Web Authn Implementation

Julian Stampfli (julianjimmy.stampfli@students.bfh.ch)

January 22, 2019

Contents

1 Introduction

Passwords are the most common used way to authenticate a user. They are easy to implement and have been used since the beginning of the internet. People are used to passwords and use them everywhere, but most of them use weak ones. Remembering strong passwords is not easy, thus, most opt for easier passwords or password reuse them. The newest recommendations from the NIST are actually to use very long passwords that make sense for a human. For isntance a sentence in a fictional language or with slang words. An appropriate password would then look something like 'awsumfurrycybercat', but not that. [1]

Even when user use strong passwords with this it is hard to remember a new password for every site. Thus, they will reuse passwords for multiple sites. Password reuse can lead to dangerous password credential stuffing attacks where the password that was leaked from one service can be used to access another service. [2], [3] Those are two weaknesses that passwords always had. Firstly, used passwords are generally too weak, secondly, they are reused for multiple services.

FIDO2 is a specification that aims to increase security for end users by eliminating the weaknesses that come with passwords. The main advantages are strong privacy, privacy protection, multiple choices, cost-efficiency and a layered approach. It tries to do that by using secure authenticators that are used instead of a password. [4]

The main force behind FIDO2 is the FIDO Alliance. Some noticable members are Microsoft, Google and Yubico. Microsoft for instance wants to use FIDO2 for the windows hello login. [5] With that force behind it it has been adopted in all major web browser. [6] There are also already authenticators available from yubico that can be used. [7]

This paper discusses the implementation for the replying party when the user already has a fido2 authenticator.

2 FIDO2

FIDO2 is an authentication standart wich uses public key cryptography to authenticate an user. Compared to a password the user doesn't prove that he knows something but that he has something that he previously has registered with the application. This authenticator is an external device that interacts with the application through a protocol called CTAP. CTAP is also part of the FIDO2 specification but this paper does not go into detail of how this protocol works. [8]

The WebAuthn specification forms the second part of FIDO2. This part deals with the Application that wants to authenticate an user. It contains two steps. Attestation which deals with registering a new user and assertion which handles the authentication of an existing user. Both functions are explained in the Section 3.

2.1 Main Ideas

Traditionally, when a user wants to register or authenticate, he supplies the application with a password. A shared secret that only the user is supposed to know. We already

discussed how passwords usually lead to a weak authentication. This issue was usually solved by adding a second factor to the authentication. With FIDO U2F this second factor would be very strong and the authentication would be resilient against big attacks. However, many sites offer weaker forms of second factor authentication like codes via e-mail or phone. Both of those methods are weak to message interception where an attacker intercepts the message before the end user recieves it. [9]

By using certified authenticators, FIDO2 makes sure that a user needs to have access to his authenticator and be present when the authentication is triggered. With this an attacker could still steal the physical authenticator and authenticate with it. However, this kind of physical attack can't be used to steal the authenticator for a large group of people. Additionally once the user notices that his authenticator has been stolen, he can inform the service provider and disable this authenticator for future authentications. Additionally to secure authenticators that are simply left in the USB slot of a machine, FIDO2 requires the user to be present during the authentication. With this an attacker can't simply put some malware on the users computer and trigger the login.

2.2 Authenticator

2.2.1 Level 1

2.2.2 Level 2

2.2.3 Level 3

2.2.4 Level 3+

2.3 FIDO2 vs FIDO U2F

3 Replying Party

3.1 Registration / Attestation

3.1.1 Create registration

3.1.2 Verify registration

Step1

Step2

Step3

Step4

Step5

Step6

Step7

Step8

Step9

Step10

Step11

Step12

Step13

Step14

Step15

Step16

Step17

Step18

Step19

3.1.3 Summary

3.2 Login / Authentication

3.2.1 Create registration

3.2.2 Verify registration

Step1

Step2

Step3

Step4

Step5

Step6

Step7

Step8

Step9

Step10

Step11

Step12

Step13

Step14

Step15

Step16

3.2.3 Summary

4 Conclusion

References

[1] M. Garcia, *Easy ways to build a better p@$5w0rd*, NIST, 2018. [Online]. Available: https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

[2] *52% of users reuse their passwords*, Panda Security, 2018. [Online]. Available: https://www.pandasecurity.com/mediacenter/security/password-reuse/.

[3] R. Munroe, *Password reuse*, 2014. [Online]. Available: https://xkcd.com/792/.

[4] *What is fido2?* Yubico, 2019. [Online]. Available: https://developers.yubico.com/FIDO2/.

[5] R. Manning, *Passwordless login with the yubikey 5 comes to microsoft accounts*, Yubico, 2018. [Online]. Available: https://www.yubico.com/2018/11/passwordless-login-with-the-yubikey-5-comes-to-microsoft-accounts/.

[6] *Fido2 browser support, new certified products continue momentum towards passwordless future*, fidoalliance, 2018. [Online]. Available: https://fidoalliance.org/fido2-browser-support-new-certified-products-continue-momentum-towards-passwordless-future/.

[7] J. Chong, *Introducing the yubikey 5 series with new nfc and fido2 passwordless features*, Yubico, 2018. [Online]. Available: https://www.yubico.com/2018/09/introducing-the-yubikey-5-series-with-new-nfc-and-fido2-passwordless-features/.

[8] *Client to authenticator protocol (ctap)*, fidoalliance, 2018. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html.

[9] D. Price, *It's time to stop using sms and 2fa apps for two-factor authentication*, 2018. [Online]. Available: https://www.makeuseof.com/tag/two-factor-authentication-sms-apps/.