

Passwordless 2-Factor Windows Authentication

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Gerhard Hassenstein
Experte: Prof. Dr. Andreas Spichiger
Industriepartner: FIVE Informatik AG, Urtenen-Schönbühl

Mit dem Anniversary Update von Windows 10 im August 2016 unterstützt Microsoft zwei neue passwortlose Benutzerauthentisierungen: Mit der Web Authentication API ist im Webbrowser Edge von Microsoft ein Login an einer Webapplikation mit PIN oder Biometrie möglich und das Companion Device Framework erlaubt es, den Computer passwortlos zu entsperren. In unserer Bachelorarbeit haben wir uns mit diesen Technologien auseinandergesetzt und jeweils einen Prototypen entworfen.

Ausgangslage

In unserer zweiteiligen Thesis soll zuerst ein «Proof of Concept» für ein Weblogin entworfen werden, bei dem mit der Web Authentication API neben Benutzername und Passwort ein weiterer Faktor hinzugefügt wird. Im zweiten Teil soll die Entsperrung eines Windows 10 PCs mithilfe eines Prototyps, basierend auf dem Companion Device Framework, realisiert werden.

Web Authentication API

Für den ersten Teil haben wir einen Prototyp entwickelt, welcher die Web Authentication API einsetzt, um Windows Hello bei der Authentisierung zu integrieren. Anstelle einer reinen Benutzernamen/Kennwort Authentisierung kann die Identität des Benutzers nun via Windows Hello ermittelt werden. Eine angepasste Version des Prototyps haben wir für die Firma FIVE Informatik AG hergestellt. Die konfigurierbare Kombination von Faktoren bieten mehr Flexibilität und Sicherheit. Der Prototyp orientiert sich an der W3C Member Submission: «FIDO 2.0 Web API for accessing FIDO 2.0 credentials».

Companion Device Framework

Einen Client PC anstatt mit einem Passwort mit einem Companion Device zu entsperren klingt sehr interessant und erhöht die Benutzerfreundlichkeit von Windows 10. Ein Companion Device kann ein Fitness-Armband, ein Handy oder in unserem Fall ein Raspberry Pi sein. Voraussetzung für die Nutzung dieses Frameworks ist eine Kommunikationsmöglichkeit mit dem Client PC (via Bluetooth, WLAN, etc.). Auf dem Gerät wird später das Schlüsselmaterial sicher abgelegt, welches nur noch der Arbeitsstation, in Ver-

bindung mit einer Benutzer-Session, bekannt ist. Dafür wurden Applikationen für die Registrierung, Authentisierung und Kommunikation zwischen App und Companion Device in C# geschrieben. Diese ermöglichen den Austausch von HMACs, womit sich Device und Arbeitsstation gegenseitig eindeutig authentifizieren können.

Fazit

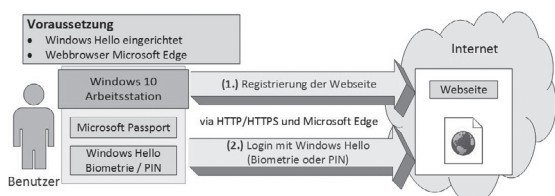
Die beiden Prototypen konnten erfolgreich umgesetzt werden und bieten einen guten Einblick in die Möglichkeiten und Limitationen dieser Komponenten. Ein nachteiliger Aspekt war, dass bei so neuen Technologien nicht viele Informationen rund um das Thema bekannt sind und kommerzielle Lösungen keinen Einblick in ihre Funktionsweise bieten. Microsoft will die Funktionalität der Web Authentication API wie auch des Companion Device Frameworks zukünftig erweitern.



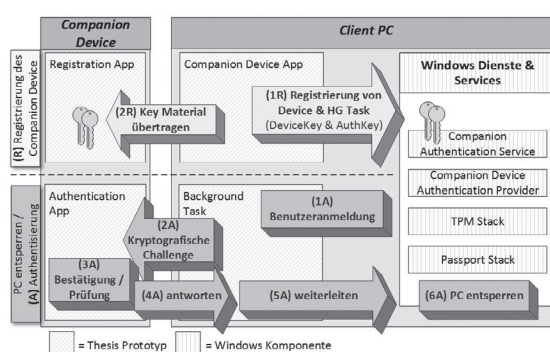
Fabian Jouko Schwab



Marcel Tschanz



Login mit Web Authentication API



Registrierung und Anmeldung mit Companion Device