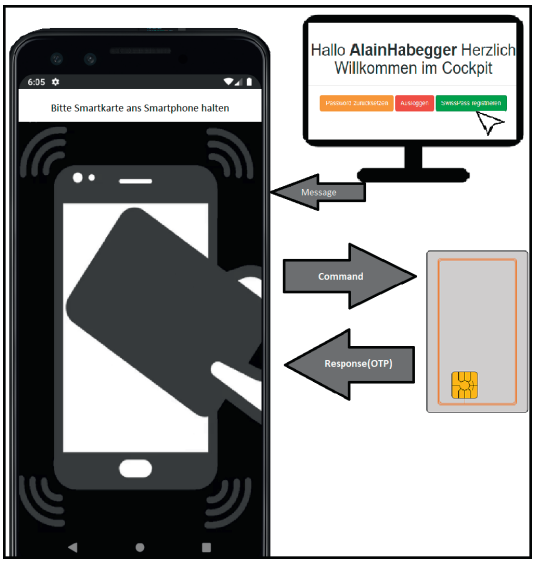
Für den Server wurde ein Raspberry PI 4 benutzt. Auf diesem befinden sich der IdP und das Backend. Serverseitig wurden PHP, HTML und Javascript für die Umsetzung benutzt. Die Smartphone-App wurde in Angular und Nativescript implementiert, da es das Ziel war eine plattformübergreifende Sprache zu verwenden. Nativescript kann für Android wie für IOS verwendet werden.

Fazit

Es war eine grosse Herausforderung den Protoypen umzusetzen, war aber sicher auch das Tolle an diesem Projekt. Meinem Auftraggeber konnte ich eine Softwarelösung übergeben, welche die Grundlage für ein zukünftiges Projekt sein könnte. In naher Zukunft wird diese Umsetzung vielleicht allgegenwärtig sein und viele Schweizer werden sie täglich benutzen.



Alain Habegger



Auslesen des OTP's