Quantitative Analysis of FIDO2 Client Support

Florian Nawrath
Universität des Saarlandes
s9flnawr@stud.uni-saarland.de

Abstract

With the release of the new standard, Fast Identity Online 2 (FIDO2), integration and usage of passwordless authentication methods have become easier. FIDO2 challenges the incumbent standard for web authentication: passwords. However, it is unclear if the users can adapt to the new standard. The question we want to answer is: Do users have the necessary hardware available and if so does this hardware work as intended? This paper aims to test the client support of FIDO2 passwordless authentication methods with the goal of providing insights into technical as well as hardware limitations and restrictions from the users' side. To test this, we conducted a study, where the users had to attempt passwordless registration with their own devices. The results indicate that most of the successful registrations were limited to platform authenticators. Additionally, there are browser and operating system combinations that do not work together as they are still in development. According to our participants' statements, although some of them accept the new standard, there are still trust issues and misconceptions regarding the security of passwordless authentication. Despite that, FIDO2 has the potential to become the new default for web authentication. However, there is still some work to be done, when it comes to the support of certain operating systems and browsers, as well as the users' awareness and acceptance.

1 Introduction

The incumbent method to authenticate to web services are passwords. This can be traced back to their easy and low-cost implementation [2]. Although they are good in theory, there are many problems concerning the practical usage and creation of passwords. Theoretically, a password with a high entropy would be hard to break but it is also hard to remember. This problem of memorability causes users to choose passwords containing personal information, such as names of family members, pets, or dates of birth. This makes social engineering and dictionary attacks more effective. Additionally, users have an inclination to reuse passwords [9], again decreasing account protection, as one leaked or breached password may grant access to multiple accounts. The most common threats remain database breaches, social engineering attacks, and phishing [11].

Mitigating the mentioned problems can be challenging, because in general users prefer usability over security [5]. This is because users tend to construct their own mental models of security threats, based on often inadequate security knowledge. Most users justify their security choices by arguing that they are no potential target or that their passwords contain a degree of personalisation not comprehensible by an attacker. Although many users prefer convenient and quick biometric authentication methods [3], such as fingerprints or FaceUnlock, these are currently almost exclusively being used for unlocking the screen of their smartphones or laptops. Therefore, common authentication on web services still remains vulnerable.

But there is a new solution that promises to replace text-based passwords by building on top of hardware tokens ("authenticator" devices) and incorporating biometric authentication: Fast Identity Online 2 (FIDO2). This standard consists of two protocols: the Web Authentication Specification (WebAuthn) by W3C and the Fido Alliance's corresponding Client-To-Authenticator-Protocol 2 (CTAP2). The goal of the Fido Alliance is to create a passwordless and secure future for authentication in the web. The Fido Alliance has over 300 members including Google, Paypal, Visa, Windows, Apple, Facebook, and Twitter, all interested in pushing the new standard. Authenticators using the CTAP2 protocol are also known as FIDO2 or WebAuthn authenticators and will be the

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

main focus of this paper. FIDO2 authenticators are split into internal (platform) and roaming (cross-platform) authenticators. Roaming authenticators can be connected via Bluetooth Low Energy (BLE), Near Field Communication (NFC), and USB. Platform authenticators, as the name suggests, are integrated into the client platform such as mobile devices or laptops. But even when the standard is properly integrated into websites, it can only be used if users are equipped with supported hardware. However currently it is unclear, which types of authenticators the users possess, do the authenticators work as intended, and if so, can users use them?

In this paper the users' client support of FIDO2 authentication methods is evaluated. We set up a study website using the current standard [4] and we tested our participants' ability to register with the two types of authenticators, platform and roaming, respectively. The goal of this paper is to provide insights into technical limitations and restrictions from end-users. These insights are collected by hosting a user study on Amazons Mechanical Turk (MTurk), letting users register with their own devices on the study website for quantitative evaluation, followed by a short qualitative survey, asking about the problems encountered.

2 Research Questions

This paper aims to answer the following research questions:

1. Are users able to successfully register with FIDO2 on their own device?
2. Is there a difference in successful registrations between desktop and mobile platforms?
3. Is there a difference in successful registrations between platform and cross-platform authenticators?
4. Which problems do the users encounter during registration?

Hypotheses: Since current mobile devices come with an integrated authenticator (such as ARM TrustZone) using fingerprint sensors or front cameras compliant with the CTAP2 protocol, it can be expected that they have a higher success rate. For desktop devices, this is rather rare and for laptops such additional hardware (e.g. biometrics or iris scanners) comes with a higher price for the device. The same holds for the comparison of platform and cross-platform authenticators as external hardware, such as security keys, has to be purchased. The resulting hypotheses are as follows:

- H_A1 : There are more successful FIDO2 registrations when using mobile than desktop devices
- H_B1 : There are more successful platform than cross-platform registrations

3 Methodology

To evaluate the users' client support when using FIDO2 on their own devices, a website was built, with the current FIDO standard [4] integrated and the additional functionality of logging the users' browser and operating system including the corresponding versions (if available). This way, external validity was ensured and the validation of the success rate was not reliant on self reported data. To guarantee an equal distribution, the recruitment was split into two groups: $Group_{mobile}$ and $Group_{desktop}$. Mobile devices include any smartphone or tablet except Surface tablets or similar devices as they use Windows as an operating system, which is no mobile operating system. Desktop devices include operating systems like Windows, MacOS or Linux.

Before starting the study, the participants were informed about the voluntary participation, the right to decline continuation at any time, estimated duration, payment, and were ensured of the anonymity of the results. The participants were instructed to click two buttons, attempting to register with their device integrated authenticator and an external authenticator, if available. The groups were separated according to their operating system, because it is easier to attempt both registrations on one device instead of registering one of the methods on two different devices. Therefore evaluation of H_A1 can be done with this between-groups design. As for H_B1 all results are combined and evaluated with respect to the, within the study separated, registration attempts.

The final part of the study was a qualitative survey for collecting additional insights. These consisted of demographics (age, CS education), previously used authentication methods, current authenticators in the participants' possession and a text field to describe the encountered problems, if the registration failed. In total there were 161 participants with 81 in $Group_{desktop}$ and 80 in $Group_{mobile}$.

The participation was considered successful if both buttons where clicked and thereby platform and cross-platform registrations were attempted. Additionally the post study questionnaire had to be completed.

Recruitment: Due to the large number of required participants, a reliable way of recruitment with integrated payment functionality was needed. We decided to use MTurk due to the work by Redmiles et al. [10] showing that MTurk provides a representative sample from the population of the United States. The study was designed to take no more than 5 minutes with the participants being compensated $1. According to Hara et al. [7] the average payment per hour amounts to $7.25. The decision to exceed this value was made in order to encourage the workers' participation. Although finishing the task takes only 5 min, we allowed 90 minutes to finish the task to not unnecessarily pressure the participants.

Application for IRB approval at our institution is not mandatory but at the discretion of the researchers (e.g., depending on requirements in a CfP or by a funding body as well

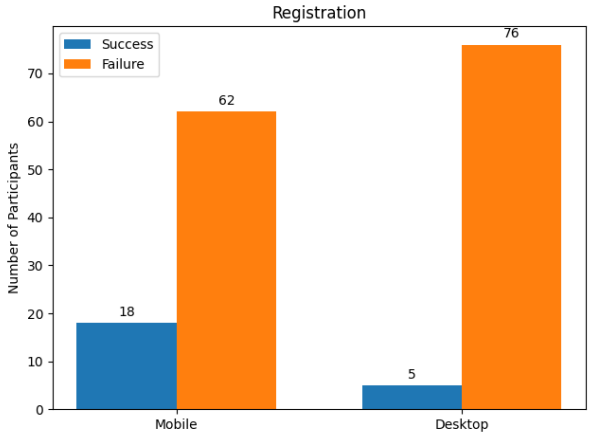

Figure 1: Successes & Failures for registration per participant

as following ethical research guidelines). After considering the extent of the data we collect (we do not store any primary user information that can be used to identify participants) and ensuring we follow ethical research guidelines—minimal risks to individuals, voluntary consent and option to leave the study at any point, privacy protection, security best practices for data protection (the survey was hosted on a maintained server with support for SSL/TLS with a university CA issued certificate, where only involved researchers had access to the collected data), no deception of participants, fair wages for MTurk workers—we decided to forego an IRB application for the BSc thesis that underlies this paper. Regardless, in retrospective, it would have been better if this study had undergone the review process as external review can catch issues undetected in internal review.

4 Results

$Group_{mobile}$ had a total of 18 out of 80 participants that managed to successfully register, while the $Group_{desktop}$ had 5 out of 81 as shown in Figure 1. All of the 18 successful registrations in $Group_{mobile}$ used a platform authenticator (5 with CS background). As for $Group_{desktop}$, 4 participants registered with a platform authenticator (1 with CS background) and 1 with a cross-platform authenticator (with neither a CS background nor having registered a platform authenticator). The demographics of our participants are summarized in Table 1.

$Group_{mobile}$ used two kinds of operation systems: 49 Android (61.25%) and 31 iOS (38.75%), while there were three operating systems used in $Group_{desktop}$: 70 Windows (86.42%), 5 MacOS (6.17%), and 6 Linux based (7.41%). The browsers used by the participants are shown in Table 1.

The evaluation of the results showed that the five successful registrations in the $Group_{desktop}$ where using the combination of Windows 10 and Chrome Version 88. As for the $Group_{mobile}$ the successful registrations were on Android with Chrome or a Chromium based browser (different versions of Android and Chrome).

Variable	$Group_{mobile}$	$Group_{desktop}$	total
N	80	81	161
CS background	21 (26.25%)	26 (32.1%)	47 (29.2%)
$platform_{success}$	18 (22.5%)	4 (4.94%)	22 (13.66%)
$cross\text{-}platform_{success}$	0 (0%)	1 (1.23%)	1 (0.62%)
$total_{success}$	18 (11.25%)	5 (3.09%)	23 (7.14%)
$total_{fail}$	62 (88.75%)	76 (96.91%)	138 (92.86%)
Browser			
Chrome	56 (70%)	67 (82.72%)	123 (76.4%)
Safari	23 (28.75%)	1 (1.23%)	24 (14.9%)
Firefox	1 (1.25%)	13 (16.05%)	14 (8.7%)

N = number of participants; CS background = computer science education

Table 1: Demographics & Success Rates

5 Discussion

Mobile vs. Desktop The question arising is: What are the reasons for the significant (chi square with a contingency matrix: $\chi^2 = 7.48$, $p = 0.006$) difference in successful registrations between the devices (H_A1)? First of all, most of the current mobile devices using iOS, Android or similar operating systems possess an integrated authenticator (using hardware such as ARM TrustZone) compliant with FIDO2, thereby supporting passwordless authentication with fingerprint sensors, FaceUnlock, or the devices' PIN. When conducting the study in Feb 2021, iOS version 14.5 was not released, therefore explaining no successful registrations with iOS devices at the time. By now, for most mobile users FIDO2 compliant authentication methods are therefore already available.

For desktop devices and laptops, it is rather common that they have integrated hardware (e.g. TPM) that can be used by an authenticator. But for desktop devices, users encounter another problem: Even with a fully functioning platform authenticator on desktop devices, it has to be configured first depending on the operating system (e.g. Windows Hello).

As for cross-platform authenticators, with the most used authenticator type here being security keys, another problem arises. In addition to people without computer science background often not knowing about security keys, they also have to spend money on it. Common users do not see the necessity to buy additional hardware as their current authentication methods work. This seems to be the case, as the results show that only one participant (who also had no computer science background) successfully registered a cross-platform authenticator within this study. Although the number of participants is limited and a larger study may show different results.

The survey offered the participants the opportunity to indicate if they possess either a platform or cross-platform authenticator on their current device, e.g *Do you possess a Security Key (Yubikey, Strongkey or similar)?* For both groups, more

participants indicated that they had authenticators in their possession, than there are successful registrations, with 48 participants of $Group_{mobile}$ indicating that they possess an authenticator (47 platform, one cross-platform) and 25 of $Group_{desktop}$ (23 platform, 2 cross-platform). There could be a variety of reasons why their registrations were not attempted or failed. First of all, despite the question if they have the authentication method on their current device available, some participants described the problems encountered with having the registration options on another device: "[...] *using my laptop instead of my smartphone*[...]" (P_{101}). Then there were participants with trust issues regarding their sensitive information that seemingly stem from misconceptions about how WebAuthn works: "*I did not want to enter my PIN as I was not sure what your program would do with that information*" (P_{87}). The most likely reason for their failed registration, if not canceled on purpose (P_{127}: "*I cancelled it*"), relates to the current platform/browser support of FIDO2. It has to be added that, after conducting this study in Feb 2021, iOS version 14.5 was released, effectively enabling single factor authentication with FIDO2. Still, for Android based smartphones only Chrome and Chromium based browsers support FIDO2. As for the participants from $Group_{desktop}$, it can only be suspected that their device had no supported hardware available or was not configured (e.g., Windows Hello set up).

Due to the ease of use of mobile devices and their commonly already configured authentication methods, results point at FIDO2 being a rather mobile-friendly solution when no cross-platform authenticator is available. Pre-configured platform authenticators on mobile devices seem to be more applicable for end-users than additionally bought external hardware, when it comes to passwordless authentication.

Platform vs. Cross-Platform: We further found a significant difference (McNemar: $p < 0.001$) between the authenticator categories platform and cross-platform (H_B1) for successful registrations. There are different factors that have to be considered which could explain the difference in the numbers of successful registrations (22 platform, 1 cross-platform). The currently most used form of cross-platform authenticators is security keys. Although studies [6], [8] showed that security keys are perceived as highly usable, despite drawbacks like the form factor and the recovery options, the users' perception was measured when having a security key at their disposal. As they have to be additionally bought and by being external from the device, which some perceive as an inconvenience [5], especially because of the fear of losing it, only a small percentage of users actually possess them. If users are already provided with a FIDO2 conform platform authenticator, given they actually use FIDO2, they do not see the need to purchase one or even two security keys, which would be the recommended recovery option [12]. Thereby the intended use-case and advantage over platform authenticators is ignored: They can be utilized on multiple platforms. But so can passwords. A recent study has shown that, although provided with the necessary hardware, users prefer to keep on using passwords [5], due to them not caring about the increased security, but being annoyed by carrying the additional hardware. Still there are many frequently used websites like Google, Dropbox, Facebook, Twitter, and Github that have fully integrated FIDO2 and thereby support security keys on their websites. Google presented a study [8], in which they enrolled FIDO Universal Second Factor (U2F) over two years within their company for more than 50,000 employees, reporting not only internal positive feedback, but also from their users regarding the U2F availability integrated into their services. Although their results and the continuous support of the standard are promising for a passwordless future, a goal also shared with Microsoft and the Fido Alliance, there is still some work to do when it comes to users' awareness and acceptance.

Because of security keys' drawbacks, there is a tendency to platform authenticators. As they are already integrated, users can adopt FIDO2 without the need to buy additional hardware. Therefore, platform authenticators seem to be the primary method for FIDO2, at least during the early adoption phase by end-users.

Internal vs. External Validity: By testing participants' capability of registering FIDO2 authenticators on their own devices, the study results have a high external validity. Previous work [6] mostly focused on checking on the users' interactions with FIDO2 and passwordless authentication in lab studies. The insights those studies provided, although promising regarding acceptance and usability, were limited by the controlled environment. This holds especially as the participants were provided with hardware. The advantage of our papers' findings is that the availability of passwordless authentication methods is tested in the wild on the actual users' devices. At the same time we had the disadvantage of not having control over which devices in which configurations the participants used and were reliant on binary results and self-reported data for the evaluation. Despite that, we can confirm some results of previous work (e.g. trust issues). Additionally we can provide new insights regarding passwordless authentication with FIDO2.

6 Limitations

As expected, there are certain limitations and biases of the study design that have to be discussed. Regarding the qualitative data collected via the survey, unfortunately most of the participants filled out the free text answers inattentively. Still, due to the studies' main purpose being quantitative evaluation of the users' client support, qualitative answers were only considered when they could shed additional light on the quantitative data, from which we derived our results.

The study duration is also a factor to be considered. As the study was designed to take only 5 minutes, there were certain questions that could not be asked and some considerations

had to be done regarding the importance of the questions. For example, the browser and operating system used by participants were solely logged on the study website by saving the user agent. This string can be altered, although we assume this is uncommon for layman end-users.

Another expected bias emerging from the participants' thoughts about the study is trust. Some participants, even if intrigued by the research conducted, were worried about sensitive data being stolen if they registered [1]. Our instructions clearly stated that no sensitive data of any kind would be logged. Still, for some participants, this was a risk they were not ready to take, thereby reducing successful registrations. Only a few participants used the possibility to voice their concerns about this in the survey, but it has to be expected that others felt so as well, without explicitly stating it.

7 Conclusion

Besides some participants having trust issues regarding the safety of their personal data when using passwordless authentication in our study setup, the main issue is the FIDO platform/browser support. For Android, the only browser that works with an internal authenticator is Chrome (or Chromium based). For other browsers, full Webauthn support is in development, so the only thing that users affected by this limitation can do, is to wait. As mentioned before, the problem encountered in this study regarding the internal authenticators on iOS devices has been fixed with the release of iOS version 14.5. Still, the problem with roaming or cross-platform authenticators remains. As most users do not see the necessity of purchasing additional hardware for authentication purposes (yet), shown by the low number of successful cross-platform registrations (see Table 1), FIDO2 appears to be a platform authenticator oriented solution, at least for the early adoption and maybe even beyond that early phase. Because of that, users' acceptance of the new alternative is better for mobile devices, as it is more common for them to have integrated and configured internal authenticators.

In conclusion, although FIDO2 is supported, integrated and pushed by many big companies such as Google, Windows and Facebook, increasing hardware support for end-users is still an ongoing effort and the availability of multiple types of authenticators in the early adoption phase by end-users might potentially bias the users' mental models towards certain authenticator designs and features, such as an association with biometrics rather than tokens.

Acknowledgments

We would like to thank our anonymous reviewers for taking the time for revising this paper and providing valuable feedback. A special thanks goes out to my supervisor of the thesis, which this paper is based on.

References

[1] "it's stored, hopefully, on an encrypted server'': Mitigating users' misconceptions about fido2 biometric webauthn. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, August 2021.

[2] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567, 2012.

[3] B. Dike-Anyiam and Q. Rehmani. Biometric vs. password authentication: A user's perspective. *Journal of Information Warfare*, 5(1):33–45, 2006.

[4] J. Cullum et al. Fido2 library. https://github.com/webauthn-open-source/fido2-lib, 2020.

[5] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth. "you still use the password after all" – exploring fido2 security keys in a small company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 19–35. USENIX Association, August 2020.

[6] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. 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, 2020.

[7] K. Hara, A. Adams, K. Milland, S. Savage, C. Callison-Burch, and J. P. Bigham. A data-driven analysis of workers' earnings on amazon mechanical turk. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14, New York, NY, USA, 2018. Association for Computing Machinery.

[8] J. Lang, A. Czeskis, D. Balfanz, and M. Schilder. Security keys: Practical cryptographic second factors for the modern web. In *Financial Cryptography*, 2016.

[9] S. Pearman, J. Thomas, P. Emami Naeini, H. Habib, L. Bauer, N. Christin, L. Cranor, S. Egelman, and A. Forget. Let's go in for a closer look: Observing passwords in their natural habitat. pages 295–310, 10 2017.

[10] E. M. Redmiles, S. Kross, and M. L. Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1326–1343, 2019.

[11] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. *Do Users' Perceptions of Password Security Match Reality?*, page 3748–3760. Association for Computing Machinery, New York, NY, USA, 2016.

[12] Yubico. Backup Recovery Plan. https://www.yubico.com/blog/backup-recovery-plan/, 2019. [Online; accessed 4-March-2021].