Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication

Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, Sven Bugiel
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
{sanam.lyastani, michael.schilling, neumayr, backes, bugiel}@cispa.saarland

***Abstract*—The newest contender for succeeding passwords as the incumbent web authentication scheme is the FIDO2 standard. Jointly developed and backed by the FIDO Alliance and the W3C, FIDO2 has found support in virtually every browser, finds increasing support by service providers, and has adoptions beyond browser-software on its way. While it supports MFA and 2FA, its single-factor, *passwordless* authentication with security tokens has received the bulk of attention and was hailed by its supporters and the media as the solution that will replace text-passwords on the web. Despite its obvious security and deployability benefits—a setting that no prior solution had in this strong combination—the paradigm shift from a familiar knowledge factor to purely a possession factor raises questions about the *acceptance* of passwordless authentication by end-users.**

This paper presents the first large-scale lab study of FIDO2 *single-factor* authentication to collect insights about end-users' perception, acceptance, and concerns about *passwordless* authentication. Through hands-on tasks our participants gather first-hand experience with passwordless authentication using a security key, which they afterwards reflect on in a survey. Our results show that users are willing to accept a direct replacement of text-based passwords with a security key for single-factor authentication. That is an encouraging result in the quest to replace passwords. But, our results also identify new concerns that can potentially hinder the widespread adoption of FIDO2 passwordless authentication. In order to mitigate these factors, we derive concrete recommendations to try to help in the ongoing proliferation of passwordless authentication on the web.

I. Introduction

For decades we have tried to replace text-based passwords with more secure alternatives for end-user authentication on the web. But none of the alternatives has achieved this goal until today [1], [2], since none of them could improve security while at the same time offering the same level of deployability and usability as passwords. The newest contender for succeeding text-based passwords is the FIDO2 standard that was jointly developed by the FIDO Alliance—an organization with more than 250 member companies worldwide [3], including Google, Facebook, Microsoft, Amazon, or VISA—and the World Wide Web Consortium (W3C), the main international standards organization for the web. FIDO2 continues the development of the Universal 2nd Factor (U2F) authentication standard and offers websites a standardized way to make use of hardware authentication devices, such as security keys. Like U2F, it supports hardware authentication devices as a second-factor, however, most importantly, it also supports them as a *single-factor* for *passwordless* authentication. Considering the institutions backing FIDO2, this new standard has been presented in the media as a "password-killer" [4], [5], [6], [7]. Also from an academic point of view, using the framework by Bonneau et al. [1] (as we explain in Section II), FIDO2 seems like a promising candidate for succeeding text-based passwords as the incumbent end-user authentication scheme: it provides credentials that cannot be phished, replayed, nor are they subject to server breaches; being an open web authentication standard (WebAuthn), it is supported by virtually all browsers, and native implementations, like on Android and Windows, exist and more are forthcoming; it can provide a consistent user experience; and it supports various authenticator devices, including security keys, like the ones from Yubico or Feitian, but also integrated authenticators commonly available on end-user devices, like Trusted Platform Modules, Android keystore, or Apple TouchID. In fact, in our expert assessment, *none of the existing alternatives to text-based passwords offers as many benefits in Bonneau's et al. framework as FIDO2 with single-factor authentication.*

Thus, while FIDO2 offers strong end-user authentication, high convenience, and has great potential for widespread availability, it is an open question whether end-users accept this paradigm shift from "something they know" to "something they have" (i.e., passwordless authentication). More concretely, we want to find an answer to *"whether end-users accept FIDO2-based authentication as a single factor"* and if not, *"which factors could inhibit an adoption by end-users and which potential paths exist to address the end-user concerns?"*

To answer these questions, we conducted the first large-scale comparative user study of FIDO2 passwordless authentication. We recruited 94 participants and randomly distributed them among two groups. In the course of hands-on tasks, one group used a Yubico Security Key as 1FA (passwordless) and the other group, here acting as a control group, used regular text-based passwords for web authentication. Afterwards, we asked participants to reflect on this experience in a survey. The usability and the acceptance of the authentication mechanisms as well as user-specific factors that may effect these variables were measured using standardized methods. In order to get a more complete picture of user perception, we then used free

DOI 10.1109/SP40000.2020.00047

text questions to capture the ideas/benefits/drawbacks/concerns regarding the two authentication methods. As a result, our collected data allowed us to evaluate the usability and acceptance of FIDO2 passwordless authentication and to gather user concerns and feedback about the paradigm shift to FIDO2 passwordless authentication.

Our results show that lay users are very satisfied when directly *replacing* text-based passwords with a security key and are *willing to accept such passwordless authentication over regular text-based passwords*. This is an encouraging result on the road to replace passwords and indicates that FIDO2 has the potential to be the kingslayer of text-based passwords. However, we also identified several potential obstacles that could stop FIDO2 from reaching its goal. Besides known problems of token-based authentication, we identify new issues: First, we find that in case of 1FA, users associate possession of the authenticator with the implicit guarantee that no one else can access the account and, vice versa, the loss of the device with an (impending) illegal account access. This raises the question for a secure and efficient *authenticator revocation* in addition to account recovery—none of which exists as of today. Second, our study identifies new *problems with the physical form factor and features of authenticators*. Our participants questioned the suitability for everyday use and mentioned authentication scenarios for which, in contrast to passwords, they do not see the possibility to use a security key (e.g., public computers without connectivity or delegation of account access to trusted persons). Last but not least, we find that it is often very difficult for users to trust this new technology, mainly because it is such a strong break to previous authentication methods. Our participants had *no mental models* to understand and evaluate the functionality and security of such security keys.

In this light, we find it astonishing that users accept 1FA authentication with security keys so strongly despite these shortcomings. The main reason could be that the disadvantages and weaknesses of text-based passwords have become so obvious and overwhelming for users that they are looking for a technology that can free them from this burden. In summary, we find that there is still a gap between the users' concerns and what the current status-quo of FIDO2 1FA provides. While FIDO2 has the potential to be the kingslayer of passwords, the further development of the standard and of authenticator devices has to more strongly include the perspective of the users and their needs to gain the support of lay end-users. Building upon our results, we try to give concrete recommendations for the supporters of FIDO2, web developers, and further research that hopefully help to foster the proliferation of passwordless authentication on the web.

II. Background on FIDO2

FIDO2 is an open authentication standard developed jointly by the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C), extending prior work by the FIDO Alliance on the Universal 2nd Factor (U2F) standard, which has also been subject of the academic studies (see Section III). The standard consists of two specifications that

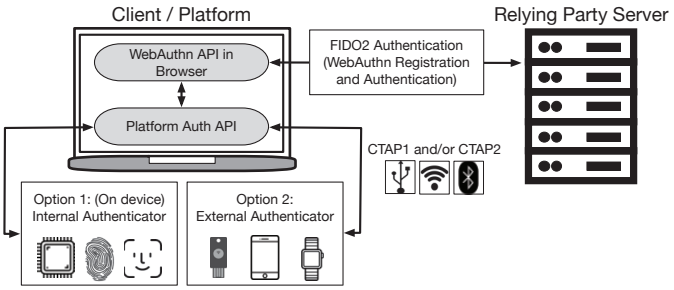


Fig. 1: FIDO2 authentication with WebAuthn and CTAP2

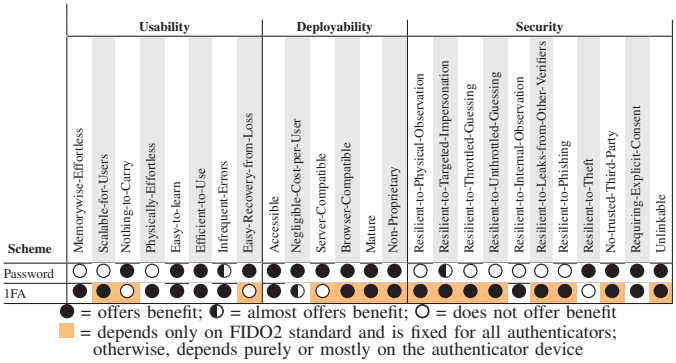
reflect the two authoring organizations (see Figure 1): (1) the WebAuthn protocol [8] for a standardized access by WebAuthn relying parties (e.g., website) to authenticate users via CTAP2 or backwards-compatible via U2F (now considered CTAP1) through a WebAuthn conforming client like the browser; (2) the Client-to-Authenticator-Protocol (CTAP2) [9], an application layer protocol used for communication between a WebAuthn client (like browser) and a conforming cryptographic authenticator device that can either be external and roaming via USB, Bluetooth, or NFC communication (e.g., security key or Android smartphone [10]), or internal (e.g., TPM, Trusted Execution Environment, or TouchID [11]). In contrast to its predecessor U2F, FIDO2 supports two-factor as well as multi-factor and even single-factor (i.e., *passwordless*) user authentication [12]. As a result, FIDO2 supports different levels of user verification, such as a simple test-of-user-presence (e.g., pressing the button on the authenticator) or user authentication to the authenticator via PIN or biometrics. Particularly in single-factor mode, this should ensure user consent to the authentication process.

At the time of writing, various browsers have already integrated stable support for WebAuthn [13], including Chrome, Firefox, Safari, and Edge, and also the number of websites that support WebAuthn is steadily increasing, for instance, Dropbox [14], Microsoft accounts [15], [16], Google accounts, Twitter [17], and others [18] offer FIDO2-based second factors. Also native platform support for FIDO2 is forthcoming, for instance, Microsoft supports it as part of their Windows Hello authentication [19]. Adopters of FIDO2 for non-browser clients or for websites (relying parties) are also supported in their task through an increasing number of FIDO2 libraries and tutorials [20], [16], [21], [22], [23], [24].

In terms of security, FIDO2 is an extension of FIDO U2F and offers the same high security-level based on public key cryptography (see [25] for an overview). At its core, FIDO2 is a challenge-response protocol with mutual authentication using hardware-based authenticators, which offers various advantages over text-based passwords: no shared secrets between user and websites that can be leaked through server breaches, phishing, or key-loggers; unlinkable reuse of the same authenticator for different accounts; or resilience to replay attacks.

Yubico Security Key: The Yubico Security Key is an implementation of a FIDO2 roaming authenticator that of-

TABLE I: Comparison between FIDO2 single-factor authentication using Yubico Security Key and text-based passwords based on the framework by Bonneau et al. [1]



fers two-factor, multi-factor, and single-factor (passwordless) authentication. It ships either as a pure USB token or with additional NFC support. It requires neither dedicated hardware (e.g., a reader) nor software, but works with preinstalled drivers on commonly available media (i.e., USB, NFC). To authenticate, users are required to show physical presence during command execution by pressing a capacitive button on the key (i.e., support for test-of-user-presence), indicated by the button flashing. There is no need for any further user input. In our study, we use the USB-only version of the Yubico Security Key as an authenticator in passwordless authentication (see Section V).

Comparison of passwords and FIDO2 1FA with Security Key

We provide context for FIDO2 by applying the framework of Bonneau et al. [1] in an expert assessment to compare the FIDO2 standard to text-based password authentication. Lang et al. [25] also provide a comparison of U2F Security Keys with text-based passwords using this framework and Das et al. [26] concurred with their assessment; however, as we explain in the following, we extend this comparison to FIDO2 and also consider the type of authenticator device as an additional dimension in our assessment.

Bonneau's et al. framework contains 25 subjective factors ("benefits") for measuring the security (11 benefits), deployability (6), and usability (8) of authentication schemes, which also pick up prior recommendations by Stajano [27] for token-based authentication. Table I summarizes the comparison of benefits that each scheme provides in those categories. As mentioned before, a user could use various types of authenticators, such as USB token, TPM, smartphone, etc. Thus, to apply the framework by Bonneau et al. [1], we had to consider that there are some benefits that only depend on the FIDO2 standard and benefits that are only dependent on the specific design of the authenticator device. This is motivated by the fact that the user primarily has to handle the authenticator, while not being directly concerned with the underlying protocols.

Hence, when we apply the framework by Bonneau et al. [1], we make this explicit distinction between benefits that are derived directly from the FIDO2 protocols and are fixed for all types of authenticators (marked with ■ background in Table I), and benefits that are mostly or purely dependent on the authenticator, here, the Yubico Security Key that we used in our study (no background color in Table I). Thus, those benefits might look different if we would use another authenticator, like a smartphone or Apple's TouchID. Here, we only give a summary of our evaluation of FIDO2, a more detailed explanation can be found in Appendix A.

Summary: FIDO2 with a Yubico Security Key as an authenticator scores almost perfectly in the framework by Bonneau et al. [1], missing *Nothing-to-Carry*, *Easy-Recovery-from-Loss*, *Server-Compatible*, and *Resilience-to-Theft*. In fact, none of the existing alternatives to text-based passwords offers as many benefits in Bonneau's et al. framework as FIDO2 with single factor authentication. While this seemingly makes FIDO2 a very strong candidate to replace text-based passwords, we are interested in our study in reasons beyond those 25 factors that might affect the acceptance of FIDO2 by users.

III. Related Work

We review prior works on the usability and acceptability of single-factor and two-factor authentication schemes.

A. Related studies of single-factor authentication

Replacing text-based passwords with alternatives is a very active research area and because of space constraints we refer to the excellent related work sections by Bonneau et al. [1] and Stajano [27] for a more comprehensive overview. We focus in the following on selected works that are either conceptually closer to FIDO2 or found widespread deployment.

Stajano [27] proposed Pico for replacing passwords with a hardware token, which shares many design aspects with U2F and FIDO2. For instance, it is based on a challenge-response protocol based on public key cryptography, offers mutual authentication between Pico and the verifier, and considers the user's privacy (e.g., no tracking). In an evaluation of Pico's usability in the wild [28], users appreciated avoiding passwords. Although this field study only had 11 users, this can be seen as encouraging for the acceptance of FIDO2. Additional user concerns were recovery in case of device loss and blocking Pico remotely.

TLS *client* certificates [29] can be used for online authentication. However, Parsovs [30] pointed out that current implementations have a poor user experience and that client certificates allow services to track users. The implementation of FIDO2 avoids those privacy risks and its implementation in browsers is tailored to providing a simpler, less error-prone, and more consistent user experience.

Very recently, Conners and Zappala [31] proposed a certificate-based authentication where client certificates are managed with an authenticator. Their *Let's Authenticate* solution provides appealing features, such as automatic account registration/login, easier account recovery, and privacy protection, but builds on top of a CA that issues client credentials to users in contrast to the decentralized nature of FIDO2.

B. Related studies of two-factor authentication

The usability and acceptability of two-factor authentication with different forms of second factors, such as OTP tokens, SMS, push messages, or most recently U2F Security Keys, has been studied in different works. Here, we focus on the most relevant works to our study of FIDO2 authentication with security keys for *passwordless* authentication.

1) General two-factor authentication: Two-factor authentication solutions for web services have been studied, for instance, by Strouble et al. [32], Weir et al. [33], [34], Gunson et al. [35], Krol et al. [36], or De Christofaro et al. [37]. Generally, their results showed that users found specialized hardware for authentication burdensome, that users lose said hardware, and that convenience is more important than perceived usability and security for users' willingness to adopt a new authentication technology. Fagan and Khan [38] studied the general motivation of users to (not) follow common computer security advice, including the advice to use two-factor authentication. They also conclude that users abstain from two-factor authentication to avoid inconvenience and cost. In our study, we are interested in concerns that would impede adoption of FIDO2 *single*-factor authentication.

2) Acceptability and usability of 2FA with Security Keys: Usability and convenience have been key design factors for U2F security keys, such as the Yubico Security Key. Recent studies [25], [26], [39], [40], [41] have focused on the acceptability and usability of U2F security keys and are closest and most informative to our study.

Lang et al. [25] report about the two year experience by Google for deploying U2F security keys to more than 50,000 of their employees. Their results showed that security keys are easy to deploy and refer to their use as "brainless" in comparison to OTP-based two-factor authentication. However, they did not conduct any user study but rely on user feedback and logs (e.g., authentication attempts or time spent authenticating).

Das et al. [26], [39] conducted a two-phase study and asked their participants to setup a U2F Yubico Security Key as second factor for their GMail accounts. Their results showed that clearer setup instructions led to significant improvements in usability, but did not change the overall acceptability of the solution. A major constraint on the acceptability was the concern about loss of the key, where concern about being locked out of the account was more salient than losing access to an attacker. Many of the participants were also confused about how to recover their account in case their key is lost. Their results highlight that the acceptance of the solution does not depend solely on convenience and usability.

Reynolds et al. [40] describe two usability studies of Yubico YubiKey as second factor: setup and day-to-day usage. In the first study, 31 participants were asked to setup and configure the YubiKey for a Windows 10, Google, and Facebook account. The result of the first study revealed that most participants struggled to setup their accounts with 2FA in general and Yubikey in particular. In a follow-up study, 25 participants were asked to use a Yubikey in their daily lives for a four-week period. In contrast to the first study, participants in the second study reported that the Yubikey is usable in day-to-day usage and gave a high SUS [42] score. However, in both studies, participants had consistent problems with using the YubiKey on Windows 10, which also affected our decision to focus on web authentication with two mockup websites instead of using Windows 10, currently being the only platform supporting FIDO2 *single-factor* authentication. Moreover, FIDO2 has been integrated into browser software and platform support exists, which removes many of the problems the participants in Reynolds' et al. study encountered. Reynolds et al. further recommend to standardize the setup process to improve usability of this crucial step. In our study, we improved the setup part by showing a short video to our participants and explaining step by step how to log into accounts using a Yubico Security Key.

Reese et al. [43] conducted comparative usability studies of the usage and setup of five two-factor authentication methods: SMS, push notifications, TOTP, U2F with Security Key, and printed out codes. The goal was to eliminate confounding factors and provide better comparison of these methods. Their results show that users generally find all five different methods usable and the majority of participants considers the extra effort worth the gain in security. A third of their participants, however, noted that they do not always have their second factor available, causing inconveniences.

Ciolino et al. [44] conducted a comparative lab study of the setup process of three different U2F authenticator devices and SMS OTP as well as a diary study on the continued use of one such authenticator. Their results underline that the setup of security keys is a high inconvenience for users due to lacking instructions and guidance, and that particular user interface design choices of the web services or by the vendor of the authenticator contribute to this problem. Their participants also expressed concerns about the form factor of the authenticator, e.g., easier losing smaller devices, breaking larger devices, or recognizing buttons as such.

Das et al. [41] investigated the user experience of Security Keys with ten older adults (>60 years) and found that non-inclusive design and inadequate risk communication resulted in minimal adoption in their participant pool. In particular, the form factor of the authenticator device (e.g., too small to be handled easily in daily use) and device compatibility were found to be crucial. Our results indicate that the form factor of the authenticator and the applicability of FIDO2 authentication are of general concern.

IV. RESEARCH QUESTIONS

It was our goal to answer the following research questions:

1) *How do users perceive FIDO2 passwordless authentication in terms of usability?*
2) *Are users accepting FIDO2 passwordless authentication?*
3) *What thoughts and concerns arise in the users' minds when using FIDO2 passwordless authentication?*

To do so, our user study compared passwordless authentication against traditional password-based authentication. In the

following section, we develop concrete hypotheses based on prior research findings.

Usability is determined by the users' perception of how well a technology is suited to effectively, efficiently, and satisfactorily achieve their goals. Passwords as the default authentication method on the web can already cover many points concerning usability [1]. However, the two aspects of usability that text-based passwords cannot satisfy —*Memorywise-Effortless* and *Scalable-for-Users*—are particularly important, as average users nowadays have a large number of online accounts [45], [46]. FIDO2 passwordless authentication fulfills these two important requirements and also has the advantage that it is *Physically-Effortless*. Subsequently, we assume that:

H1: *FIDO2 passwordless authentication has a higher usability than traditional password-based authentication.*

The user acceptance for a (technological) system [47] describes factors that, according to the Technology Acceptance Model [48], are direct precursors of the actual usage of a technology in the future. This makes acceptance particularly important if passwordless authentication aims to replace passwords in the long run. The perceived convenience and usefulness of passwordless authentication could lead to a very high acceptance of this technology. On the other hand, users have been accustomed to using passwords for a long time and this extensive previous experience should also lead to a high acceptance of this technology [49]. Since it is not clear which of the two authentication methods should be accepted more, we assume that there are differences:

H2: *FIDO2 passwordless authentication and the traditional password-based method differ in their acceptance.*

Control variables: Prior research has identified several situational and user-specific variables that may also influence users' acceptance. Therefore, we include the following variables in our experimental design to control for their effects: (1) Usability, is one of the most important predictors of technology usage and acceptance [48] and depends heavily on users' preferences and prior experiences [49]. We therefore assume that usability may have an effect on acceptance regardless of the authentication method. (2) Affinity for technology interaction (ATI) describes a person's tendency to enjoy and proactively engage in technology interaction [50], [51]. People with a high ATI should have more fun using a new authentication method and therefore accept it more. (3) Privacy concerns describe users' concerns that can arise if it is not clear what will happen to one's own data [52]. As new authentication technologies, such as FIDO2, are by their very definition related to private information, we controlled for users' individual privacy concerns. (4) A Computer science background—for example, a corresponding degree or course of studies—imparts technical basics and weaknesses of established authentication methods. In order to exclude an effect of this prior education we controlled for such a background.

V. METHODOLOGY

The core idea of our study was to look at the perception, acceptance, and thoughts of users about FIDO2 passwordless authentication with a security key and compare these to traditional password-based authentication. Thereby, we used a combination of both quantitative and qualitative approaches that are described in more detail in this section.

A. Study design and procedure

In our user study we used a between-group research design and invited participants to interact with the registration and authentication process of web applications in a controlled (laboratory) environment to gain hands-on experience.

We explicitly decided to let each participant try only one of the two authentication methods in order to avoid that the participants focus mainly on the differences between both schemes. Corresponding contrast effects [53] that could occur in a within-person design might have introduced significant bias into the qualitative analysis of participants' thoughts and concerns. Therefore, we randomly assigned our participants to a study (referred to as Group_{1FA}) and a control group (Group_{Pass}), which differed only in the authentication method available to the participants during this hands-on experience.

Members of Group_{1FA} could log in with a self-generated user name and a security key. Thereby, we focused on the Yubico Security Key as the authentication device because it is the most popular end-user security key on the market and has already been the subject of studies in the past [40], [26], [25].

Members of Group_{Pass} had to create a password in addition to a user name during registration. Thereby, the only password policy in place was a restriction to a minimum length of 8 characters, which corresponds to the lowest possible hurdle according to the NIST password guidelines [54].

At the beginning of the study, participants read the privacy policies and gave their consent. Afterwards, the participants were led to a workplace with a laptop and (in Group_{1FA}) a Yubico Security Key. The study consisted of a survey with seven stages that guided participants through the entire process in a standardized form (see Figure 2):

Stage 1 (welcome message): the study began with a welcome message, including the study instructions.

Stage 2 (topic introduction): Participants watched a video (≈3 min) introducing the topic of the study—"authentication security." From the perspective of Alice (a fictitious character), common problems associated with the registration and use of online services were presented. Alice' story focused on the theft and abuse of account credentials and how to protect against those threats. This video was designed to balance different levels of prior knowledge between our participants.

The next three stages (stages 3, 4 and 5) were only completed by the Group_{1FA}, while the participants in Group_{Pass} were redirected straight to stage 6.

Stage 3 (FIDO2-specific information): Prior work has shown that lack of clarity about the functionality and security benefits of authentication methods leads to lower security ratings, lower acceptance, and reluctance to switch to a new authentication method [34], [33], [55], [26]. FIDO2 is very likely unknown to the users, so we decided to give our

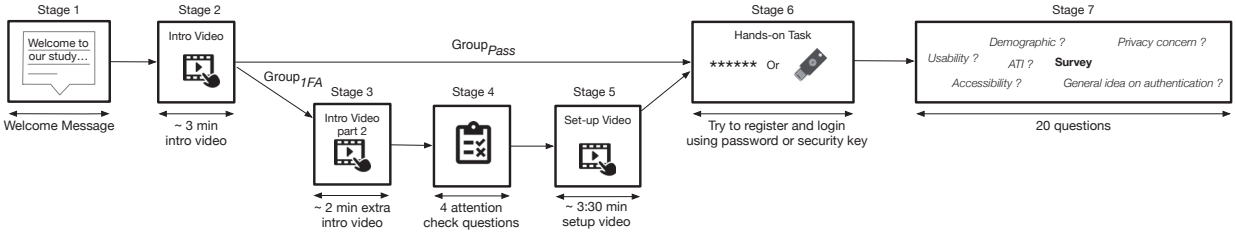


Fig. 2: Overview of our study procedure

participants an introduction to this new technology in order to examine the informed decisions and opinions of users without bias generated by a potential lack of knowledge. Corresponding information was provided to our participants as another video (≈2 min), as it was suggested from users' side in related work [40]. This video dealt with the practical use of a Yubico Security Key for single-factor authentication, its known benefits and drawbacks, and is seamlessly integrated into the introduction video and the story-line of Alice.[1]

Stage 4 (attention check question): Four attention test questions were used to determine if the participants understood the information from the previous stage correctly. None of our participants failed this check.

Stage 5 (setup video:) Afterwards, the participants in Group_{1FA} were provided with a setup video (≈3:30 minutes) that explained the setup process for FIDO2 with a Yubico Security Key. The content of the video was a step by step guide through the registration and authentication process using the Yubico Security Key on a demo site that supports FIDO2.

Stage 6 (hands-on task): The participants of both groups received a first-hand experience with their corresponding authentication method. The participants were asked to configure an account on two mockup websites, "Schmoogle" and "Fakebook," which were strongly inspired by the social media service Facebook and the email provider GMail to provide a realistic scenario. These two websites were chosen because we assumed that their structure, design, and the way of interaction with them is known to many users. This was especially important as we were not interested in the user interaction with the service as a whole, but especially in the perception of the registration and authentication process. Additionally, there were several reasons why we decided to use mockup websites and not real web services: 1) At the time we designed this study there was no web service that used FIDO2 in passwordless mode; 2) Even though Microsoft is promoting passwordless authentication with FIDO2 for its services [19], [5], a PIN or biometrics is still required to unlock the authenticator, which users may mistake as text-based password or device-local authentication. Moreover, prior works encountered poor user experiences of Windows' support for security keys [40], which we wanted to avoid in our study; 3) We aimed for a controllable and standardized environment, with no risk that our results might be affected by changes in the login process or the user interface of the web service. As a task in Group_{Pass} the participants had to register and log-in to the websites using text-based passwords. Group_{1FA} had to use the Yubico Security Key to register and authenticate. There was no time limit and participants could try and explore the methods as long as they wanted. For the implementation of our mockup websites for Group_{1FA}, we used the FIDO2 example projects [23], [24] by Adam Powers. We removed the password fields from registration/login forms. Instead, the registration/login button triggers the WebAuthn API. The introduction and setup videos as well as videos of the workflows for our websites can be found at [56]. Our participants used the Chrome browser for this task.

Stage 7 (survey): After completing the practical task, participants completed the questionnaire with our study variables, which will be described in the next two sections.

B. Quantitative data collection and analysis

To answer our first two research questions and to test the corresponding hypotheses, we used the following measures. A full overview of all used scales can be found in Appendix B.

Usability (SUS). We measured usability (α = .80) with the 10-item System Usability Scale (short SUS) from Brooke [42]. Participants stated their level of agreement or disagreement for the 10 items based on their experience with the authentication method. The resulting scores are between 0 and 100 whereby higher scores indicate a higher/better usability.

Acceptance. Acceptance (α = .90) was measured with the scale from van der Laan et al. [47]. This scale measures acceptance with 9 semantic differentials. The resulting scores are between 1 and 5 whereby higher scores indicate a higher/greater acceptance.

Affinity for Technology Interaction (ATI). We measured Affinity for Technology Interaction (α = .92) using the scale from Franke et al. [50], which measures the construct on a 9-item scale. The resulting scores are between 1 and 6 where higher scores indicate a higher/greater affinity.

Privacy Concern (PC). The participants' privacy concern (α = .82) was measured by a 4-item scale taken from Langer et al. [57]. The resulting scores are between 1 and 7 whereby higher scores indicate higher/more privacy concerns.

Demographic Questions. To gain further insight into our study sample, participants answered questions regarding their

[1]In practice, most websites do not offer such detailed user guidance for new authentication technologies. In Section VI-E, we therefore conduct a "reality check" of our introduction approach to ensure the stability of our results.

age, gender, highest educational degree, computer science background, and field of study/work.

C. Qualitative data collection and analysis

While standardized measuring instruments allow a comparison between our two authentication methods, they are limited in their ability to fully capture individual perception, thoughts, and concerns of users. Therefore, we collected additional qualitative data to answer our third research question.

Our participants answered open-ended text questions about their general impression of the authentication methods, the advantages and disadvantages they see, as well as their willingness to use the method in their personal lives. Our open-ended questions about general impressions were inspired by closest related work [40] and adapted to our specific study setting using best-practices from commercial user experience testing [58] and literature [59] (e.g., recommendations for question form and wording). The open-ended questions about the advantages and disadvantages were added to gain further insights into encouraging and hindering factors in the adaptation of the authentication methods. Additionally, it was of interest to us to find out more about reasons for (un-)willingness to use the authentication methods. The questions were successfully evaluated in a pilot study with five participants, which did not mention any issues. The corresponding questions can be found in Appendix B. Subsequently, we used inductive coding (see [59], [60], [61], [62]) to analyze their answers.

In a first step, three researchers independently read all open-ended text answers of our participants and marked all statements that might contain information related to our general research questions. The results were discussed and an initial coding scheme was developed. In the next step, the initial categories were merged by axial coding to category clusters and topics. After this step had been carried out independently by three researchers, they merged their category systems, discussed inconsistencies and created the final code book. Based on this code book, all answers were coded again by two independent researchers. The coders achieved a good mean inter-rater reliability (correspondence between the coders) of Krippendorff's Alpha = .817 [63]. A complete overview of the coding system can be found in Table VI in Appendix C.

D. Ethical concerns

The study design and protocol were reviewed and approved by the ethical review board of our university. We did not collect any personal information, such as username and password. We temporarily stored participants' email address to reimburse them with an Amazon voucher ($12 for ≈45 minutes of participation) and deleted the email addresses after that. All server-side software (i.e., a Limesurvey Community Edition software) was self-hosted on a maintained and hardened university server to which only researchers involved in this study have access.

VI. Results

Our data were collected from mid-December 2018 to end-February 2019 in a laboratory on the campus of our university. Participant recruiting took place via social media groups as well as in lectures and with flyers on our campus.

TABLE II: Overview descriptive data

Variable	$Group_{Pass}$	$Group_{1FA}$	Statistics	ES
N	48	46		
Gender			$\chi^2(1) = 0.000$	.01
Female	27	26	$p = 1.000$	
Male	20	20		
No answer	1	0		
Age	24.08 (3.63)	25.78 (6.44)	$t(92) = 1.585$ $p = .117$	.33
Education			$\chi^2(5) = 9.462$	.32
< High school	0	2	$p = .052$	
High school	23	12		
Bachelor	12	20		
Master	12	11		
Diploma	0	1		
Ph.D	1	0		
ATI	3.84 (1.12)	4.01 (0.95)	$t(92) = 0.798$ $p = .427$	.16
PC	5.43 (1.31)	5.36 (1.13)	$t(92) = -0.249$ $p = .804$	.05
CS background			$\chi^2(1) = 4.241$	.23
Yes	18	28	$\mathbf{p = .038}$	
No	30	18		
SUS	71.92 (11.09)	81.79 (12.15)	$t(92) = 4.116$ $\mathbf{p < .001}$	.85
Acceptance	3.41 (0.70)	4.29 (0.60)	$t(92) = 6.522$ $\mathbf{p < .001}$	1.35

Note: ES = Effect Size; *N* = Number of participants; ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS background = Computer science background; SUS = System Usability Scale. Depending on the variable, the frequencies or the scale mean values including standard deviation are presented in the cells. The statistics column shows the statistical data parameters for a group comparison with two sample t-test respectively with Fisher's exact test for the corresponding variable. p values below the 5% criterion are printed in bold. Effect Sizes are specified in Cohen's *d* for t-tests and in Cramer's V for Fisher's exact test. N(total) = 94.

A. Sample and participant demographics

Our final sample included N = 94 participants, 56.4% (n = 53) of whom identified themselves as female and the mean age was 24.91. The participants' educational background met the expectations of a university sample. Table II presents descriptive data for both groups. The second to last column indicates whether there were significant differences between the groups. We found differences for our dependent variables as well as for some control variables which we will discuss in more detail in our statistical analysis. In general, there were no differences in the demographic composition of the groups.

B. Quantitative results

Usability: Regarding **H1**, an unpaired two-sample *t*-tests showed significant higher SUS scores in $Group_{1FA}$ ($M = 81.74$) than in $Group_{Pass}$ ($M = 71.77$); $t(92) = 4.116$, $p < .001$, Cohen's $d = .85$ These results provide support for our hypothesis: **FIDO2 passwordless authentication is perceived as more usable than traditional password-based authentication.** However, when comparing the SUS scores in our study with other systems and the descriptions provided by Bangor et al. [64] and Sauro et al. [65], both authentication methods are evaluated positively (as "Good", receiving a B grade).

Acceptance: With respect to **H2** an unpaired two-sample *t*-tests showed significant higher acceptance scores in $Group_{1FA}$ ($M = 4.29$) than in $Group_{Pass}$ ($M = 3.41$); $t(92) = 6.522$,

p < .001, Cohen's d = 1.35. In other words: **Passwordless authentication with the Yubico Security Key was more accepted by our participants than traditional password-based authentication.**

In a next step we assessed the acceptance of the authentication methods with a regression analysis to include the potential effects of the control variables. Stepwise we built regression models including: 1) the control variables, 2) SUS, 3) authentication type ($\text{Group}_{\text{Pass}}$ is the base line against which $\text{Group}_{\text{1FA}}$ is compared) and 4) all possible interactions between all those variables. We used robust regression techniques [66] to calculate the standard error for all estimates in our models, as the Breusch-Pagan test [67] indicated a violation of homoscedasticity (χ^2 = 11.949, df = 5, p-value < .05) for our models. Before the analysis, all metric predictor variables were grand-mean centered to facilitate the interpretation later on.

Considering the complexity of the models, Model 3 containing the first three types of predictor variables mentioned above could explain our empirical data best (see Appendix D for model comparison). This model explained 48.8% (R^2 = .488) of the total variance in users' acceptance scores. Table III gives an overview of the predictors in this model. Our results showed that the SUS score (b = .02, p < .001), an individual's computer science background (b = -.33, p = .025), and the predictor representing the difference between the two groups had a significant effect on the acceptance of the authentication methods by the users (b = .76, p < .001).

Neither ATI nor Privacy Concerns showed a significant effect on the acceptance of the authentication method. A post-hoc relative importance analysis showed that the predictor representing the group differences accounted for the majority (51.5%) of the explained variance while SUS accounted for another 42.8%. Although computer science background is a significant predictor of acceptance, its contribution to the explained variance is very limited (3.7%). The remaining 2.0% can be statistically attributed to the non-significant factors ATI and Privacy Concerns. Overall, these results suggest that: (a) The more usable users perceive an authentication method, the more they will accept that specific authentication method; (b) Even when the control variables are taken into account, the FIDO2 1FA authentication method is widely more accepted than the traditional password-based method; (c) Moreover, we found that people with a computer science background showed in general lower acceptance scores than people without such a background, independently of the authentication method. This is in contrast to recent results about usability of biometrics [68], where experts more readily adopted new technology than non-experts. However, our post-hoc relative weight analysis showed that this effect is minimal and negligible compared to other significant predictors.

TABLE III: Regression model predicting users acceptance

	Acceptance			
Predictors	b	CI	RI	p
(Intercept)	3.64	[3.43, 3.84]		**<0.001**
ATI	0.05	[−0.09, 0.19]	1.9%	0.486
PC	−0.01	[−0.10, 0.09]	< 0.1%	0.876
CS (yes)	−0.33	[−0.62, −0.04]	3.7%	**0.025**
SUS	0.02	[0.01, 0.03]	42.8%	**<0.001**
Group (1FA)	0.76	[0.50, 1.02]	51.5%	**<0.001**

Note: Robust regression based on MM estimator [69]. Model 3 can explain 48.8% (R^2adjusted = .488) of the empirical variance (adjusted for number of terms in model); ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS (yes) = Dummy variable that encodes the effect of a computer science background (No background is the default); SUS = System Usability Scale; Group (1FA) = Dummy variable that encodes the differences for the groups ($\text{Group}_{\text{Pass}}$ is the default). p-values below the 5% criterion are printed in bold. N(total) = 94.

C. Qualitative Results

Qualitative analysis of the free text responses revealed five major concepts for perception, acceptance, and possible use.

*a) **Shift from cognitive to physical effort**:* The vast majority (74; 79% both groups) of our study participants mentioned in one way or another the effort associated with the usage of the specific authentication methods, but in both groups different forms of effort were mentioned. For traditional passwords, primarily the cognitive efforts associated with the use were described. Participants found the creation of secure and unique passwords (5; 10% $\text{Group}_{\text{Pass}}$) but also their memorization (16; 33% $\text{Group}_{\text{Pass}}$) a difficult and demanding task. According to them, the ever-increasing number of accounts that users have to manage are a very burdening factor, as users frequently forget their passwords, resulting in losing access to their accounts. Regarding passwordless authentication, cognitive effort was not an issue for our participants. In fact, the reduction of cognitive effort compared to password-based authentication was seen as a great (if not the greatest) advantage of passwordless technology (44; 96% $\text{Group}_{\text{1FA}}$).

> *"No recalling of the password. For [a] new account, one need not [to] worry to come up with a password and remember it for later use."(P92, $\text{Group}_{\text{1FA}}$)*

In addition to mental efforts of an authentication method, our participants also described physical efforts associated with these methods. Corresponding topics were particularly evident for passwordless authentication. Eighteen (39%) of the participants in $\text{Group}_{\text{1FA}}$ criticized that this method requires carrying a device to be able to authenticate. It was seen as problematic and annoying that it is not possible to use web services if the security key is not present, which restricts spontaneous and ad hoc use.

> *"I think the only problem with this kind of authentication system is that the user[s] have to carry their Yubikey [Yubico Security Key] everywhere with them [...]"* (P62, $\text{Group}_{\text{1FA}}$)

This physical effort was perceived as one of the major disadvantages of passwordless authentication and led to further concerns which we will discuss later. In contrast to passwordless authentication, only a few of our participants saw a physical effort in classical password-based authentication. Solely the fact that typing passwords can be annoying was mentioned (5; 10% $\text{Group}_{\text{Pass}}$) as a disadvantage in this area.

Comparing both authentication methods, the switch from password-based to passwordless authentication was associated with a clear shift in the participants' perception from cognitive

to physical effort. This reflects the paradigm shift underlying the switch to FIDO2 1FA—away from 'something I know', over to 'something I have.'

b) ***Changes in threat model****:* Participants from both groups thought about factors and problems that could affect the security of their accounts (59; 63% both groups), although the prevailing threat models differed greatly. In $\text{Group}_{\text{Pass}}$ participants (25; 51%) were primarily worried that weak passwords, password reuse, or phishing attacks could lead to an attacker gaining access to their accounts and abusing them.

The participants of $\text{Group}_{\text{1FA}}$ (28; 61%) were mainly afraid that someone else could gain access to their accounts with a lost or stolen security key. They were particularly worried as they considered their accounts to be completely unprotected as soon as their key fell into the wrong hands (8; 17% $\text{Group}_{\text{1FA}}$).

> *"I just have one concern: What if someone steal[s] my Yubikey [Yubico Security Key]? Does that mean he can access all my accounts just inserting it [to] his computer?"* (P66, $\text{Group}_{\text{1FA}}$)

For this reason, some of our participants wanted an additional layer of protection, such as biometrics, to protect the security key against unauthorized use.

> *"[...] I would prefer a finger print verification rather than a push of a button because it is unique only for me."* (P91, $\text{Group}_{\text{1FA}}$)

Moreover, our participants (11; 24% $\text{Group}_{\text{1FA}}$) were worried about a point that was no issue in $\text{Group}_{\text{Pass}}$: The loss of control over one's own account and thus one's own data if the security key is lost, stolen, forgotten, or damaged.

> *"If I forget the YubiKey [Yubico Security Key], I can't get into my accounts."* (P63, $\text{Group}_{\text{1FA}}$)
>
> *"If my Yubikey [Yubico Security Key] gets broken (let's say my coffee spilled on it) I won't be able to login to my accounts."* (P54, $\text{Group}_{\text{1FA}}$)

Thereby, several participants raised the question how to "revoke" and "recover" account access in such a case. These concerns went so far that they expressed a desire for a backup authentication method.

> *"There should be a way to use your accounts without the yubikey [Yubico Security Key]. Otherwise you would be very dependent on it."* (P50, $\text{Group}_{\text{1FA}}$)

Interestingly, one of our participants, who claims to have *"already been on the receiving end of the password theft,"* points out that the biggest advantage of passwordless authentication is the implicit guarantee that no one else can access users' accounts as long as they are in possession of their own security key. In this way, the disappearance of the security key from one's own possession immediately warns the user of a potential (impending) unauthorized access to their account—something that passwords simply cannot offer.

If we compare the two types of authentication, we can see that the threat model for passwordless authentication is fundamentally different from the one for passwords. Because a physical object is required for authentication, the concerns of our participants about threats from the online world, such as phishing or password leaks, are radically reduced. On the other hand, such a dependency brought attention to the inherent natural weakness of such physical objects, their susceptibility to loss, theft, and destruction. Especially the fear of losing access to one's own accounts seems to be of great concern.

c) ***Restrictions in applicability****:* Another major problem that has arisen in relation to passwordless authentication are situational barriers associated with this type of authentication. Participants (14; 30% $\text{Group}_{\text{1FA}}$) complained about technical incompatibilities, which can be traced back to the specific implementation of the security key, especially the applicability for mobile devices, like smartphones or tablets. For our participants, an implementation using USB, as we studied it, seems problematic and perhaps even outdated.

> *"Nowadays an USB dongle seem to be a bit old, new computer doesn't have this port, also probably most of the authentication on these days are done in mobile devices..."* (P70, $\text{Group}_{\text{1FA}}$)

On the other hand, participants (7; 14%) from $\text{Group}_{\text{Pass}}$ came up with cases of authentication in which passwords seem to be superior to other technologies because of their flexibility. In this context, they mentioned the ability to spontaneously delegate accounts via telephone or the usage of specially protected computers (e.g., public computer in a library) that do not provide access to standard interfaces.

> *"...If necessary, you can also help relatives via telephone or Internet by changing something in their account or doing something for them if they are prevented from doing so."*(P9, $\text{Group}_{\text{Pass}}$)
>
> *"Public PCs may not provide an accessible USB interface."* (P84, $\text{Group}_{\text{1FA}}$)

In summary, these findings indicate that passwordless authentication cannot yet cover all user scenarios (at least with the tested USB implementation) and that neglecting specific corner-cases could be very problematic.

d) ***Breaking with traditions and habitual patterns****:* In contrast to the previous points, many statements of the participants also described aspects connected to the mental migration process from passwords to passwordless authentication. As such, this shift means a break with the well-established habits and traditions of users. Over the course of our study, it became very clear that our participants (40; 82% $\text{Group}_{\text{Pass}}$) have a clear mental model of password-based authentication. They know the pros and cons and have a certain understanding of the factors responsible for the security of a password (35; 71% $\text{Group}_{\text{Pass}}$). At least for our participants this positive mental model does not seem to have been challenged by prior negative experiences (e.g., by account theft) and therefore became the mental default for authentication.

> *"[I use passwords] for all accounts, because I have never had any problems with it, which means my accounts have never been hacked."* (P33, $\text{Group}_{\text{Pass}}$)

For passwordless authentication, on the other hand, such mental models must first be established in the users' minds.

Although the videos in our study already seem to be a helpful introduction to this new technology from the participants' point of view (5; 11% Group_{1FA}), obvious misconceptions in the free-text responses (27; 59% Group_{1FA}) show that their mental models are only rudimentary.

> *"Is it possible to track my exact location once I insert the Yubikey [Yubico Security Key]?"* (P52, Group_{1FA})

Such lack of technical background knowledge and the associated lack of trust can be one of the biggest obstacles to the adoption of any kind of new authentication method. One of our participants summarizes this quite clearly:

> *"Most people might rather use a password because they better understand and know how it works."* (P72, Group_{1FA})

However, these hindering factors for adoption were countered in our study by an affective reaction to passwordless authentication that was very positive. Thereby, the majority of participants (27; 59%) in Group_{1FA} described the authentication as a fun, pleasant, and exciting new user experience.

> *"It was overall very nice and pleasant. I found it very intuitive to use."* (P62, Group_{1FA})

This is countered by a rather negative affective reaction to password-based authentication (3; 6% Group_{Pass}), which is described as "monotonous," "boring," and in total "annoying."

In summary, it can be said that due to the lack of mental models and knowledge about the security of passwordless authentication, it might be still a bumpy road to embed this authentication method as a real alternative to passwords in users' minds. Nevertheless, the very positive affective reaction of our participants to passwordless authentication gives us hope that users are ready to replace passwords.

e) ***Security key characteristics****:* After all these mainly conceptual aspects of FIDO2 passwordless authentication, we would like to mention two further points regarding the specific authenticator we used. A few of the participants (7; 15% Group_{1FA}) mentioned experiences that may raise doubts about the robustness and maturity of the device. For instance, the form factor of the Yubico Security Key led to ambiguous and misleading situations for our participants.

> *"[I] inserted the Yubikey [Yubico Security Key] into the wrong slot, and later when the message still kept showing, realized that hadn't inserted into the correct slot "* (P92, Group_{1FA})

> *"Once the Yubikey [Yubico Security Key] didn't react and I didn't know if I had to press it or it's enough to just hold my finger on it."* (P60, Group_{1FA})

In addition, several participants (10; 22% Group_{1FA}) considered the price of the Yubico Security Key to be very expensive.

> *"... I don't want to spend money on the key [Yubico Security Key]..."* (P57, Group_{1FA})

While these findings apply in particular to the security key, we will further address implications and recommendations for the design of authenticator devices in the following discussion.

TABLE IV: Willingness to (not) use passwordless auth.

Category	N(Cat)	Arguments	N(Arg)
Yes	16	Easy/Secure/Memorywise-effortless	3
Yes, but	13	Fear of losing access to own account	5
		Fear of account access by others	4
		Mistrust	3
		Lack of universal access	3
		Costly	1
Rather not	11	Fear of losing access to own account	4
		Mistrust	4
		Costly	3
		Lack of universal access	3
		Annoying to carry extra device	1
No	6	Mistrust	3
		Annoying to carry extra device	3
		Fear of losing access to own account	2
		Lack of knowledge	1
		Fear of account access by others	1
		Costly	1
		Lack of universal access	1

Note: N(Cat) = No. of participants who fell into that category; N(Arg) = No. of participants naming that argument; Total No. of participants in Group_{1FA}: 46.

D. Willingness to (not) use passwordless authentication

In the end we asked our participants if they now would be willing to use passwordless authentication in their private lives. We identified four different categories in our participants' responses, which we coded as "Yes", "Yes, but", "Rather not" and "No." Table IV summarizes our participants' answers. We also coded their arguments about why they would (not) use it and we list the most mentioned arguments in the table.

Of all 46 participants in Group_{1FA}, 16 (35%) mentioned that they would be willing to use the scheme without any further conditions and explicitly highlighted the ease and convenience of the method over passwords. Most of them also mentioned they would use the method on almost all kinds of websites. This indicates that they found the scheme secure enough to apply even on their most important websites.

The remaining participants (30; 65% Group_{1FA}) had different kinds of concerns. Participants in the "Yes, but" subgroup gave concrete conditions that have to be met for them to be fully willing to use passwordless authentication, while participants in the "Rather not" and "No" subgroups gave explicit reasons why they are not willing to use passwordless authentication. All three concerned groups mentioned the almost exact same set of arguments, only with slightly different rankings. In general, the "Fear of losing access to the own account" or "Fear of access to their account by others" and "Mistrust" were mentioned most frequently (16; 53% and 10; 33% respectively), followed by "Lack of universal access" and "Costly." Only participants in the "No" subgroup argued more frequently with the "Annoyance to carry an extra device."

Overall, the results in Table IV suggest that there is a high potential willingness to use passwordless authentication over text-based passwords, if certain obstacles were addressed. On the other hand, there are also reasons that seem to discourage users from switching to passwordless authentication. In the following Section VII, we make suggestions how most of these problems could be addressed in a way so that passwordless authentication may appeal to the majority of the users.

E. Stability of Findings

In practice, the process of introducing users to new authentication methods is usually not as detailed as in our study. On the one hand, most websites only offer minimal information in the form of an abstract text and rarely a step-by-step guide. On the other hand, not all users are willing to spend several minutes watching an introduction video. To ensure the validity of our findings also for such conditions, after our main study we tested another group of participants (1FA control group, or short: $\text{Group}_{\text{1FAcon}}$) to whom we explicitly provided no detailed introduction about FIDO2 and the security key.

$\text{Group}_{\text{1FAcon}}$ (n = 47) went through the same test procedure as $\text{Group}_{\text{1FA}}$ from our main study except for the following two changes: 1) we omitted the introduction video and any communication of benefits or risks (Stages 2–5 in main study); and 2) we added minimal guidance on how to use the security key in a modal dialog on the websites' registration pages. This dialog was optional for registration/login and only appeared if participants explicitly *"clicked for more info"* on the registration page (see Figure 3 in Appendix E). The design of this dialog was copied from the 2FA instructions for activating a security key on the actual Facebook and Google sites (see Figures 4 and 5 in Appendix E for a comparison).

a) Quantitative results: Appendix E provides all analyses presented for the main study supplemented by the data of $\text{Group}_{\text{1FAcon}}$. In general, $\text{Group}_{\text{1FAcon}}$ did not substantially differ from the other groups in terms of demographic composition. In line with the results from the main study, we found significant higher SUS and acceptance scores in $\text{Group}_{\text{1FA}}$ and $\text{Group}_{\text{1FAcon}}$ than in $\text{Group}_{\text{Pass}}$ ($M = 71.77$) , but no differences between the two FIDO2 groups ($\text{Group}_{\text{1FA}}$ and $\text{Group}_{\text{1FAcon}}$). A regression analysis, following the approach from our main study, showed very similar results. In total 42.6% of the empirical variance in acceptance could be explained by the predictors in the model. Significant effects on the acceptance were found only for SUS ($b = .03$, $p < .001$) and the predictors that represent the differences between $\text{Group}_{\text{Pass}}$ ($b = .70$, $p < .001$) and $\text{Group}_{\text{1FAcon}}$ ($b = .66$, $p < .001$). A more detailed analysis showed no significant difference between the two FIDO2 groups ($b = .04$, $p = .720$). In contrast to the main study, a post-hoc relative importance assigned SUS a slightly higher relative importance (56.2%) than the predictors that represent the differences between the groups (41.9%). Thereby, the calculation of the relative importance of predictors is also subject to effects of sampling measurement error, which may explain deviations in this range [70]. In summary, the quantitative results of $\text{Group}_{\text{1FAcon}}$ suggested that even without a detailed introduction, FIDO2 passwordless authentication was perceived as more usable and was more accepted than traditional password-based authentication.

b) Qualitative results: Two independent researchers evaluated the free text answers of $\text{Group}_{\text{1FAcon}}$ and neither found a topic that was not yet included in the code-book from the main study. Consequently, this coding scheme was used to allow comparison to the results of the main study. In general, there were only very limited differences in the response patterns between $\text{Group}_{\text{1FAcon}}$ and $\text{Group}_{\text{1FA}}$. For instance, in both groups a similar proportion of participants mentioned the reduction of cognitive effort as a great advantage of passwordless technology ($\text{Group}_{\text{1FAcon}}$ 94%, $\text{Group}_{\text{1FA}}$ 96%), but also specific restrictions in applicability of passwordless authentication were mentioned by participants from both groups ($\text{Group}_{\text{1FAcon}}$ 13%, $\text{Group}_{\text{1FA}}$ 30%). However, specific differences between both groups were found for *B.2 Threat model* and *D.2 System transparency*. In contrast to $\text{Group}_{\text{1FA}}$ (17%), a higher proportion of people in $\text{Group}_{\text{1FAcon}}$ (49%) were worried as they considered their accounts to be unprotected as soon as their security key fell into the wrong hands (*P47: "I am very afraid that the key will be lost and someone else will get access to all my passwords"*). Also, a larger proportion of the participants in $\text{Group}_{\text{1FAcon}}$ (49% vs 20% in $\text{Group}_{\text{1FA}}$) showed distrust regarding the security key (*P28: "Privacy, how do they collect our data and how much data do "they" have (Who are "they"?)"*). Additionally, participants in the $\text{Group}_{\text{1FAcon}}$ more often (47%) explicitly stated that they lack the knowledge to understand and trust passwordless authentication than in the $\text{Group}_{\text{1FA}}$ (17%)(*P43 :"[. . .] I would need more information about how it works, to really judge the key"*). In summary, the qualitative results of $\text{Group}_{\text{1FAcon}}$ suggested that even without the detailed introduction of passwordless authentication, the same thoughts and opinions were triggered as in the main study. However, the results also showed that, as expected from previous research, a lack of clarity about the functionality and security benefits of authentication methods can lead to more open questions and concerns among users.

c) Willingness to (not) use passwordless authentication: We applied the same code book (see Table IV in Section VI) for the $\text{Group}_{\text{1FAcon}}$ responses about why or why not they would be willing to use 1FA authentication. Our results show that the "Yes, but" subgroup is the largest in $\text{Group}_{\text{1FAcon}}$. In contrast to $\text{Group}_{\text{1FA}}$ (13; 28%), 25 (53%) out of 47 participants in $\text{Group}_{\text{1FAcon}}$ mentioned that they would be willing to use 1FA under some conditions. This is twice as many as in $\text{Group}_{\text{1FA}}$. Most of the participants in both $\text{Group}_{\text{1FA}}$ and $\text{Group}_{\text{1FAcon}}$ mentioned the almost exact same arguments, only with different ranking: in $\text{Group}_{\text{1FAcon}}$, almost of a quarter (10; 21%) of the participants named "Mistrust," while only 3 (6%) mentioned this in $\text{Group}_{\text{1FA}}$. A detailed comparison of the willingness among the two 1FA groups is presented in Table XI in Appendix E.

VII. Discussion

We discuss the results of our study and make recommendations to try to address users' concerns.

A. Closer to a Password Killer?

In our expert assessment, FIDO2 with a security key ticks off almost all benefits and our quantitative results also clearly show that end-users consider this solution both usable and convenient, and do accept it more than text-based passwords. So, is FIDO2 the kingslayer for web authentication? While its

high acceptance is encouraging for the future, our qualitative results show a gap between the users' demands and concerns and the current status of FIDO2 authentication with hardware tokens. In the following, we discuss the aspects that we find most interesting in more detail and try to outline recommendations on how the users' concerns could be addressed.

1) ***Recovery at scale****:* A predominant concern among the participants in Group_{1FA} was the loss of the security key, which they feared would bar them from accessing their accounts. This is in line with prior user study results on 2FA with security keys. Up until today, this issue has not been properly addressed, e.g., the FIDO Alliance recommends as account recovery practice for relying parties [71] to *"strongly encourage account holders to add additional authenticators when the account is created or when the account with no additional authenticator is identified"*, such that users retain account access in case an authenticator is lost or broken. A review of how top websites advise their users to set up fallback and backup authentication mechanisms (see Table V) showed mixed and inconsistent guidance. Most websites only require setup of one second factor but do not enforce a backup factor, with the notable exceptions of Dropbox and Google's Advanced Protection Program.

A new, very likely future challenge for account recovery with FIDO2 1FA (and even with 2FA), in contrast to prior scenarios, will be the scale of the recovery effort. The unlinkable reuse of a single authenticator is considered a strong point of FIDO2 authentication, since the user only needs one device for all accounts. However, if the device is lost, the user has to potentially recover access to *all* accounts for which this authenticator was registered. Unless the user employed the same backup device for all accounts, allowing for an easy switch of the authenticator, the task of account recovery can become burdensome and frustrating, considering that users have an increasing number of accounts [45]. This can potentially impede future adoption of FIDO2 1FA.

Recommendation: *Reusing an authenticator across websites amplifies the risk of losing access to multiple accounts at once. Users have to be supported and guided in strategies for* scalable *account recovery.*

2) ***Authenticator revocation****:* A new concern in this setting that a few participants raised is device theft and account access by the thief. Security discussions around FIDO2 and also prior work on 2FA [26] noted that this risk is lower than the risk of being victim of a phishing campaign or server breach, and further, that the thief needs physical access. This is the objective view of a global risk assessment, which is in stark contrast to the users' subjective view we found. We think that those concerns are discarded too prematurely in a discussion of passwordless authentication. Recent results [72] have shown the length to which abusers in intimate partner violence are willing to go or users might have added personally identifiable information to their key [73] that allows linking the key with accounts. It is unclear to which extent passwordless authentication will ease or hamper such targeted attacks (e.g., a physical token might not be as concealable as a memorized password, but passwords can be more easily phished). We think that if the industry does not take these user concerns seriously, FIDO2 will fail as the password replacement.

TABLE V: User guidance to set up 2FA on popular websites

Website	During 2FA Setup	User Settings
Google (regular)	User can chose between different authentication options (Security Key, Google Prompt, Text message/voice call)	Shows hints and warnings about backup authentication; information on various additional factors
Google (A.P.P.)	User needs two security keys (one key as backup)	—
Dropbox	Only SMS/TOTP as factor, optional backup with phone and OTP	Offers additional factors
Github	Only SMS/TOTP as factor, recommended OTP as backup	Offers additional factors
Facebook	Only SMS/TOTP as factor	Offers additional factors
Twitter	SMS or security key	Offers additional factors

During Setup: User requirements for setting up 2FA and information given during registration about additional authentication options. *User Settings*: Information given to user, if user clicks on "Learn more" or searches the account settings after setup.

Recommendation: *The user has to be able to securely revoke access to their account without the need to first recover access themselves in order to have a chance of account lockdown before the illegitimate access. Potential inspiration can be drawn from established solutions, such as key revocation in PKI [31] or GPG, or revisiting key sharing as in Pico [27].*

3) ***Corner cases****:* Some participants pointed out that the Yubico Security Key cannot be used on devices without an (accessible) USB port. In fact, in contrast to passwords, which can be entered anywhere—the *FROM-ANYWHERE* benefit by Stajano [27]—token-based authentication will currently always have corner cases in which it is not applicable (e.g., public or embedded computers without accessible USB, Bluetooth, or NFC interface). We argue that it is unlikely that this situation changes in the near future.

Recommendation: *Users should be informed about corner cases in which they cannot make use of passwordless authentication, since layman users presumably cannot predict consequences of the combination of client devices and authenticator.*

4) ***Form and features of the authenticator****:* A few participants pointed out problems with the authenticator we used in our study, a Yubico Security Key. Most of those concerns were about the limited connectivity and hence lack of support for other client devices (e.g., mobile phone via NFC or Bluetooth). Other concerns were about the price of the device, its robustness and usability, the lack of additional authentication to the authenticator, or more generally about the fact that users have to carry an extra device.

Recommendation: *Since FIDO2 does not define the form of the authenticator, just its capabilities and protocols, this is a great opportunity to tailor authenticator form and features to user demands, maybe avoiding the need to buy and carry dedicated devices and offer personalized authentication.*

For instance, mobile phones have been recognized as attractive second factors, since most users already own one, carry them with them all the time and notice their loss quickly [74], [75], they are increasingly equipped with biometrics, and they support multiple media (NFC, Bluetooth). However, other forms are imaginable, such as wearables, like fitness tracker wristbands. Yet, an interesting question is to which extent the authenticator device type could undermine the security guarantees of FIDO2, for instance, if users lose their phone regularly [76], do not protect access to their device [77], [78], or depend on the battery life of the phone [34].

*5) **Establishing mental models**:* Finally, during our study, we noticed that our participants identify "authentication" automatically with "passwords" and naturally did not have a mental model of how passwordless authentication with a security key works, what its benefits and drawbacks are, or its applicability. The results of our Group_{1FA} and Group_{1FAcon} show that our introduction video panned out positive—our Group_{1FA} mentioned the security benefits, ease of use, and acceptance of FIDO2 passwordless authentication while Group_{1FAcon} had remaining trust issues and misunderstood benefits. Yet, the result of Group_{1FA} is not ideal. Some participants expressed mistrust into the hardware token, mostly due to a lack of transparency, and recent security incidents [79] could reinforce such mistrust. Thus, work that increases the trustworthiness of the device [80] is important. Further, our participants raised concerns that we did not cover in our video (e.g., recovery and revocation) or that we did not predict (e.g., corner cases).

Recommendation: *Transition to FIDO2 passwordless authentication requires establishing mental models of users that see authentication more systematically, drawing from existing models about physical keys (e.g., possession of key means no other can access the account; spare keys can & should be used; do not store them with personally identifying information; associate account and the right physical key; etc.).*

B. Threats to Validity

Our participants were comparatively young, which is a common problem of lab studies in a university setting. On the other hand, the ATI scores, which usually correlate negatively with the age variable, are in our sample comparable to other studies that had a much more diverse age distribution among their participants (e.g., [50]). This suggests that our results should be fully transferable to age-diverse samples.

For our hands-on tasks, we used artificial scenarios, since FIDO2 passwordless authentication is not (reliably) supported by any service, and our setup phase is simplistic (i.e., no wizards or user settings, but in-place substituting passwords for the security key on the registration/landing page of our websites). Prior work has identified the setup phase as problematic [40] and recommended to study this phase separately. However, for FIDO2 the used security key was really just plug'n'play and even Group_{1FAcon} with minimal, optional instructions was able to intuitively use it. Thus, we argue this allowed us to study the larger context of users switching to 1FA and to derive concrete recommendations for future studies and their design of the user registration processes.

We only used one type of authenticator (the Yubico Security Key, as one of the most popular authenticators in the market) and did not collect any behavioral data (i.e. the time required for the login process). Therefore, some of our results may only apply to this particular setting and neglect such objective aspects of usability. Both these choices resulted from our focus on qualitative research questions, such as for users' perceptions of FIDO2 and subjective obstacles for the usage of this technology. Future work could follow a pure quantitative approach, that uses a between-subject design to test the usability and acceptance of different types of authenticators (e.g. different form factors or pin protection) as well as the effects on the time efficiency of the login process. However, prior works have already shown that in general security keys are more efficient [25], [43] than text-based passwords.

VIII. Conclusion

The FIDO2 standard has great potential to become the successor to text-based passwords for user authentication on the web. To gain insights on whether also end-users would accept this paradigm shift from the traditional knowledge-based factor to the new possession-based factor, we conducted a large-scale lab study. Our participants shared with us their impressions, thoughts, and concerns about using FIDO2 passwordless authentication with a Yubico Security Key.

Our results show that users consider FIDO2 passwordless authentication as more usable and more acceptable than the traditional password-based authentication, but also that concerns remain that impede many users' willingness to abandon passwords. Most notably, the fear of losing the authenticator is not only connected with account recovery but also with an imminent illegal access to the account and the need for revocation—-a subjective threat model by users that differs from the objective risk assessment of FIDO2. Further, limited applicability and critique of the authenticator devices themselves have been pointed out. Thus, our results highlight new hurdles on the road to replace passwords with FIDO2 1FA. We think that these concerns are rooted in a gap between the user's *personal* perspective onto this new technology and the global view of the FIDO2 designers that might not sufficiently include the users' views. In the end, fulfilling users' subjective needs is what determines the success of a new authentication technology. What would be the point of trying to kill the king if the people would not follow the new ruler? We made some recommendations for the supporters and adopters of FIDO2 in an effort to address the concerns we could identify.

Acknowledgments

We like to thank our anonymous reviewers for their valuable feedback. We also thank Blase Ur for being an extremely supportive point of contact for the revision of this paper. Finally, we like to thank Roman Tabachnikov for his work on the Fakebook and Schmoogle setups.

References

[1] 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 *S&P*, 2012.

[2] C. Herley, P. C. van Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?" in *FC*, 2009.

[3] FIDO Alliance. (2019) Fido members. [Online]. Available: https://fidoalliance.org/members/

[4] L. H. Newman. (2018, Sep.) The new yubikey will help kill the password. [Online]. Available: https://www.wired.com/story/yubikey-series-5-fido2-passwordless/

[5] S. Ranger. (2018, May) Windows 10: We're going to kill off passwords and here's how, says microsoft. [Online]. Available: https://www.zdnet.com/article/windows-10-were-going-to-kill-off-passwords-and-heres-how-says-microsoft/

[6] L. Vaas. (2019, Feb.) Android nudges passwords closer to the cliff edge with fido2 support. [Online]. Available: https://nakedsecurity.sophos.com/2019/02/26/android-nudges-passwords-closer-to-the-cliff-edge-with-fido2-support/

[7] S. Ceti. (2018, Sep.) The password is dead, long live web authentication. [Online]. Available: https://www.computerworld.com.au/article/647205/password-dead-long-live-web-authentication/

[8] World Wide Web Consortium. (2019, Mar.) Web authentication: An api for accessing public key credentials level 1 — w3c recommendation, 4 march 2019. [Online]. Available: https://www.w3.org/TR/webauthn/

[9] FIDO Alliance. (2019, Jan.) Client to authenticator protocol (ctap) — proposed standard, january 30, 2019. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html

[10] ——. (2019, Feb.) Android now fido2 certified, accelerating global migration beyond passwords. [Online]. Available: https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/

[11] D. Peck. (2018, Oct.) Webauthn and biometrics. [Online]. Available: https://davepeck.org/2018/10/26/webauthn-and-biometrics/

[12] J. Chong. (2018, Aug.) 10 things you've been wondering about fido2, webauthn, and a passwordless world. [Online]. Available: https://www.yubico.com/2018/08/10-things-youve-been-wondering-about-fido2-webauthn-and-a-passwordless-world/

[13] A. Deveria. (2019, May) Can i use webauthn? [Online]. Available: https://caniuse.com/#search=webauthn

[14] B. Girardeau. (2018, May) Introducing webauthn support for secure dropbox sign in. [Online]. Available: https://blogs.dropbox.com/tech/2018/05/introducing-webauthn-support-for-secure-dropbox-sign-in/

[15] A. Simons. (2018, Nov.) Secure password-less sign-in for your microsoft account using a security key or windows hello. [Online]. Available: https://www.microsoft.com/en-us/microsoft-365/blog/2018/11/20/sign-in-to-your-microsoft-account-without-a-password-using-windows-hello-or-a-security-key/

[16] Microsoft. (2018, Jul.) Web authentication and windows hello. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-edge/dev-guide/windows-integration/web-authentication

[17] B. Wong. (2019, May) WebAuthn: The future of device based 2FA at Twitter. [Online]. Available: https://blog.twitter.com/engineering/en_us/topics/infrastructure/2019/webauthn.html

[18] M. Wielgoszewski. (2019, May) Securing your gemini account with webauthn. [Online]. Available: https://medium.com/gemini/securing-your-gemini-account-with-webauthn-b5f369b8beec

[19] Y. Mehta. (2019, May) Windows hello fido2 certification gets you closer to passwordless. [Online]. Available: https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Hello-FIDO2-certification-gets-you-closer-to/ba-p/534592

[20] C. Brand and E. Kitamura. (2019) Enabling strong authentication with webauthn. [Online]. Available: https://developers.google.com/web/updates/2018/05/webauthn

[21] Yubico. (2019) Developer program. [Online]. Available: https://developers.yubico.com

[22] Y. Ackermann. (2019) Webauthn awesome: A curated list of awesome webauthn/fido2 resources. [Online]. Available: https://github.com/herrjemand/awesome-webauthn

[23] A. Powers. A node.js library for performing fido 2.0 / webauthn server functionality. [Online]. Available: https://github.com/apowers313/fido2-lib

[24] ——. A simple webauthn / fido2 javascript application. [Online]. Available: https://github.com/apowers313/webauthn-simple-app

[25] J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas, "Security keys: Practical cryptographic second factors for the modern web," in *Financial Cryptography and Data Security*, 2017.

[26] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A qualitative study on usability and acceptability of yubico security key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST '17)*, 2018.

[27] F. Stajano, "Pico: No more passwords!" in *Security Protocols Workshop*. Springer, 2011.

[28] S. Aebischera, C. Dettoni, G. Jenkinson, K. Krol, D. Llewellyn-Jones, T. Masui, and F. Stajano, "Pico in the wild: Replacing passwords, one site at a time," in *2nd European Workshop on Usable Security (EuroUSEC '17)*, 2017.

[29] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8446.txt

[30] A. Parsovs, "Practical issues with tls client certificate authentication," in *Proc. 21th Annual Network and Distributed System Security Symposium (NDSS '14)*, 2014.

[31] J. S. Conners and D. Zappala, "Let's Authenticate: Automated Cryptographic Authentication for the Web with Simple Account Recovery," in *Who Are You?! Adventures in Authentication Workshop (WAY '19)*, 2019.

[32] D. Strouble, G. m. Shechtman, and A. S. Alsop, "Productivity and usability effects of using a two-factor security system," in *SAIS*, 2009.

[33] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," *Computers & Security*, vol. 28, no. 1, pp. 47 – 62, 2009.

[34] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153 – 164, 2010.

[35] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, no. 4, pp. 208 – 220, 2011.

[36] K. Krol, E. Philippou, E. D. Cristofaro, and M. A. Sasse, ""they brought in the horrible key ring thing!" analysing the usability of two-factor authentication in uk online banking." in *Workshop on Usable Security and Privacy (USEC'15)*, 2015.

[37] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A comparative usability study of two-factor authentication," in *Workshop on Usable Security and Privacy (USEC'14)*, 2014.

[38] M. Fagan and M. M. H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," in *Proc. 12th Symposium on Usable Privacy and Security (SOUPS'16)*, 2016.

[39] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor: A two-phase usability study of the fido u2f security key," in *Financial Cryptography and Data Security*, 2018.

[40] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," in *Proc. 39th IEEE Symposium on Security and Privacy (SP '18)*, 2018.

[41] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards Implementing Inclusive Authentication Technologies for Older Adults," in *Who Are You?! Adventures in Authentication Workshop (WAY '19)*, 2019.

[42] J. Brooke, "Sus—a quick and dirty usability scale," *Usability Evaluation Industry*, vol. 189, no. 194, pp. 4–7, 11 1996.

[43] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," in *Proc. 15th Symposium on Usable Privacy and Security (SOUPS'19)*, 2019.

[44] S. Ciolino, S. Parkin, and P. Dunphy, "Of two minds about two-factor: Understanding everyday FIDO u2f usability through device comparison and experience sampling," in *Proc. 15th Symposium on Usable Privacy and Security (SOUPS'19)*, 2019.

[45] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proc. 16th International Conference on World Wide Web (WWW'07)*, 2007.

[46] S. G. Lyastani, M. Schilling, S. Fahl, S. Bugiel, and M. Backes, "Studying the impact of managers on password strength and reuse," in *Proc. 26th USENIX Security Symposium (SEC' 18)*, 2018.
[47] J. D. Van Der Laan, A. Heino, and D. Waard, "A simple procedure for the assessment of acceptance of advance transport telematics," *Transportation Research Part C: Emerging Technologies*, vol. 5, pp. 1–10, 02 1997.
[48] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, no. 3, pp. 319–340, Sep. 1989.
[49] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science*, vol. 46, no. 2, pp. 186–204, 2000.
[50] T. Franke, C. Attig, and D. Wessel, "A personal resource for technology interaction: Development and validation of the affinity for technology interaction (ati) scale," *International Journal of Human–Computer Interaction*, vol. 35, no. 6, pp. 456–467, 2019.
[51] C. Attig, D. Wessel, and T. Franke, "Assessing personality differences in human-technology interaction: An overview of key self-report scales to predict successful interaction," in *HCI International 2017 – Posters' Extended Abstracts*, 05 2017, pp. 19–29.
[52] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, 2004.
[53] N. Schwarz and S. Sudman, *Context effects in social and psychological research*. Springer Science & Business Media, 2012.
[54] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, and J. P. Richer, "NIST SP800–63B: Digital authentication guideline (Authentication and Lifecycle Management)," June 2017, last visited: 30/05/2019.
[55] R. West, "The psychology of security," *Commun. ACM*, vol. 51, no. 4, pp. 34–40, Apr. 2008.
[56] S. Ghorbani Lyastani. (2020, Jan.) Introduction videos for fido2 1fa user study. [Online]. Available: https://www.youtube.com/watch?v=_UCLBLo-fQI&list=PLJ3WH6JNU1HSyZKAfWtRLG0ONd5nsuABJ
[57] M. Langer, C. J. König, and A. Fitili, "Information as a double-edged sword: The role of computer experience and information on applicant reactions towards novel technologies for personnel selection," *Computers in Human Behavior*, vol. 81, pp. 19–30, 2018.
[58] S. Farrell. (2016, May) Open-ended vs. closed-ended questions in user research. [Online]. Available: https://www.nngroup.com/articles/open-ended-questions/
[59] J. Lazar and S. D. J. Barbosa, "Introduction to human-computer interaction," in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*, 2017.
[60] D. A. Gioia, K. G. Corley, and A. L. Hamilton, "Seeking qualitative rigor in inductive research: Notes on the gioia methodology," *Organizational Research Methods*, vol. 16, no. 1, pp. 15–31, 2013.
[61] A. Wilhelmy, "Journal guidelines for qualitative research? a balancing act that might be worth it," *Industrial and Organizational Psychology*, vol. 9, no. 4, p. 726–732, 2016.
[62] S. B. Merriam and E. J. Tisdell, *Qualitative research: A guide to design and implementation*. John Wiley & Sons, 2015.
[63] K. Krippendorff, *Content Analysis: An Introduction to Its Methodology (second edition)*. Sage Publications, 2004.
[64] A. Bangor, P. Kortum, and J. Miller, "Determining what individual sus scores mean: Adding an adjective rating scale," *J. Usability Studies*, vol. 4, no. 3, May 2009.
[65] J. Sauro, *A practical guide to the system usability scale: Background, benchmarks & best practices*. Measuring Usability LLC Denver, CO, 2011.
[66] M. Koller and W. A. Stahel, "Nonsingular subsampling for regression s estimators with categorical predictors," *Computational Statistics*, vol. 32, no. 2, pp. 631–646, Jun 2017.
[67] T. S. Breusch and A. R. Pagan, "A simple test for heteroscedasticity and random coefficient variation," *Econometrica: Journal of the Econometric Society*, pp. 1287–1294, 1979.
[68] F. Wolf, R. Kuber, and A. J. Aviv, ""pretty close to a must-have": Balancing usability desire and security concern in biometric adoption," in *Proc. 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, 2019.
[69] M. Koller and W. A. Stahel, "Sharpening wald-type inference in robust regression for small samples," *Computational Statistics & Data Analysis*, vol. 55, no. 8, pp. 2504–2515, 2011.
[70] J. W. Johnson, "Factors affecting relative weights: The influence of sampling and measurement error," *Organizational Research Methods*, vol. 7, no. 3, pp. 283–299, 2004.
[71] FIDO Alliance, "Recommended account recovery practices for fido2 relying parties," Feb. 2019. [Online]. Available: https://fidoalliance.org/recommended-account-recovery-practices/
[72] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart, "The spyware used in intimate partner violence," in *Proc. 39th IEEE Symposium on Security and Privacy (SP '18)*, 2018.
[73] Yubico Developer Program. Card edit. [Online]. Available: https://developers.yubico.com/PGP/Card_edit.html
[74] S. Brunswick, "ecommerce fraud – time to act," *Card Technology Today*, vol. 21, no. 1, pp. 12–13, 2009.
[75] N. Dragoljub, "Stronger security," *Card Technology Today*, vol. 19, no. 1, pp. 9–10, 2007.
[76] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David, "Biometric authentication on a mobile device: A study of user effort, error and task disruption," in *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12)*, 2012.
[77] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proc. 21th ACM Conference on Computer and Communication Security (CCS '14)*, 2014.
[78] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014.
[79] C. Brand. (2019, May) Advisory: Security issue with bluetooth low energy (ble) titan security keys. [Online]. Available: https://security.googleblog.com/2019/05/titan-keys-update.html
[80] E. Dauterman, H. Corrigan-Gibbs, D. Mazières, D. Boneh, and D. Rizzo, "True2f: Backdoor-resistant authentication tokens," in *Proc. 40th IEEE Symposium on Security and Privacy (SP '19)*, 2019.

APPENDIX A
DETAILS ON COMPARISON OF TEXT-BASED PASSWORDS WITH FIDO2 1FA USING A YUBICO SECURITY KEY

A. Benefits dependent only on FIDO2

a) Usability: FIDO2 is *Scalable-for-Users* (●), as a single authenticator can be used for hundreds of accounts. It never offers the *Nothing-to-Carry* (○) benefit, since it uses *hardware-based* authenticators. FIDO2 does not inherently provide *Easy-Recovery-from-Loss* (○), but the website has to offer recovery or secondary authentication options.

b) Deployability: FIDO2 is not *Server-Compatible* (○), since the relying parties have to support it separately and cannot piggyback on text-based password authentication. However, with WebAuthn as a W3C standard implemented in all browsers, FIDO2 is *Browser-Compatible* (●), *Mature* (●), and *Non-Proprietary* (●[2]).

c) Security: FIDO2 is *Resilient-to-Physical-Observation* (●), since it shifts the authentication to a possession-based factor. As a challenge-response protocol based on a public key cryptography, it is *Resilient-to-Targeted-Impersonation* (●), *Resilient-to-Throttled-Guessing* (●), and *Resilient-to-Unthrottled-Guessing* (●). Further, since there is no shared secret between the user and the relying party, which has to be entered or sent by the user, or stored by the website, and there is mutual authentication between the authenticator and the website, FIDO2 is also *Resilient-to-Leaks-from-Other-Verifiers* (●) and *Resilient-to-Phishing* (●). FIDO2 has *No-Trusted-Third-Party* (●). Lastly, during the registration a new unique key pair is created by the authenticator per account and use of the key restricted to a single origin, which prevents a linking of authenticators and hence linking/tracking of user accounts (based on the used key pair), and makes FIDO2 *Unlinkable* (●).[3]

[2]Most authenticators in the market are proprietary, although open-source solutions exist and one can build their own authenticator.

[3]Naturally, accounts could be linked based on information independent of FIDO2, e.g., username, email address, etc.

B. Benefits dependent primarily on authenticator

a) Usability: FIDO2 with the Yubico Security Key as single-factor is *Memorywise-Effortless* (●) because the user only needs to press the capacitive button to authenticate, but does not have to remember a secret. This is a good first example where this benefit purely depends on the authenticator. For instance, Windows Hello uses the TPM as authenticator [15]. The TPM is an internal authenticator and does not have any physical entry method, such as a separate keyboard or button, thus the user has to "show presence" and approve authentication by supplying a PIN (in absence of biometric devices), which would make the TPM as a single factor at most *Quasi-Memorywise-Effortless* according to Bonneau et al. [1]. The simple button push makes the Security Key also *Physically-Effortless* (●). The TPM as authenticator with PIN entry would be at most *Quasi-Physically-Effortless*. Inserting the Security Key and pressing a flashing button when prompted by the browser is not more complicated than using text-based passwords and makes the Security Key *Easy-to-learn* (●) and *Efficient-to-use* (●). It is easily conceivable that not all authenticators are necessarily as intuitive as a button press. Assuming proper implementation, FIDO2 should have *Infrequent-Errors* (●) [25], however, this error rate depends on the authenticator. For instance, biometric user authentication to the authenticator might induce more frequent errors [68].

b) Deployability: The Security Key is *Accessible* (●), since pushing the button does not form a higher hurdle than a password entry. Again, this might change with a different authenticator device (e.g., being able to handle a smartphone). FIDO2 does not impose additional costs per user on the service, however, depending on the authenticator device, the investment by each user varies. With a one-time investment of $20–$27 for the Yubico Security Key, we consider this solution as *Quasi-Negligible-Cost-per-User* (◐), since built-in authenticators like TPM or Apple's TouchID & FaceID would not incur extra costs, while, for example, the Feitian BioPass FIDO2 Security Key costs with $50 around twice as much.

c) Security: Since the Security Key has its own physical button, it is *Resilient-to-Internal-Observation* (●). However, authenticators like the TPM, which do not have a trusted path to the user, are still susceptible to internal observation of the PIN/password to use the TPM and have to rely on complex setups like extended authorization policies to overcome this limitation. A security key, when used as single factor, is not *Resilient-to-Theft* (○), since possession of the token alone suffices to authenticate. Requiring pushing the button is *Requiring-Explicit-Consent* (●) to authenticate. Internal authenticators without a trusted path might not be able to provide this benefit.

APPENDIX B
SURVEY QUESTIONS

Acceptance: Please judge the presented authentication method on the following adjectives.

Useless	○	○	○	○	○	Useful
Unpleasant	○	○	○	○	○	Pleasant
Bad	○	○	○	○	○	Good
Annoying	○	○	○	○	○	Nice
Superfluous	○	○	○	○	○	Effective
Irritating	○	○	○	○	○	Likeable
Worthless	○	○	○	○	○	Assisting
Undesirable	○	○	○	○	○	Desirable
Sleep-inducing	○	○	○	○	○	Raising alertness

System Usability Scale (SUS): Please state your level of agreement or disagreement for the following statements based on your experience with the presented authentication method. There are no right or wrong answers. (Strongly disagree; Disagree; Neither disagree nor agree; Agree; Strongly agree.)

1) I think that I would like to use this system frequently.
2) I found the system unnecessarily complex.
3) I thought the system was easy to use.
4) I think that I would need the support of a technical person to be able to use this system.
5) I found the various functions in this system were well integrated.
6) I thought there was too much inconsistency in this system.
7) I would imagine that most people would learn to use this system very quickly.
8) I found the system very awkward to use.
9) I felt very confident using the system.
10) I needed to learn a lot of things before I could get going with this system.

Affinity for Technology Interaction (ATI): In the following, we will ask you about your interaction with technical systems. The term "technical systems" refers to apps and other software applications, as well as entire digital devices (e.g., Mobile phone, computer, TV, car navigation). Please indicate the degree to which you agree/disagree with the following statements. There are no right or wrong answers. (Completely disagree; Largely disagree; Slightly disagree; Slightly agree; Largely agree; Completely agree)

1) I like to occupy myself in greater detail with technical systems.
2) I like testing the functions of new technical systems.
3) I predominantly deal with technical systems because I have to.
4) When I have a new technical system in front of me, I try it out intensively.
5) I enjoy spending time becoming acquainted with a new technical system.
6) It is enough for me that a technical system works; I don't care how or why.
7) I try to understand how a technical system exactly works.
8) It is enough for me to know the basic functions of a technical system.
9) I try to make full use of the capabilities of a technical system.

Privacy Concern: Please state how much you agree or disagree to the following statements. There are no right or wrong answers. (Strongly disagree; Disagree; somewhat disagree; Neither disagree nor agree; somewhat agree; Agree; Strongly agree.)

1) I am concerned that companies are collecting too much information about me.
2) I am concerned about my privacy.
3) To me it is important to keep my privacy intact.
4) Novel technologies are threatening privacy increasingly.

Technical Problems: Were there any technical problems while watching the video and trying out the presented authentication method?
(i) No problems, (ii) Few problems, (iii) Some problems, (iv) Many problems
If you have experienced technical problems before, during, or after watching the video or trying out the presented authentication method, please describe them briefly.

Open-Ended Questions: How would you describe your general experience about the presented authentication with a Yubikey[4] (Only in Group_{1FA})? [Free response]
Which advantages do you see in the usage of the presented authentication method ? [Free response]
Which disadvantages do you see in the usage of the presented authentication method? [Free response]
Would you use the presented authentication method yourself? If you would, why and on which accounts would you use it? If you wouldn't, why not (Only in Group_{1FA})? [Free response]

Further Questions: How do you choose your password for a new email account? (i) Reuse an existing password, (ii) Modify an existing password, (iii) Create an entirely new password, (iv) No answer, (v) Other
Has ever one of your passwords been leaked or been stolen? (i) Yes, (ii) No

[4]For simplicity for our participants, we called the "Yubico Security Key" just "Yubikey" in our study

Demographic Questions: Please indicate your gender.
(i) Male, (ii) Female, (iii) Other, (iv) No answer
Please indicate your highest educational degree. (i) High school graduate, (ii) Bachelor's degree, (iii) Master's degree, (iv) Diploma, (v) Ph.D, (vi) Other
How old (in years) are you? Free response
Please indicate if you have a computer science background. (i) Yes, (ii) No
Please indicate your area of studies/area of work. Free response

APPENDIX C
CODE BOOK

TABLE VI: Code book

Topics and aspects
A. Shift from cognitive to physical effort
A.1 Mental effort (password)
A.1.1 Creating passwords
A.1.2 Memorizing passwords
A.1.3 Efficient and easy to use
A.2 Mental effort (1FA)
A.2.1 Reduction of cognitive effort
A.2.2 Efficient and easy to use
A.3 Physical effort (password)
A.3.1 Password entry
A.3.2 No extra hardware
A.4 Physical effort (1FA)
A.4.1 Carrying an extra device
B. Changes in threat model
B.1 Threat model (password)
B.1.1 Cracking and phishing passwords
B.2 Threat model (1FA)
B.2.1 Device theft/loss
B.2.2 Access to account by owner (recovery)
B.2.2 Access to account by other (revocation)
B.2.2 Fallback authentication
C. Restrictions in applicability
C.1 Applicability (password)
C.1.1 Universally applicable
C.2 Applicability (1FA)
C.2.1 Device and connectivity support
C.2.2 Account sharing
D. Breaking with traditions and habitual patterns is hard
D.1 System transparency (password)
D.1.1 Personal secret
D.1.2 Familiar scheme
D.1.3 Positive past experience
D.2 System transparency (1FA)
D.2.1 Mistrust
D.2.2 Lack of knowledge
D.2.3 Perceived security
D.3 Affective perception (password)
D.3.1 Boring / monotonous
D.4 Affective perception (1FA)
D.4.1 Fun / Excitement
D.4.2 Positive feedback about introduction video
E. Security key characteristics
E.1 Robustness and maturity
E.2 Cost

TABLE VII: Model Comparison

	Res.Df	R^2adj.	step-wise comparison		
			δDf	W	p
Users characteristics	90	<0.1%			
+ usability	89	28.0%	1	35.96	**<.01**
+ authentication type	88	48.8%	1	34.47	**<.01**
+ interactions	84	51.5%	4	7.26	.12

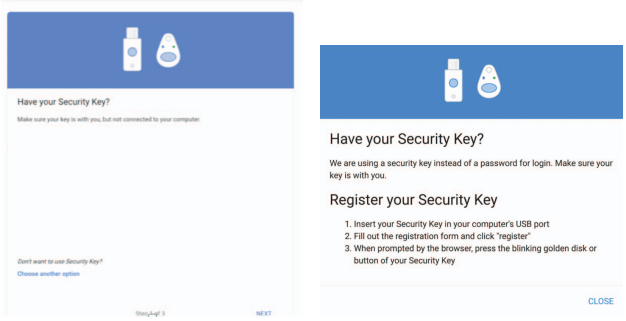
Note: Res.Df = Residual Degrees of freedom, R^2adj. = Percentage of the empirical variance that could be explained by the regression model (adjusted for number of terms in model). Model 3 explains the empirical data best under the conditions of parsimony (Occam's razor), δdf = differences in the number of constraints between models, W = Wald statistic, p values below the 5% criterion are printed in bold. N(total) = 94.

APPENDIX D
MODEL COMPARISON

APPENDIX E
RESULTS INCLUDING GROUP$_{1FACON}$

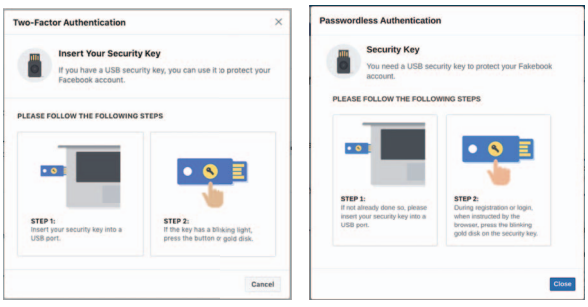
(a) Hint on Schmoogle (b) Hint on Fakebook

Fig. 3: Hint about passwordless login on registration pages with link to modal dialog for information



(a) Google (b) Schmoogle

Fig. 4: Google vs. Schmoogle



(a) Facebook (b) Fakebook

Fig. 5: Facebook vs. Fakebook

TABLE VIII: Overview descriptive data including Group_{1FAcon}

Variable	Group			Statistics	ES
	Pass	1FA	1FAcon		
N	48	46	47		
Gender				$\chi^2(2) = 1.923$	.12
Female	27	26	20	$p = .392$	
Male	20	20	25		
No answer	1	0	2		
Age	24.08	25.78	25.21	$F(2, 138) = 1.479$	.02
	(3.63)	(6.44)	(4.19)	$p = .231$	
Education				$\chi^2(8) = 14.462$	.23
< High school	0	2	3	***p* = .026**	
High school	23	12	10		
Bachelor	12	20	25		
Master	12	11	8		
Diploma	0	1	0		
Ph.D	1	0	1		
ATI	3.84	4.01	4.05	$F(2) = 0.533$	.01
	(1.12)	(0.95)	(1.03)	$p = .588$	
PC	5.43	5.36	5.63	$F(2, 138) = 0.668$	.00
	(1.31)	(1.13)	(1.07)	$p = .514$	
CS background				$\chi^2(2) = 6.047$	.21
Yes	18	28	27	***p* = .047**	
No	30	18	20		
SUS	71.92	81.79	79.20	$F(2, 138) = 9.122$	.12
	(11.09)	(12.15)	(11.91)	***p* < .001**	
Acceptance	3.41	4.29	4.16	$F(2, 138) = 24.420$	.26
	(0.70)	(0.60)	(0.66)	***p* < .001**	

Note: ES = Effect Size; *N* = Number of participants; < High school = Less than high school; ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS background = Computer science background; SUS = System Usability Scale. Depending on the variable, the frequencies or the scale mean values including standard deviation are presented in the cells. The statistics column shows the statistical data parameters for a group comparison with one-way anova respectively with Fisher's exact test for the corresponding variable. p values below the 5% criterion are printed in bold. Effect Sizes are specified in Eta-squared (η^2) for one-way anova and in Cramer's V for Fisher's exact test. N(total) = 141.

TABLE IX: Regression model predicting users acceptance data including Group_{1FAcon}

Predictors	Acceptance			
	b	CI	RI	*p*
(Intercept)	3.57	[3.38 , 3.75]		**<0.001**
ATI	−0.01	[−0.12 , 0.10]	0.9%	0.846
PC	−0.02	[−0.10 , 0.06]	0.3%	0.591
CS (yes)	−0.12	[−0.34 , 0.10]	0.7%	0.269
SUS	0.03	[0.02 , 0.04]	56.2%	**<0.001**
Group			41.9%	
1FA	0.70	[0.47 , 0.94]		**<0.001**
1FAcon	0.66	[0.42 , 0.89]		**<0.001**

Note: Robust regression based on MM estimator [69]. Model 3 can explain 47.1% (R^2adjusted = .471) of the empirical variance (adjusted for number of terms in model); ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS (yes) = Dummy variable that encodes the effect of a computer science background (No background is the default); SUS = System Usability Scale; Group_{1FA} = Dummy variable that encodes the differences for the groups (Group_{Pass} is the default). Group_{1FAcon} = Dummy variable that encodes the differences for the groups (Group_{Pass} is the default). *p*-values below the 5% criterion are printed in bold. *N*(total) = 141.

TABLE X: Model Comparison including Group_{1FAcon}

	Res.Df	R^2adj.	step-wise comparison		
			δDf	*W*	*p*
Users characteristics	137	<0.1%			
+ usability	136	31.0%	1	61.15	**<.01**
+ authentication type	134	47.1%	2	40.44	**<.01**
+ interactions	126	49.9%	8	15.39	.06

Note: Res.Df = Residual Degrees of freedom, R^2adj. = Percentage of the empirical variance that could be explained by the regression model (adjusted for number of terms in model). Model 3 explains the empirical data best under the conditions of parsimony (Occam's razor), δdf = differences in the number of constraints between models, *W* = Wald statistic, *p* values below the 5% criterion are printed in bold. *N*(total) = 141.

TABLE XI: Willingness to (not) use passwordless auth including Group_{1FAcon}

Category	**N(Cat)**		**Arguments**	**N(Arg)**	
	1FA	1FAcon		1FA	1FAcon
Yes	16	8	Easy/Secure/Memorywise-effortless	3	3
Yes, but	13	25	Fear of losing access to own account	5	1
			Fear of account access by others	4	3
			Mistrust	3	10
			Lack of universal access	3	2
			Costly	1	0
Rather not	11	6	Fear of losing access to own account	4	0
			Mistrust	4	2
			Costly	3	0
			Lack of universal access	3	2
			Annoying to carry extra device	1	2
			Lack of knowledge	0	2
No	6	6	Mistrust	3	4
			Annoying to carry extra device	3	0
			Fear of losing access to own account	2	1
			Lack of knowledge	1	1
			Fear of account access by others	1	1
			Costly	1	0
			Lack of universal access	1	2

Note: N(Cat) = Nr. of participants who fell into the corresponding category; N(Arg) = Nr. of participants who named the corresponding argument; Total Nr. of participants in Group_{1FA}: 46, in Group_{1FAcon}: 47.

TABLE XII: Comparison qualitative data

Category	**Group_{1FA}**	**Group_{1FAcon}**
N	46	47
Mental effort		
Reduction of cognitive effort	30 (65%)	37 (79%)
Efficient and easy to use	35 (76%)	37 (79%)
Physical Effort		
Carrying an extra device	16 (35%)	14 (30%)
Threat model		
Device theft/loss	28 (61%)	36 (77%)
Access to account by owner (recovery)	11 (24%)	7 (15%)
Access to account by other (revocation)	8 (17%)	23 (49%)
Fallback authentication	12 (26%)	7 (15%)
Applicability		
Device and connectivity support	14 (30%)	6 (13%)
System transperancy		
Mistrust	9 (20%)	22 (47%)
Lack of knowledge	8 (17%)	22 (47%)
Perceived security	20 (44%)	12 (26%)
Affective perception		
Fun / Excitement	22 (48%)	18 (38%)
Security Key characteristics		
Robustness and maturity	7 (15%)	10 (21%)
Cost	10 (22%)	2 (4%)

Note: (N): Number of participants in both Group_{1FA} and Group_{1FAcon}. Categories that are mentioned here are based on code book in Table VI in Appendix C.