Hardware Security Tokens In Context Of FIDO2

Seminar: Advances in Cryptography and IT-Security

Robert Hartings

December 22, 2021
RWTH Aachen
Research Group IT-Security

Organizer: Ulrike Meyer
Supervisor: Vincent Drury

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.

1 Introduction

Credentials with username and password are still the most common variant of user authentication today, despite their problems with phishing or dictionary attacks, for example. To create secure accounts, it is recommended to use strong passwords (including capital and lower letters, numbers and speical characters and a minimum length) while refraning from reuse. The user has to memorize these rather complex different passwords or use a password manager which has its own disadvanteages. If credentials are reused on multiple accounts, they are vulnerable to credential stuffing attacks, in which an attacker uses stolen credentials from one service on other services hoping for same or similar credentials, making it easier for him to guess the right combination of username/email and password. Username and password are always vulnerable to phishing, because it cannot be ruled out that even the most experienced user will make a mistake and enters thier credentials on an website owned by an attacker.

This problem is challenge by the FIDO Alliance and the W3C by providing a possible solution: The Fast Identity Online 2 (FIDO2) standard. The main difference between the proposed standard and status quo is the paradigm shift from "something a user knows" to "something a user poses". The FIDO2 standard includes a successor to the Universal 2nd Factor (U2F), which was also developed by the FIDO Alliance and, in addition to the familiar Second Factor, also offers the possibility for Singe Factor Authentication, making password as we know them superfluous. The cost, inconvenience and unfamiliarity of security keys are currently reason for thier low uptake.[LHGU21][GLSN+20]

But like other authentication variants, FIDO2 has its own unsolved problems and drawbacks. In this paper I would like to summarize these problems and possible solutions.

2 Background

2.1 Hardware Secruity Tokens (HSTs)

HSTs are used to securly store a secret key used for cryptographic functions in a tamper-resistant storage. The main idea is that the secret never leaves the secure storage. The secret key is used for deriving subsequent authentication keys for creation of public / private identities. The derived keys are mainly used to sign recived challenges, but can also be used to identiy a user.[PMD+21]

HST, also called authenticators, can be so called security keys but also integrated authenticators including Trusted Platform Module (TPM), Andriod keystore and Apple TouchID. Microsoft Hello is one example for the TPM.

Security keys from vendors like Yubico (Yubikey), Feitian (FIDO Key) and Google (Titan Key) are very popluar. In the most cases a user has to touch a sensor to verify his presence. They can also be shipped with biometric scanners / sensors, most commenly finger print sensors. If the authenticator is external, communication with the device takes place via USB, NFC (Near Field Communication) or BLE (Bluetooth Low Energy).[GLSN+20]

2.2 Fast Identity Online 2 (FIDO2)

The Fast Identity Online 2 (FIDO2) Project is an joint effort from the FIDO Alliance and the World Wide Web Consortium (W3C). It is an open authentication standard succeeding prior work of the FIDO Alliance on Universal 2nd Factor (U2F). [GLSN+20] It consits of two protocols. The WebAuthn protocol, maintained by the W3C, and the Client to Authtioacation Protocol 2 (CTAP2), maintained by the FIDO Alliance. Members of the FIDO Alliance include Amazon, Google, Meta and Microsoft.

The WebAuthn protocol specifices a JavaScript-based API used for communication between a service provider / WebAuthn relying parties (e.g. websites) and a WebAuthn client like a browser. All major browsers support WebAuthn today.[Aut21] The CTAP2 standardize the communication between a client and the (external) authentication device.[LHGU21][AWAC20]

The main idea of FIDO2 is to use public-private cryptography instead of known credentials like username and password. Furthermore, it creates a public-private keypair unique to a given application or website, which is used to sign challenges from the service and is only generated and stored on the authenticator. This is realized through a mutal authentication using a service identificator. In case of websites the authenticator recives the domain of the requesting website. Effectivley rendering phishing useless, because a relying attacker cannot provide the authenticator with the right domain.[UAA+21] Also preventing replay attacks and password theft. Tokens acquired through server breaches cannot be reverted to the original secret key on the authenticator nor can they be used to determine private keys used for other services.

To ensure quality and security the FIDO Alliance setup a metaservice which can be inquired to verify the used authenticator. The relaying party can check

if the authenticator meets the FIDO Alliance standards and has no known vulnerabilities.[AWAC20]

3 Problems of FIDO

3.1 Misconceptions

3.2 Convenience

3.3 Threats to OFA FIDO2

3.4 Downgrade Attacks

3.5 Distribution

4 Conclusion

References

[Aut21] Auth0. Does my browser support webauthn. https://webauthn.me/browser-support, 2021. Accessed: 2021-12-22.

[AWAC20] Fatima Alqubaisi, Ahmad Samer Wazan, Liza Ahmad, and David W Chadwick. Should we rush to implement password-less single factor fido2 based authentication? In *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, pages 1–6, April 2020.

[GLSN+20] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, May 2020.

[LHGU21] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "it's stored, hopefully, on an encrypted server'': Mitigating users' misconceptions about FIDO2 biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108. USENIX Association, August 2021.

[PMD+21] Katharina Pfeffer, Alexandra Mai, Adrian Dabrowski, Matthias Gusenbauer, Philipp Schindler, Edgar Weippl, Michael Franz, and Katharina Krombholz. On the usability of authenticity checks for hardware security tokens. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 37–54. USENIX Association, August 2021.

[UAA+21] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing eliminated with FIDO? social engineering downgrade attacks against FIDO protocols. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3811–3828. USENIX Association, August 2021.