Sicherheitsevaluation von Multi-Faktor-Authentifizierung im Vergleich zur Web Authentifizierungs API

Master-Thesis

Bearbeiter:

Tim Brust

Studiengang:

IT-Sicherheit und Forensik

Abgabedatum:

30.09.2019

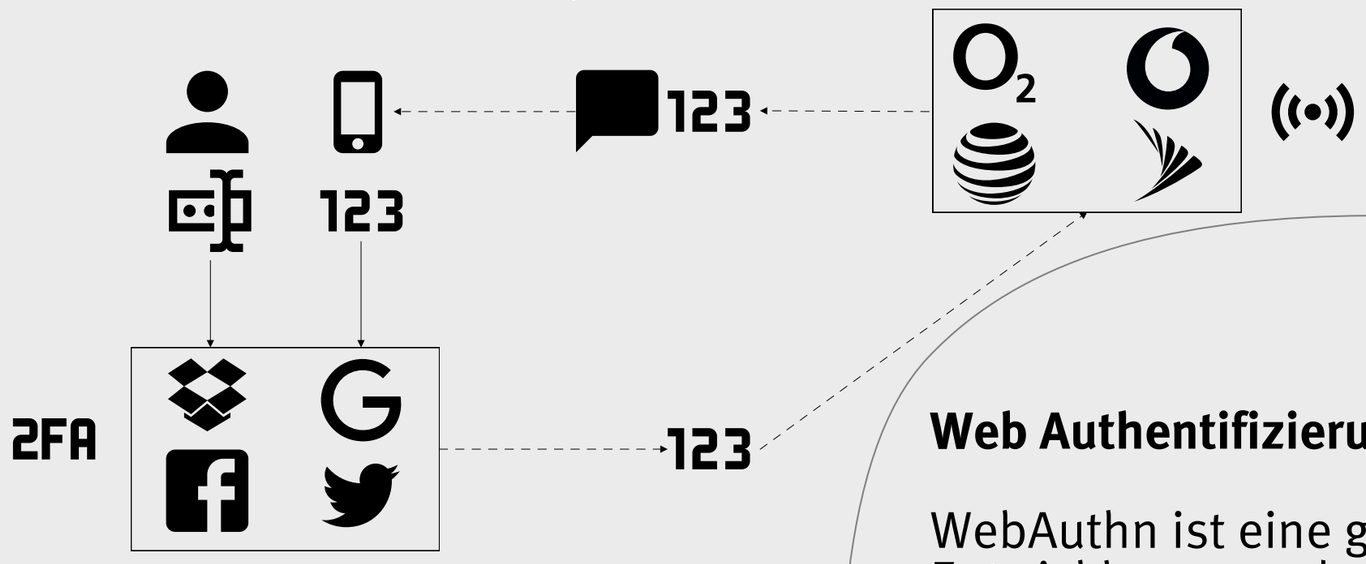
1. Betreuer:

Prof. Dr.-Ing. habil. Andreas Ahrens

2. Betreuer:

Prof. Dr. rer. nat. Nils Gruschka

Internetnutzer sind einem ständigen Risiko ausgesetzt, da Sicherheitsbrüche fast täglich auftreten. Um dieser Bedrohung entgegenzuwirken, muss der Nutzer zusätzliche Sicherheitsmaßnahmen einsetzen. Im Rahmen dieser Masterarbeit werden verschiedene Methoden der Authentifizierung und Multi-Faktor Authentifizierungen (MFA), z. B. Einmalpasswörter und Sicherheitsschlüssel, mit Fokus auf ihre Sicherheit vorgestellt und evaluiert. Weiterhin wird die Web Authentifizierungs API erläutert und mit den o. g. MFAs verglichen. Es soll die Frage geklärt werden, ob die Web Authentifizierungs als Ersatz für bestehende MFA Lösungen oder komplementär dazu eingesetzt werden kann.



(Zeitbasierte) MFA

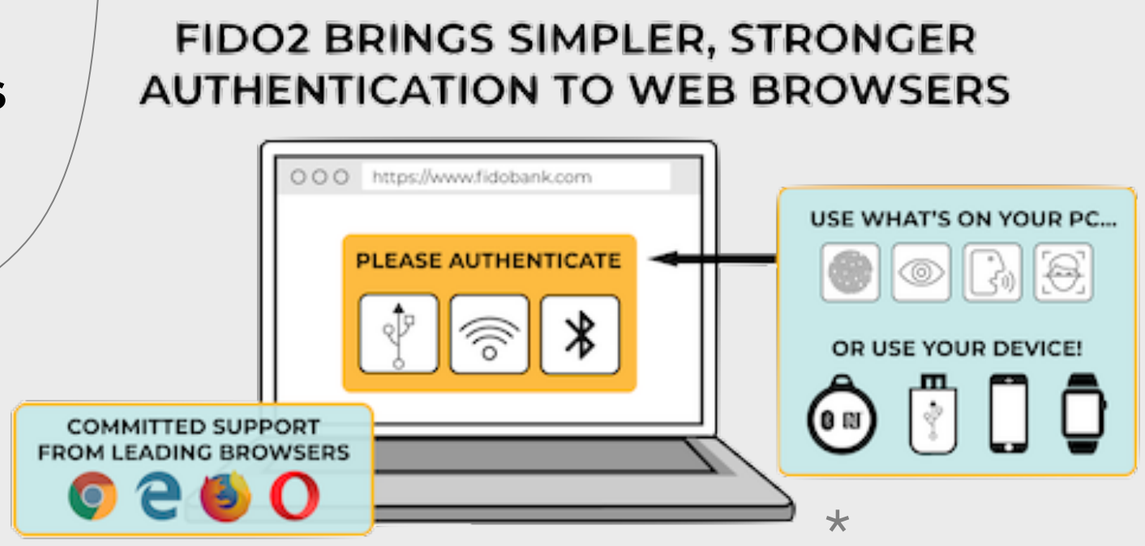
Die am häufigsten verwendete Methode von MFA zusammen mit dem Passwort ist der Besitz des „Shared Secrets“ von zeitbasierten Einmalpasswörtern. Jedoch ist besonders das Transportmedium SMS und der Service Provider anfällig für Attacken.

Zeitbasierte Einmalpasswörter sind daher nicht resistent gegenüber Phishing und insbesondere die Transportmedien ein Ziel für das Ausnutze von Sicherheitslücken und Social Engineering Attacken.

Web Authentifizierungs API (WebAuthn)

WebAuthn ist eine gemeinsame Entwicklung von der FIDO Allianz und des W3Cs und eine Weiterentwicklung des U2F Protokolls und basiert auf der Public-Key Authentifizierung. Im Vergleich zu anderen MFA Lösungen, bietet die API Schutz gegen Phishing Attacken und lässt dem Nutzer die Wahl über den verwendeten „Authenticator“.

WebAuthn bietet Schutz gegen Phishing und hat das Potenzial Passwörter zu ersetzen, ist aber noch nicht in allen Webbrowsern vollständig implementiert.



*

Fazit:

Multi-Faktor Authentifizierung kann zwar die Sicherheit erhöhen, ist aber immer noch Phishing-Angriffen ausgesetzt ist. Es erfordert ein Wechsel der Transportmechanismen oder Verfahren, um Resistenz gegenüber Phishing zu erreichen. Darüber hinaus hat die Web Authentifizierungs API das Potenzial, Passwörter zu ersetzen. Sie ist aber für den Endverbraucher aktuell noch nicht ausreichend nutzbar, da die API noch nicht in allen Betriebssystem und Webbrowsern umfassend unterstützt wird.

* Bildquelle: https://www.w3.org/2018/04/pressrelease-webauthn-fido2.html; letzter Zugriff am 03.11.2019

Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

www.fiw.hs-wismar.de