Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones

Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, Tatsuru Higurashi
Yahoo Japan Corporation

Abstract

Web Authentication (WebAuthn) is an authentication standard developed by the World Wide Web Consortium (W3C) that enables passwordless login to a website using a variety of authentication methods. While the security issues of biometrics through WebAuthn and its widespread usage may be solved by technological advances, we anticipate that various usability challenges will remain. Therefore, we conducted a first usability study on passwordless authentication using WebAuthn-enabled Android smartphones for consumer users. In particular, we focus on fingerprint authentication as a WebAuthn biometric in this study. We conducted objective, quantitative (SUS), and subjective analyses for the participants' behavior and comments and were able to clarify key design implications, especially pertaining to the setup process. Our findings cover usability implications applicable to all Android WebAuthn-enabled sites.

1 Introduction

Biometrics, especially those related fingerprints or the face, are now common on many smartphones and are utilized by many users to unlock screens. With fingerprints, the rate at which users utilize lock screens has increased [6], and the use of physical user biometric information is now being accepted as an alternative to entering passwords, PIN numbers, or patterns.

Passwords have traditionally been the most popular form of Web login. However, passwords come with significant security and usability problems [2, 10, 13, 16], and users often reuse one password for multiple accounts and/or use simple passwords.

Various methods have been proposed to enhance passwords. One of the most common enhancements offered by commercial services is two-factor authentication (2FA) [5, 7, 8, 11, 15]. Although 2FA has strengthened password security, it requires the use of other devices, SMS numbers, or email addresses in addition to the password input, which makes it trickier to use than a simple password.

Another technology that has attracted attention for passwordless authentication is Web Authentication (WebAuthn) [14], which is a W3C standard. By using WebAuthn, various authentication methods can be provided to users when they log in to a website. Biometrics such as fingerprints are increasingly considered viable alternatives to passwords among these authentication methods.

In 2018, our website [1] became the first commercial portal in the world to adopt WebAuthn in response to the problem of user passwords. Our users can log in using fingerprint authentication instead of passwords. In particular, on Android smartphones, it is possible to selectively adopt a screen unlocking method such as a fingerprint-based one that users can utilize on a daily basis as a login method. However, not all users have chosen to log in without a password, and we assume there must be certain usability barriers users feel that prevent them from adopting the new method. We conducted this study to clarify what these might be.

To this end, we conducted an observation study to investigate the usability of WebAuthn registration and authentication using Android smartphones and clarified the challenges we need to solve so that users feel more comfortable using WebAuthn-based fingerprint authentication in a passwordless fashion. Our WebAuthn server can provide consumer users with various authentication methods that can be accessed by WebAuthn. In this study we focus on the Android phone, where fingerprint authentication is currently available via the WebAuthn API.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

[1] https://www.yahoo.co.jp/

2 Methodology

We conducted an observation study in November 2019 to figure out the challenges facing users when they register authenticators for passwordless authentication with our WebAuthn-based services.

Recruitment. We requested a research firm to recruit Android smartphone users who had never completed the WebAuthn registration for our authentication service or who had tried but failed the setup process for some reason. We also requested them to gather as close to the same proportion of males and females in well-balanced age ranges as possible so we could obtain views from various angles. Eventually, the participants who agreed to the conditions of this study visited our office for an interview.

Demographics and Profiles. Five females and five males participated in our study. The research firm collected their personal information including gender, age, occupation, and profession (see Table 1).

Table 1: Demographics and profiles of participants ($n = 10$)

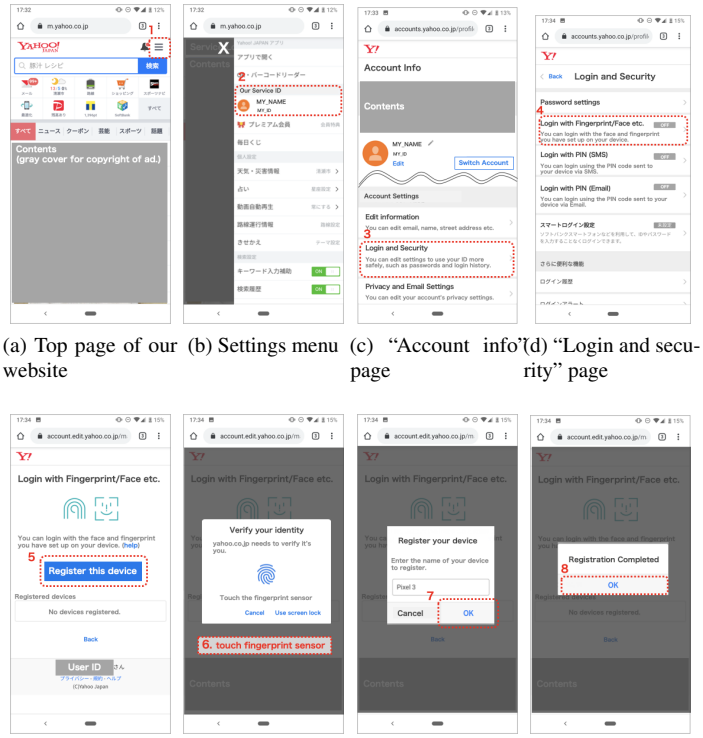
	Category	Participants
Gender	Male	P2, P3, P5, P6, P8
	Female	P1, P4, P7, P9, P10
Age	20–29	P3, P4, P6
	30–39	P1, P8, P10
	40–49	P5, P7
	50–59	P2, P9
Occupation	Employed	P1-P10
Profession	IT-related	P7
	Non-IT-related	P1–P6, P8–P10

The far right row lists which participants correspond to which item. All ten participants are represented as participant n (Pn, $1 \leq n \leq 10$).

Study Design and Process. Our study consisted of an interview and a test for each participant. A moderator asked each participant to set up the WebAuthn registration from his/her own Android smartphone by using his/her account for our service. During this time, the moderator observed the participant to ascertain whether he/she faced any barriers during the WebAuthn registration process. Figure 1 shows a series of screenshots[2] that appeared to the users during the registration process on our WebAuthn-enabled service, which has been commercially deployed. Tap the red frame in the figure to move to the next screen.

Limitations. The study population was collected by the research firm and limited to a small number of participants who did not represent all possible age ranges. Also, the participants were limited to users who had failed or never attempted the setup process for WebAuthn-based biometric authentication. Thus, the study results that we obtained are not generalizable from the above perspectives.

[2]To avoid any misunderstanding due to language differences, we've added English explanations to the screenshots on our site. Gray areas indicate parts that are hidden in consideration of advertisement copyright, as this is a commercial service.



(a) Top page of our website (b) Settings menu (c) "Account info" page (d) "Login and security" page

(e) "Login with fingerprint/face" page (f) "Verify your identity" dialog (g) "Register your device" dialog (h) "Registration completed" dialog

Figure 1: WebAuthn registration process

3 Results

We analyzed the results obtained through the study following the process described in Section 2.

Objective Analysis. We set three goals (**G1**–**G3**) to evaluate the user experience of participants during this study.

G1: Unlocking smartphone. The participant can unlock the screen of his/her smartphone by using his/her fingerprint without failure and without using other methods. The participant can discover and access the webpage that starts registering the authenticator, as shown in Fig. 1(e). **G2: Completing authenticator registration.** The participant can successfully register the authenticator by him/herself without the moderator's help. To achieve this goal, the participant needs to achieve user verification (see Fig. 1(f)).

G3: Completing login using registered authenticator. The participant can log in using the registered authenticator after logout. To achieve this goal, **G2**, that is, authenticator registration, needs to be completed first. Thus, the moderator helped

participants complete the authenticator setup if they could not do so by themselves and explained how to log out of our service. The number of participants who achieved **G1–G3** was **ten, three, and nine**, respectively.

G1 Analysis. All participants were familiar with the screen lock using fingerprints before they performed the task in this study and could unlock their phones without failure. Several participants had previously been taught by other people how to unlock with fingerprints.

G2 Analysis. Regarding **G2**, we had a noteworthy result that attracted our attention: namely, only three participants successfully completed the WebAuthn registration process by themselves. This was mostly as we had expected because we had solicited participants who had no experience with successful WebAuthn setup, as described in Section 2.

Seven participants could not hold their fingers over the sensor, despite being required to perform the same operations as needed to use the screen lock. **They all tapped the fingerprint-like icon on the dialog box (see Fig. 1(f)) displayed by the WebAuthn function of their Android smartphones** even though they were all accustomed to unlocking their screen by using their fingerprint, as confirmed by the result of **G1**. Their behavior was classified into two types. In the first type, the participant noticed he/she had encountered an error immediately after tapping the icon on the screen and then properly touched the fingerprint sensor. This type of behavior is described in the following comment.

> **P6:** *"I was lost for a moment. Since the icon was displayed in front of it, I wondered if I should tap it. I saw that there was no fingerprint sensor on the screen, so I tapped this real fingerprint sensor."*

In the second type of behavior, they did not realize that tapping the icon would be inappropriate for user verification until the moderator gave them some help. For example, P1 not only tapped the fingerprint-like icon but also kept tapping it until the moderator helped her solve the problem. During this time, she made the following comment:

> **P1:** *"I'm tapping with my middle finger because I have registered this finger for screen unlock."*

P7 also tapped the icon and could not proceed to the next step. Thus, the moderator advised her to read the text shown in the dialog box. Although she already used the fingerprint sensor in her daily life (as revealed in the result for **G1**), she did not seem to understand what the word "sensor" indicated. Ultimately, she could not complete the authenticator registration without the help of the moderator.

> **P7:** *"I don't know about the sensor. I only know this (tapping the fingerprint icon)."*

G3 Analysis. According to the results of **G3**, nine participants (all except P9) could log in by using their authenticator without any problems once they finished registering the authenticator and learned how to use their fingerprints for WebAuthn-based passwordless authentication.

System Usability Scale Analysis. We used the SUS calculation method [3] to calculate the SUS scores for quantitative evaluation of the usability of WebAuthn-based fingerprint authentication. The SUS scores for P1–P10 were **15.0, 67.5, 70.0, 57.5, 67.5, 60.0, 47.5, 87.5, 72.5, and 90.0**, respectively. According to acceptability ranges [3] when using SUS [1], the average SUS score of **63.5** indicates "Marginal high." In this study, the score reveals that WebAuthn-based fingerprint authentication was generally well received by the participants.

Subjective Comment Analysis. Among the many questions asked by the moderator during the interviews with each participant, we analyzed the following five, as the answers provided us with insight on how to encourage users to change from password to passwordless authentication.

Q1: Do you reuse passwords at multiple sites? (Yes: 80% = 8/10)

Q2: Did you know that you can login through fingerprint authentication on our site? (Yes: 90% = 9/10)

Q3: Are you willing to use your fingerprint to login? (Yes: 60% = 6/10)

Q4: Did you read the text in the dialog box that appeared when you registered the authenticator? (Yes: 100% = 9/9)

Q5: Will you continue to use fingerprint-based authentication for login? (Yes: 88% = 8/9)

According to **Q2**, most of the participants knew that fingerprints could be used to log in to our site, but **Q3** indicated that recognizing this did not necessarily mean the users intended to do it. When a participant was confused about registration, the moderator's first form of help was to read them the dialog text. Participants who did not directly touch the fingerprint sensor complained about the text. When a participant was confused about registration, the moderator's first form of help was to read the dialog text. Participants who did not directly touch the fingerprint sensor complained about the text.

> **P3:** *"There is a fingerprint mark where 'Touch the fingerprint sensor' is written."*
>
> **P7:** *"At least it is easier to read 'Touch the fingerprint sensor' than 'Touch the fingerprint lock of your device'."*

4 Discussion

Our analysis of the results in Section 3 revealed that WebAuthn-based passwordless authentication has the potential to provide users with high usability.

According to the results of the subjective common analysis, many participants expressed their desire to use fingerprint

[3] SUS scores of 100–70, 70–61, 61–50, and 50–0 respectively indicate "Acceptable," "Marginal high," "Marginal low," and "Not acceptable" (Bangor et al.).

authentication (**Q3**) and their affirmative intention to continuously use it once they experienced its benefits (**Q5**). Service providers can offer users a convenient authentication method as an alternative to passwords in terms of security as well, as most participants reused their passwords (**Q1**).

However, our analysis also unveiled significant impediments that participants faced in the setup process for WebAuthn-based passwordless authentication, as opposed to in the login process itself, although this was not identified in the usability studies on 2FA with security keys [4,9,12,13].

Thus, in this section we discuss **Fingerprint Dialog**. The problem here is that Android provides users with a different authentication experience than the usual screen lock. The achievements of **G1** and **G2** show that the participants frequently tapped their fingerprints on the icon in a way that we did not expect, despite the fact that they routinely use their fingerprints to unlock the screen. This shows that the dialog prompted them to log in differently than their regular screen lock. We also found that differences in the environment of each participant, such as the device, Android OS version, and fingerprint sensor position, did not affect their registration operation.

All seven participants who tapped the icon instead of touching the sensor (**G2**) knew that fingerprint authentication was available on our site (**Q2**), and about half (57% = 4/7) were willing to use that feature. In other words, their expectation toward fingerprint passwordless authentication was high.

However, most of them tried to register their phones by tapping the icons, even though they were reading the text displayed in the box (**Q4**). In addition, when logging in again after the registration using WebAuthn, all of the participants who tried logging in by using the fingerprint authentication function of Android were successful, and most of them expressed their desire to continue using this feature (**Q5**).

Also, looking at the SUS statement items, many of the participants gave a low score to the SUS question "I found the various functions for fingerprint authentication were well integrated." This score indicates that Android's fingerprint authentication feature was well integrated and that the dialog box was not appropriate for users.

For these reasons, having the characters, the icons, or both displayed in the dialog box was misleading to the participants. In other words, the things displayed in the box did not remind them of the fingerprint authentication function.

5 Design Implications

The dialog box that WebAuthn-enabled Android smartphones display during fingerprint authentication should be changed to one that is acceptable to most users. In this study we learned that 1) participants intuitively tapped the fingerprint-like icon and 2) even if a participant read the text, he/she accidentally tapped the icon. We therefore came up with the following suggestions for the design of the dialog box display.

First, when we look at the implementation of the other major OS, iOS, approval is required when installing a new application. At this time, it is sometimes necessary to press the power button twice consecutively, but depending on the model, the button may be located at the front, side, or top of the screen. This is similar to the various positions of the Android fingerprint sensor, as mentioned. In iOS, the position of these buttons is taken into account at the time of approval. Our suggestion is that, when performing authentication with Android WebAuthn, we can help users by pointing to the fingerprint sensor for each device.

Another suggestion comes from the feedback of the participants. A user who had never touched the fingerprint sensor before made the following comment.

> **Moderator:** *"Did you not touch the fingerprint sensor because there was a mark like a fingerprint?"*
> **P3:** *"There is a fingerprint mark where 'Touch the fingerprint sensor' is written."*

Participants could think of this as recognizing the "sensor" as pointing to a fingerprint icon. In that case, could this icon be made more abstract, or have its display removed, to help them succeed at fingerprint authentication more smoothly? We imagine that different actions are required for the participant's usual screen lock and WebAuthn authentication, so we feel it would be appropriate to display an icon other than the fingerprint icon to remind users of the screen lock. For example, replacing the icon with the person who has unlocked the screen may be sufficient.

6 Conclusion

To explore the usability of passwordless authentication for consumer users, we conducted an observation study on WebAuthn registration and authentication for our WebAuthn-based server using WebAuthn-enabled Android smartphones equipped with fingerprint sensors. Our study revealed significant impediments to properly setting up fingerprint authenticators in the WebAuthn registration process. The dialog box displayed by Android smartphones misled many participants in our study to tap the fingerprint-like icon on the screen instead of touching the fingerprint sensor on their phones, even though screen unlock was a routine task for them. There is a possibility that the dialog box will affect the usability of user authentication because it is displayed for users who access any sites that deploy WebAuthn, not just our site, with WebAuthn-enabled Android smartphones.

References

[1] James Miller Aaron Bangor, Philip Kortum. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Usability Studies*, 4(3):114–123, 2009.

[2] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proc. of S&P '12*, pages 553–567, 2012.

[3] J. Brooke. SUS: A Quick and Dirty Usability Scale, 1996.

[4] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Proc. of SOUPS'19*, 2019.

[5] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proc. of CHI '18*, pages 1–12, 2018.

[6] Android Developers. What's New in Android security (M and N Version) - Google I/O 2016. https://youtu.be/XZzLjllizYs, 2016.

[7] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. "Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication. In *Proc. of Euro S&PW '19*, pages 119–128. IEEE, 2019.

[8] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpeth. Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication. In *Proc. of MobiCom '18*, pages 401–415, 2018.

[9] 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 *Proc. of S&P '20*, pages 842–859, 2020.

[10] Sarah Pearman, Jeremy Thomas, Pardis Emani Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelmany, and Alain Forgetz. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proc. of CCS '17*, pages 295–310, 2017.

[11] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In *Proc. of SOUPS '17*, pages 1–7, 2017.

[12] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A Usability Study of Five Two-Factor Authentication Methods. In *Proc. of SOUPS '19*, pages 357–370, 2019.

[13] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *Proc. of S&P '18*, pages 872–888, 2018.

[14] W3C. Web Authentication: An API for Accessing Public Key Credentials – Level 1. https://www.w3.org/TR/webauthn/, 2019.

[15] Ding Wang, Qianchen Gu, Haibo Cheng, and Ping Wang. The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. In *Proc. of ASIA CCS '16*, pages 475–486, 2016.

[16] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. Password Memorability and Security: Empirical Results. *IEEE Security & Privacy*, 2(5):25–31, 2004.