Security Evaluation of Multi-Factor Authentication in Comparison with the Web Authentication API

Master's Thesis

Author:

Tim Brust

Course of Studies:

IT-Security and Forensics

Submitted by:

09/30/2019

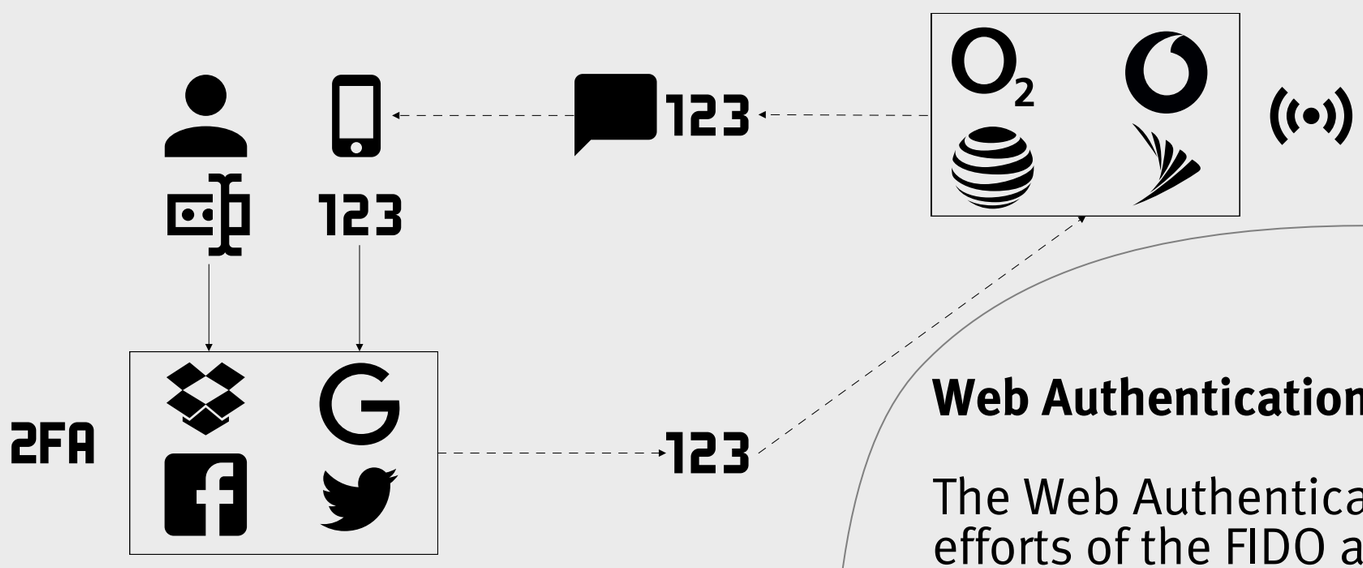
First Supervisor:

Prof. Dr.-Ing. habil. Andreas Ahrens

Second Supervisor:

Prof. Dr. rer. nat. Nils Gruschka

Internet users are at constant risk, given that data breaches happen nearly daily. In order to counter these threats, the user needs to deploy additional security measures. This master's thesis introduces and evaluates different methods of authentication and multi-factor authentication (MFA) solutions, e.g., one-time passwords and security tokens, with a focus on their security. Further, the Web Authentication API is explained and compared with the other MFA solutions. The question has to be answered, whether the Web Authentication API can replace existing MFA solutions or to what extent it can be used in conjunction with them.



(Time-based) MFA

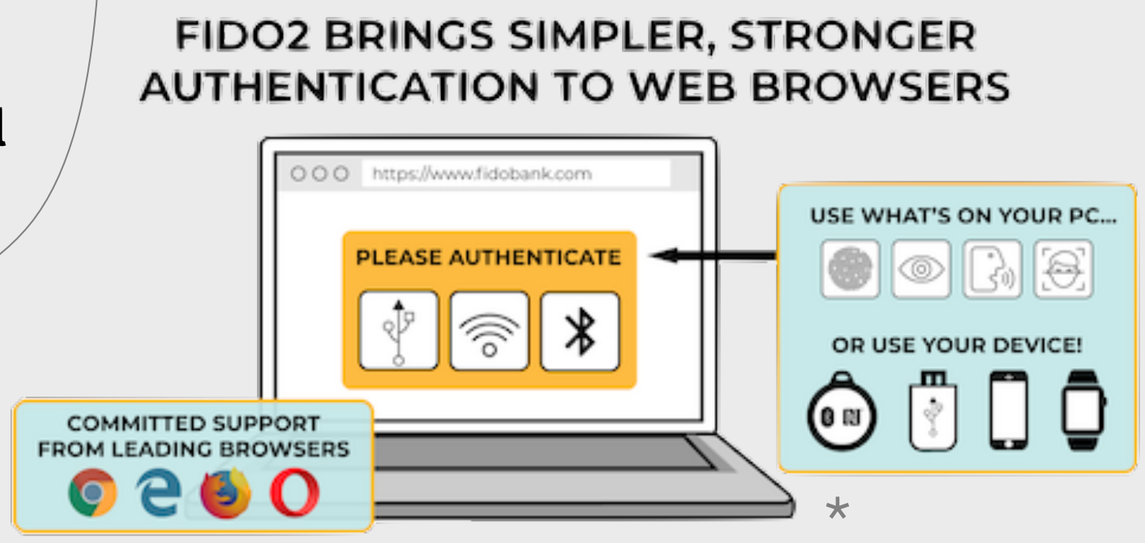
A commonly used method to achieve MFA in combination with the password is the usage of authentication by possession of the shred secret for time-based one-time password. However, the transportation mediums, such as SMS, and service providers are a lucrative attack target.

Time-based one-time passwords are not phishing resistant and especially the transportation mechanisms are a subject social engineering attacks and exploitation.

Web Authentication API (WebAuthn)

The Web Authentication API is a joint efforts of the FIDO alliance and the W3C and an evolution of the U2F protocol based on public-key cryptography.
In comparison with other MFA solutions, WebAuthn provides resistance against phishing attacks and lets the user decide which authenticator should be used, e.g., a built-in authenticator or an external token.

WebAuthn provides resistance against phishing attacks and has the potentials to replace passwords, but is not fully implemented in all web browsers, yet.



Conclusion:

Multi-factor authentication can increase the security, but is still subject to phishing attacks. It can be made phishing resistant, but it requires a change of the transportation medium or the usage of other authentication methods.
Also, the Web Authentication API has the potential to replace passwords. However, it is not yet usable enough for the end consumer, mostly because the API is not fully supported in all operating systems and web browsers.

* Source: https://www.w3.org/2018/04/pressrelease-webauthn-fido2.html; last accessed on 11/03/2019.

Faculty of Engineering
Department of Electrical Engineering and Computer Science
www.fiw.hs-wismar.de