2021-08-06

A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement

Brian Rasmussen
Brigham Young University

A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement

Brian Rasmussen

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Daniel Zapppala, Chair
Kent Seamons
Mike Jones

Department of Computer Science

Brigham Young University

ABSTRACT

A Usability Study of FIDO2 Roaming Software Tokens as a Password Replacement

Brian Rasmussen
Department of Computer Science, BYU
Master of Science

The use of passwords for user authentication has significant shortcomings. As society becomes more dependent on the internet and web services, we need to find a replacement authentication method that users are willing to use. WebAuthn is one potential technology for password replacement. Recent studies have shown that users enjoy the usability of WebAuthn and hardware tokens as a password replacement but don't want to carry them around. Meanwhile, little to no research involves the use of software tokens. I carried out a user study of WebAuthn and roaming software tokens when used as a password replacement. We were able to learn if the shortcoming of WebAuthn and hardware tokens were remedied by the use of smart phones as software tokens. Software tokens have similiar usability to hardware tokens and are more usable than passwords. Users continued fearing loss of access to their account when using software tokens. Users were less worried about carrying an extra device but replaced that fear with the fear of a dead battery or a broken phone.

Keywords: FIDO2, passwordless

Table of Contents

Chapter 1

Introduction

Passwords are the most common form of online authentication, but each year the risk associated with passwords becomes more apparent. One of the problems with passwords is the sheer amount of accounts the average user has. Expecting a user to remember a unique password for each account is impractical and has caused excessive password reuse. Das et al. found that 51% of those surveyed reported that they reuse old passwords and an additional 26% modified a pre-existing one [5]. Along with having to deal with a plethora of accounts, many security measures require users to have passwords with high complexity. Password complexity is encouraged by increasing password length and including a mixture of uppercase and lowercase letters, numbers, and symbols. A study by Wash et al. was able to show that passwords that are more complex or have higher entropy have a higher likelihood of being reused [16]. Password reuse by itself is not detrimental to overall account security, but because of other security vulnerabilities, such as data breaches and hacked accounts, password reuse is highly discouraged. The combination of data breaches and password reuse has caused many users to be susceptible to credential-stuffing attacks. Akamai, the content delivery network, recorded more than 88 billion credential stuffing attacks between January 1st, 2018, and December 31st, 2019 (2 years), [1].

In 2012 Bonneau et al. introduced the seminal paper *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*. This paper introduced a framework for judging potential password replacements by using a list of criteria that compare the security, usability, and deployability of alternate authentication methods.

Because the framework has 25 different criteria, it is unlikely that a password replacement will check all the boxes. Instead, the framework helps us see the pros and cons of each authentication method and how different password replacement stack up against each other.

One of the newest attempts to replace passwords is Fast IDentity Online 2 (FIDO2), which allows users to authenticate by using public-key cryptography and either a hardware token (resembling a USB drive) or a software token (stored on a smartphone). FIDO2 consists of Web Authentication or WebAuthn and Client to Authenticator Protocol (CTAP) protocols. WebAuthn provides an API for web browsers to interact with FIDO tokens, including both single-factor authentication (1FA) or in tandem with other authentication methods for second-factor authentication (2FA) and multiple-factor authentication. CTAP defines the protocol for the Client, usually the browser, to communicate with an authenticator, which is either a hardware or software token. The different mediums of communication include USB Human Interface Device (HID), Near Field Communication (NFC), Bluetooth Smart, and Bluetooth Low Energy (BLE).

Because FIDO2 supports use as a 1FA, it is a potential password replacement option. Although FIDO2 is relatively new, it has support from major companies such as Google, Yubico, and Microsoft. Most major browsers now support FIDO2, including Google Chrome, Edge, Firefox, and Safari. An authenticator has two types, cross-platform and platform-specific. Cross-platform authenticators are roaming devices, such as hardware tokens or mobile devices. Platform-specific authenticators only work for the device in which they reside, such as Face ID and Touch ID on Apple products or Windows Hello on Microsoft products.

Although most major browsers support FIDO2, it is difficult for the general public and online services to adopt new forms of authentication. One of the reasons that passwords have remained the most prevalent form of authentication is because it is hard to motivate users to change to a new system. There have been two recent user studies that explored if users would be willing to switch from passwords to using FIDO2 [12] [7]. Both studies noted that users are willing to switch to passwordless authentication but are less enthusiastic about

having to carry around a hardware token.

However, it is unclear whether users view smartphones used as software FIDO2 tokens differently than hardware tokens when used in the context as a password replacement. Accordingly, I carried out a user study that follows the same design as Lyastani et al. [12], but instead of using hardware tokens, I used software tokens in the form of a smartphone app. Users who participated in the study registered and logged into two mock websites by using a provided mobile device as a roaming authenticator. This was done so the user could gain and opinion about roaming software tokens as password replacement. I used the Krypton app and Chrome extension. Krypton provides cloud-based communication between the browser and smartphones and also implements all the steps required for the phone to be used as a software token for FIDO2. This allowed me to study software tokens in the context of FIDO2 and password replacements.

The study's results showed that users found roaming software tokens for 1FA more usable than passwords. When compared to roaming hardware tokens, there was no significant difference in the two forms of 1FA. Users were less concerned about carrying around an additional item but were concerned with dead phone batteries, installing another app, and needing to log in when their phone is in a different room. Some user worries continued to exist when comparing hardware and software tokens, namely what happens if their authenticator is lost, stolen, or destroyed. The System Usability Score (SUS) [4] is a strong predictor of whether users accepted the software token as a replacement for passwords, while Affinity for Technology Interaction (ATI) [8] and Privacy Concern (PC) [10] are poor predictors.

Chapter 2

Related Work

One of the contenders for password replacement is password managers. Password managers do not replace passwords, but they do address many of the security issues with passwords. When a user correctly uses password managers, there is no password reuse, and the passwords are cryptographically secure [13]. However, studies have shown that users misuse password managers. Lyastani et al. found that only 53% of passwords stored in LastPass, a password manager, were unique [12]. They also found that Chrome Autofill users and users without any form of password manager reused 80% of their passwords [11]. In addition to password reuse, there are also some usability and security issues. One of the most touched upon usability issues is logging in on a non-personal device, such as a library computer. If the password manager uses the cloud, then you can log in to any device with the proper application or browser extension. The problem persists if you do not have permission to add extensions or download the right software. Another issue with password managers is the dependency on the master password. If an attacker ever learns a user's master password, they may gain access to all of a user's accounts. Additionally, if a user forgets or loses their master password, they also lose access to all of their accounts.

Another approach to password replacement has been federated login services, such as Facebook Connect, Google OAuth 2.0, Mozilla Persona, and OpenID [14]. By using federated login, a user only has to login to the first service, and they gain access to other accounts on different websites. One of the main drawbacks of using a third-party service to facilitate single-sign-on is the leakage of privacy. The third party now knows about all accounts the

users log in to, which is a privacy concern [6]. Another issue is that if one account is ever successfully attacked, the attacker now has access to all the services instead of just one.

Because users have a hard time remembering passwords; one idea has been to move to graphical passwords. Some examples of graphical passwords include sketching images or symbols, recognizing a sequence of pictures, and remembering specific positions on images [3]. Graphical passwords have some promise, but there are a few issues. Shoulder-surfing, or looking over someone's shoulder to see their password, is a real risk with graphical passwords. Additionally, graphical passwords take more time to input and are more expensive for websites because they have to store and display images for users.

A category of authentication that has gained some steam is biometrics. There are a few common biometrics, such as fingerprint readers, eye scanners, and facial recognition. These biometric readers have found their niches for authentication for devices such as a mobile device or a laptop. Biometrics are considered acceptable for authentication for a personal device but not always for websites. One issue that applies to all forms of biometrics is that biometrics are not unique across websites. If someone uses their fingerprint to log in to the website "A" and into website "B" and website "A" leaks the fingerprint, then the user is no longer secure on the website "B." In the same scenario where a fingerprint is lost or stolen, the users can not reset the fingerprint for the website because they can not change their fingerprints [9]. Another issue is user privacy because the biomarkers for a user are unique. When a user registers at a website with a biometric it allows other parties to track the user across domains. An example is if a user registers at the website "A" and the website "B," then the website "A" could sell information about the user to website "B" because the user biometrics are unique.

There have been two recent studies in the field of WebAuthn and passwordless login. The first study, by Lyastani et al., involved ordinary users and was a lab study [12]. The users were given hardware tokens and completed tasks, which included registering and logging into websites provided by the researchers. After completing the tasks, users completed surveys to

measure their opinions about FIDO2 hardware tokens as a password replacement. According to the survey, one of the advantages of passwordless authentication is that users no longer have to remember passwords. On the flip side, users now have to carry around a hardware token, and 39% of participants disliked the need to carry an additional item. Users also worried about losing access to their accounts if the hardware token was lost or destroyed. There were other concerns with the use of hardware tokens, such as new devices that lack USB ports, accessing an account on a public device, allowing relatives to login to their account, and revocation. The second study conducted by Farke et al. tested the use of hardware tokens with 8 employees at a small company [7]. The employees were encouraged to use the hardware tokens but could use any form of authentication they wished. The researchers recorded each login, the authentication used, and how long each authentication process took. Also, periodically throughout the four weeks, the study interviewed employees about their experiences with the different forms of authentication they use. A repeated remark from the users was that a password manager auto-fills the username and password, making the authentication process quick. A common concern was that moving to this new authentication method took more time than many users were willing to invest. In summary, the users preferred password managers because it is quick and already set up. The study emphasized and noted that the four week period was not sufficient enough time to overcome the user's accustomed form of authentication, the password.

Chapter 3

User Study Design

I conducted a user study that focused on how users perceive and react to using roaming software tokens (smartphones) for passwordless authentication. Although the two studies previously mentioned got promising results, there were a variety of issues raised that correlated directly to hardware tokens. These issues include but are not limited to having to carry an extra item, lack of USB ports, fear of compromised accounts if the hardware token is lost, and loss of access if the hardware token is damaged. I carried out a user study following the steps by Lyastani et al. but used software tokens in place of hardware tokens. By using similar methods, I was be able to contrast the results of my study with theirs to compare the usability of hardware and software tokens.

One of the key issues users had with hardware tokens is the need to carry around an additional item and the worry of losing it. With many users already carrying smartphones with them, I believed that software tokens would address most of the issues users have with hardware tokens. Thus I had the following hypotheses:

- **H1:** Users will consider software tokens to be more usable than hardware tokens for authentication.
- **H2:** Users will prefer using software tokens and FIDO2 over traditional text-based authentication.

The communication options between a browser and a mobile device are limited. The Chrome browser currently supports USB HID and platform-specific means of authentication. I decided not to use USB HID because only the newest phones have this technology, which I

didn't have easy access to. Google is currently working on Cloud Assisted BLE (caBLE), but as of now, it is unavailable. To circumvent this limitation, I used Krypton, which allowed the use of software tokens. Krypton is a phone app and browser extension that turns a smartphone into a software token. Krypton accomplishes this by facilitating secure communication between the browser and the mobile device.

Krypton achieves secure communication by having software on both devices, the browser, and the phone. The communication between the two devices acts as CTAP, which allows the phone to be an authenticator. To pair the phone with the browser, Krypton uses a QR code to set up encryption keys between the devices. After the browser and the mobile device pair, the browser and the mobile device register with Amazon's Simple Notification Service (SNS) and Simple Queue Service (SQS). With the registration at the Amazon services and the public-private keys shared via the QR code, Krypton now has a secure and encrypted channel to act as CTAP and treat the phone as an authenticator.

I recruited students from campus so that I have a similar demographic to the original study, which allowed me to compare my results with the previous paper. I was able to recruit 30 participants.

By following the same methodology as Lyastani et al. and recruiting from a similar population, college students, I was able to do a between-subjects user study by using the data the Lyastani et al. has already gathered. I was able to compare the usability of software tokens to hardware tokens by determining if the same issues and results Lyastani et al. found manifested themselves with software tokens.

Once I had recruited the participants, I followed the same procedure as outlined by Lyastani et al., which included the following seven steps.

1. Welcome message

2. Topic introduction. Users watched a short video introducing authentication security and familiarized the participants with common threats and the abuse of leaked account credentials. The video explained these topics from the view of "Alice," an average but

fictional user.

3. (Steps 3-5 just for FIDO2 Users.)

   Introduction to FIDO2. The participants watched another short video introducing software tokens and the pros and cons of using them for 1FA. It is paramount to explain new technology because research has shown that users will rate new systems poorly if they do not understand them. This video also explained the technology from the view of "Alice." All videos we created were modeled after the videos in Lyastani et al.

4. Attention-based question (To make sure participants paid attention)

5. Setup Video (1FA) Step by step about registration and authentication process.

6. Hands-on task. Users registered and logged in to mockup websites Fakebook and Schmoogle. In order to register users had to first install Krypton and pair the phone with the browser by scanning a QR code. This established a secure communication between the browser and the phone. When registering and logging in users clicked a button on the website and then approved on the phone.

7. Surveys - that measure the following

   (a) Usability – system usability scale (SUS) [4]

   (b) Acceptance – A scale from Van Der Laan et al. [15]

   (c) Affinity for Technology Interaction (ATI) [8]

   (d) Privacy concern (PC) [10]

   (e) Demographics

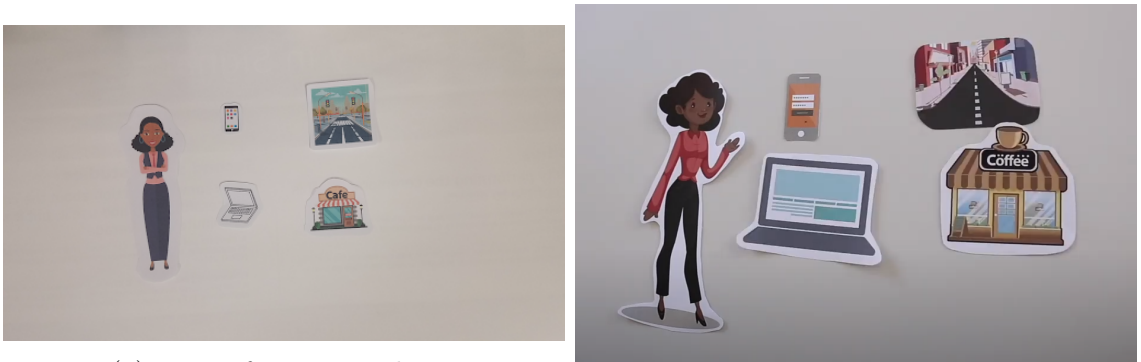
   (f) Qualitative questions

Chapter 4

User Study Preparation

4.1 Videos

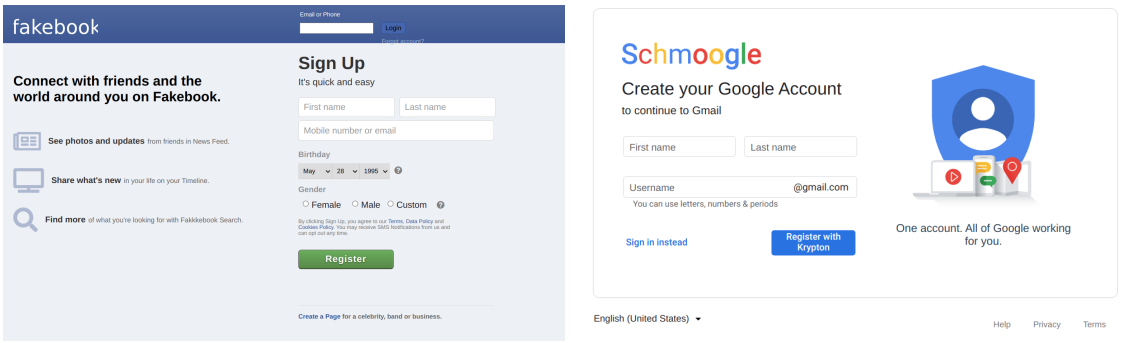
Lyastani et al. used three different videos in her study, all from the perspective of "Alice." The first explains the importance of choosing strong passwords, the second introduces FIDO2 hardware tokens, and the third shows how to setup a FIDO2 hardware token. Because the second and third videos in their study are specific to hardware tokens, we could not reuse them but had to make our own. We decided to redo all three videos, so that we could have continuity between them. To make the difference between the two studies as small as possible, we created new videos in the same style as the originals. Figure 4.2 shows the similarities. To further increase the likeness between the two works, we used the same scripts from Lyastani et al., with modifications to specify phones, software tokens, and Krypton in place of hardware tokens. We include our scripts in Appendix B, with bold, underlined text showing changes



(a) Image from our video 1

(b) Image from Lyastani et al. video 1

Figure 4.1: Comparison of videos



(a) Fakebook registration and login page (b) Schmoogle registration page

Figure 4.2: Screenshots of the mock websites

we made.

4.2 Mock Websites

In Lyastani et al., they used mock websites called Fakebook and Schmoogle that mimic the look of Facebook and Gmail for logging in. We likewise made similar mock websites. First, we wrote a simple application server using Golang that allowed for registration and logins with FIDO2. Then, we then created the mock websites Fakebook and Schmoogle. We already had a Fakebook website for another project, so we modified it to use FIDO2 instead of text-based passwords. This required (a) removing passwords fields in the UI, (b) switching the communication with the server to use WebAuthn, and (c) adding the javascript calls to use CTAP. Without access to an already built Schmoogle website, we had to create one from scratch. We built the Schmoogle website with FIDO2 allowing for passwordless authentication.

Chapter 5

Study Results

The user study started Wednesday, June 3rd, 2021, and ran until Wednesday, June 30th, 2021. A total of 30 participants completed the survey. User participants took between 25-35 minutes and received 12 USD as compensation. Brigham Young University Institutional Review Board approved this user study.

5.1 Demographics

We recruited from BYU's campus by posting fliers on bulletin boards located in campus buildings. The targeted audience was college students, so we created the fliers with BYU students in mind.

We had 30 participants, with 17 male, 12 female, and one non-binary or other. The participants were from the ages of 18-32, the average age being 23 years old. All of the participants were current BYU students.

5.2 SUS

We used SUS to measure the perceived usability of roaming software tokens. SUS uses 10 questions with 5 possible answers for each question, ranging from strongly disagree to strongly agree. Each question is worth 10 points with a total score of 100. A score of 68 is considered average. Figure **??** shows a boxplot of the results. The average SUS given to Krypton by participants in our study was 81.67: the high was 97.5, the low 42.5, and a standard deviation(SD) of 11.61. A score of 80.3 is considered an "A," so on average the use

of roaming software tokens for 1FA was well received.

From Lyastani et al., passwords received a score of 71.92 with a standard deviation of 11.09. That means our average of 81.67 was significantly higher than normal passwords; $t(76) = 3.70, p < .001$, Cohen's $d = .86$ These results support the findings Lyastani et al. that FIDO2 as a password replacement is more usable than passwords. When we compare hardware tokens to roaming software tokens, the results show little difference. Hardware tokens received a SUS score of 81.79, while software tokens received a score of 81.67. The minimal difference in scores shows that hardware tokens and roaming software tokens have similar usability; $t(74) = 0.04, p > 0.05$, Cohen's $d = 0.01$ These results show that there is no significant difference in the usability of hardware tokens, which means we reject **H1.**

One user gave software tokens a SUS of 42.5 which is significantly lower than the rest of the users. The second lowest score was 67.5 which is 25 points higher. In the open response portion of the survey the user explained their dislike for Krypton. They thought that using a phone as an authenticator was overly complicated. In addition they found that having to switch back and forth between a computer and browser to be tiresome. They also mentioned that in order to log in you need to have your phone on you constantly which is not a reality for them.

One user gave software tokens a SUS of 42.5, which is significantly lower than the scores given by the rest of the participants. The second-lowest score was 67.5, which is 25 points higher. In the open response portion of the survey, the user explained their dislike for Krypton. They thought that using a phone as an authenticator was overly complicated. In addition, they found that having to switch back and forth between a computer and a browser to be tiresome. They also mentioned that to access an account requires you to have your phone on you, which is not always possible for them. The user seemed to be wholeheartedly against using a phone for authentication.

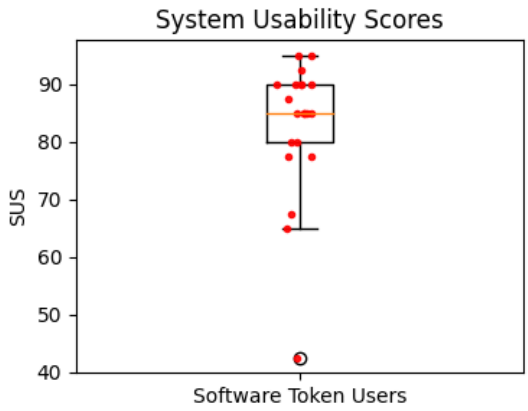


Figure 5.1: System Usability Scores from participants

5.3 Acceptance

Acceptance consists of 9 questions with 5 options. Each question receives a score between 1 and 5, with higher scores considered better. Using an unpaired two-sample t-test shows significant higher score with roaming software tokens than with passwords; $t(76) = 4.4, p < .001$, Cohen's $d = 1.02$ The t-test confirms **H2** which shows us that users accept roaming software tokens more than traditional passwords. When compared against roaming hardware tokens there was no significant difference between the two; $t(74) = 0.8, p > .05$, Cohen's $d = 0.0.19$ The t-test for hardware and software tokens shows us that software tokens have similar acceptance to hardware tokens.

5.4 Predicting Acceptance

We used ATI, PC, and SUS to determine if any of this helps predict whether a user is likely to accept Krypton as a password replacement. ATI consists of 9 questions with 6 possible options. Each question receives a score from 1-6. Privacy Concern (PC) has 4 questions with 7 possible questions. These surveys don't grade Krypton directly but allow us to see if a correlation between users accepting Krypton and their PC, ATI, and SUS results exist.

We performed simple Linear Regression using ATI, PC, and SUS as predictors for the acceptance of Krypton and FIDO as a password replacement. We created three linear models

	Acceptance			
Predictors	b	CI	R^2	p
Sus	0.176	[0.122, 0.229]	0.616	< 0.001
ATI	-1.000	[-2.099, 0.099]	0.110	0.074
PC	-0.237	[-1.420, 0.945]	0.006	0.685

Table 5.1: Results of linear regression models to predict acceptance

with one predictor for each model. Table **??** shows the results. The ATI and PC models both performed poorly with R^2 of 0.110 and 0.006 respectively. The SUS model did considerably better with a R^2 of 0.616 The models show us that of the surveys we used SUS is the best indicator of whether users will accept FIDO2 software tokens as a password replacement. We gave a linear model ATI, PC, and SUS as predictors and got an R^2 of 0.685. The difference from just using SUS to using all three survey results as predictors is minimal. The minimal difference further shows that SUS is the best indicator of acceptance. The combination of the three is slightly more than SUS by itself but not by a substantial amount.

These results are very similar to the results from Lyastani et al. In both studies SUS was the biggest predictor of whether a user would or would not accept FIDO2 as a password replacement. The model in Lyastani et al. that uses SUS as predictor had an R^2 of 0.428; this is almost 0.2 lower than the score we got. This difference may seem drastic but it really has little meaning as the two models should not be directly compared. The models in Lyastani et al. used robust regression based on MM estimators and used an adjusted-R^2. Our models were OLS regression and the R^2's were not adjusted. What we can see is that in both studies SUS was the best predictor for users acceptance of FIDO2. Additionally, in both studies ATI and PC did little to predict whether a user would or would not accept FIDO2 as a password replacement.

5.5 Qualitative Results

Looking at free-response questions helped us understand more of the pros and cons the users felt about roaming software tokens. We used standard qualitative content analysis to code

the data, with two researchers coding each question independently. The researchers then compared codes and resolved any disagreements. These codes were then combined to into more general themes, with the results presented below.

5.5.1 Phone Usage

Many users worried about losing access to their accounts if they couldn't use their phones for some reason. 21 out of 30 (70%) users mentioned this worry in some form, this is 31% higher than the user's concerns concerning hardware tokens. Most of the users weren't concerned about carrying around an extra device, but more so if they forgot their phone somewhere or the phone's battery was drained. Participant 23 said, "The only disadvantage I can think of is is one's phone were to die or if they were to change phones." The use of smartphones seems to heighten user's worry of the device becomes unusable or lost.

5.5.2 Krypton for 1FA

The use of Krypton to facilitate 1FA was well-received 24 out of 30 participants mentioned that it was easy, simple, or straightforward to use. Of the remaining 6 participants, they mentioned that it was "ordinary" and "overly complicated" or were neutral in their opinion. A drawback mentioned by a handful of users was having to click the cancel button. Having to click the cancel button is a disadvantage of using a chrome extension to facilitate the communication between the phone and the browser and could not be avoided. We could have avoided this problem if there was a built-in method of communication between smartphones and the browser. A few participants mentioned that it was annoying that the authentication only works with computers previously paired with your device. This restriction makes it harder to login into accounts while not at home or using their laptop. One user also mentioned the use of account sharing, specifically that it limits access to your account to that one phone which can be frustrating.

5.5.3 Switching to Krypton across accounts

Many users mentioned that they would be willing to use Krypton, but only for low-risk accounts that they regularly use, e.g., social media accounts. The main reason given was in case their phone was lost, stolen, or broken. Participant 26 said, " I would [use Krypton], but only for less important accounts. I still feel like independence from my phone is desirable when I am trying to get into more important accounts." The common thread was that users were willing to use their smartphones to authenticate accounts where their loss was not detrimental. For high-risk accounts, such as banking and email, users mentioned they would prefer to stick with passwords so that if the authenticator was broken, stolen, or dead, they could still access their account. A few of the users mentioned that if they did switch to Krypton, they would use it everywhere, the all or none mindset. For the users who were on the edge if they would use Krypton or not, it was dependent on whether there was a viable means of recovering their account.

5.5.4 Mobile trust

Users were confident or content with the perceived security of the app. Participant 13 did say, "The only disadvantage I see is if there are apps on the phone that can take information." This user has a legitimate worry about malware and its ability to compromise the security of authentication. The participant didn't distrust the Krypton app but more so using their phone to authenticate. Participant 17 mentioned distrust of the Krypton Chrome extension, stating that a QR doesn't seem secure if someone only needs to scan a QR code on your computer to register their device. This comment indicates a lack of understanding of Krypton's communication and authentication model.

5.6 Discussion

5.6.1 Software replace hardware?

From the study, we found out that users thought that the usability of hardware and roaming software tokens are comparable. User's complaints seemed to switch from having to carry an extra device to their phone being uncharged, in a different room, or forgotten at home. In Lyastani et al., users feared thieves could access their accounts if they stole their hardware tokens. In this study, users did not raise that issue. This issue was probably not raised by users because many users use pins or biometric authentication to lock their phones. The complaints from this study are all associated with the loss of access to their account(s). Loss of access to accounts has been a common finding in most papers, including the work done by Lyastani et al. The FIDO alliance currently recommends that users register multiple authenticators because the "The loss or breakage of a single FIDO authenticator is minimally impactful to the user when an additional authenticator is readily available" [2].

Account recovery is a complex topic, one possible remedy to this problem is to follow the advice of FIDO and have users register with their mobile device and a hardware token. The hardware token would address the issues when the smartphone becomes unusable because of a dead battery, was broken or lost. One possible problem is if the user carries their hardware token with them, e.g., on their keyring. If someone loses their phone, e.g., left their bag containing their phone somewhere, there is a good chance that their keys are also in the lost bag. This situation would essentially defeat the purpose of having the second authenticator. If the user kept the hardware token at home, it would also cause issues. If they are away from home and their phone died, they wouldn't have access to their accounts. The next logical step would be to have their mobile device and two different hardware tokens, one for the keyring and one at home, as a backup. The 2 backup hardware tokens would defeat the purpose of using a mobile as an authenticator because the user would still have to carry around an additional item. Additional research is needed to solve this problem so that

hardware tokens or software tokens can be a viable password replacement.

5.7 Establishing Trust

As mentioned in section 5.5.4 one user distrusted the use of QR codes as part of pairing the phone with the browser. The distrust of the QR code pairing shows a common problem with new authentication methods. User's misunderstanding of technology causes distrust of the new technology. The QR pairing that Krypton requires is to allow communication between the browser and the phone. The QR code is not part of the authentication process, which means that the QR code can't be the "weak link" attackers use to attack Krypton and the mobile phone. This problem of users misunderstanding new technology is hard to overcome because many users are not interested in learning about the technology or don't pay attention to the explanation.

Chapter 6

Conclusion

This study further cemented the work done by Lyastani et al. that users accept FIDO2 as a usable password replacement. The user's acceptance of FIDO2 is reflected in the confirmation of **H2.** The hope in this study was to address the issues raised by users in Lyastani et al., primarily carrying around an additional item. When we introduced smartphones, they didn't remove issues but instead replaced them with new problems. We replaced the annoyance of carrying an additional item with the fear of temporarily losing access to accounts. When users authenticated with smartphones, they gave strong SUS and Acceptance scores, this further showing that FIDO2 as a password replacement is possible. The biggest hurdle we perceive is users worry about loss of access to their accounts. If we could address this hindrance, it would drastically improve the chances of FIDO2 getting accepted as a password replacement.

References

[1] Akamai. Credential stuffing in the media industry. *State of the Internet Report / Security 6* (2020).

[2] Alliance, F. Recommended account recovery practices for FIDO relying parties, Febuary 2019.

[3] Biddle, R., Chiasson, S., and Van Oorschot, P. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys 44*, 4 (Sept. 2012).

[4] Brooke, J. SUS: a quick and dirty usability. *Usability evaluation in industry* (1996).

[5] Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. The tangled web of password reuse. In *NDSS Symposium* (2014).

[6] Dey, A., and Weis, S. PseudoID: Enhancing privacy in federated login. In *Hot Topics in Privacy Enhancing Technologies* (2010), pp. 95–107.

[7] Farke, F. M., Lorenz, L., Schnitzler, T., Markert, P., and Dürmuth, M. "You still use the password after all" – exploring FIDO2 security keys in a small company. In *Usable Privacy and Security (SOUPS)* (Aug. 2020), USENIX Association, pp. 19–35.

[8] Franke, T., Attig, C., and Wessel, D. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction 35*, 6 (2019), 456–467.

[9] Kim, H.-J. Biometrics, is it a viable proposition for identity authentication and access control? *Computers & Security 14*, 3 (1995), 205–214.

[10] Langer, M., König, C. J., and Fitili, A. 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 81* (2018), 19–30.

[11] Lyastani, S. G., Schilling, M., Fahl, S., Backes, M., and Bugiel, S. Better managed than memorized? studying the impact of managers on password strength and reuse. In *USENIX Security Symposium* (2018), USENIX Association, pp. 203–220.

[12] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., and Bugiel, S. Is FIDO2 the kingslayer of user authentication? a comparative usability study of FIDO2 passwordless authentication. In *IEEE Symposium on Security and Privacy (SP)* (2020), IEEE, pp. 268–285.

[13] Pearman, S., Zhang, S. A., Bauer, L., Christin, N., and Cranor, L. F. Why people (don't) use password managers effectively. In *USENIX Conference on Usable Privacy and Security* (2019), pp. 319–338.

[14] Ruoti, S., Roberts, B., and Seamons, K. Authentication melee: A usability analysis of seven web authentication systems. In *International Conference on World Wide Web* (2015), pp. 916–926.

[15] Van Der Laan, J. D., Heino, A., and De Waard, D. A simple procedure for the assessment of acceptance of advanced transport telematics. *Transportation Research Part C: Emerging Technologies 5*, 1 (1997), 1–10.

[16] Wash, R., Rader, E., Berman, R., and Wellmer, Z. Understanding password choices: How frequently entered passwords are re-used across websites. In *Usable Privacy and Security (SOUPS)* (June 2016), USENIX Association, pp. 175–188.

Appendix A

Surveys

A.1 System Usability Scale (SUS)

Please state your level of agreement or disagreement for the following statements based on your experience with Krypton. 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.

A.2 Acceptance

Please judge using Krypton to login to websites using the following adjectives.

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

A.3 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.

A.4 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.

A.5 Technical Problems

Were there any technical problems while watching the video and trying out Krypton?

- No problems
- Few problems
- Some problems
- Many problems

A.6 Further Qeustions

How do you choose your password for a new email account?

- Reuse an existing password
- Modify an existing password
- Create an entirely new password
- No answer
- Other

Has ever one of your passwords been leaked or been stolen?

- Yes
- No

A.7 Demographics

Please indicate your gender.

- Male
- Female
- Other
- No answer

Please indicate your highest educational degree.

- High school graduate
- Bachelor's degree
- Master's degree
- Diploma
- Ph.D
- Other

How old(in years) are you?

Please indicate if you have a computer science background.

- Yes
- No

Please indicate your area of studies/area of work.

A.8 Open-ended Questions

1. How would you describe your general experience with Krypton?
2. Which advantages do you see in the usage of Krypton?
3. Which disadvantages do you see in the usage of Krypton?
4. Would you use Krypton yourself?
5. If you would, why and on which accounts would you use it? If you wouldn't, why not?

Appendix B

Scripts

B.1 Video 1

This is Alice. Alice has various online accounts for her social networking, emails, file storage and so on. Alice needs a password for every single account. Everyone uses passwords because they are supported on all websites, are easy to use and a cheap way to secure accounts because you do not have to pay extra to use them. It is very practical that Alice uses her passwords everywhere, for example on her own smartphone, while being on the street on her laptop, while sitting in a Cafe, or even on a public computer in a library. One day Alice is watching the news and sees that the service Schmoogle she is using has been attacked. Many customers' data including passwords has been stolen. Alice doesn't know if her account has been compromised, but Schmoogle recommends that all of its users change their passwords. Alice has to change all of her passwords, even on different unrelated sites because she reuses the Schmoogle password for other accounts. Alice knows that simple passwords, which are easy to remember, can be guessed very easily by the thief. To make her passwords safer Alice now tries to find a long and complex password, which is unfortunately hard to remember. Alice is happy because she creates unique and strong passwords for all of her accounts and feels safe again. The next day Alice installs a new program on her computer. She doesn't know that this program is actually a computer virus that monitors her input to the computer for passwords and leaks it to a cyber criminal. Although Alice has changed her password to a complex and long word to avoid it being guessed, it doesn't help her in this situation, since the virus steals her password directly on her computer when she logs into the Schmoogle website. Alice notices that her password was stolen because something happened on her account. Alice directly goes to an expert who can delete the program and the virus from her computer. She now knows that she has to choose safe passwords and be careful with programs she installs on her computer. Alice is happy because her computer is safe again and nothing important from her data got stolen.

B.2 Video 2

Alice thinks about other ways that she could secure her accounts. A friend recommends that she try passwordless authentication, which is also supported by her Schmoogle email service. But what exactly is passwordless authentication? When using passwordless authentication, you can use a **phone** instead of a password to log in. One possibility is an app called **Krypton, which uses your phone to securely store secret information for logging into accounts.** With **Krypton** no passwords are needed when logging into an account. You just tap the **phone** to verify you want to login to your account. **Krypton** can be used for different accounts. This sounds great to Alice because she has had bad experiences with passwords in the past. She decides to try out passwordless authentication for Schmoogle and downloads **Krypton for free.** When Alice uses **Krypton** instead of a password, the server just stores public information from the **App** that Schmoogle needs to verify Alice's **phone has the correct secret information.** That means that no secret information from **Krypton** can be stolen that allows the thief to gain access to Alice's Schmoogle account or any other account where Alice is using **Krypton. Krypton** stores any secret information securely on the **phone** separate from the computer where the login is **taking place.** Thus Alice can use **Krypton** without a virus or malicious software being able to steal her information.

B.3 Video 3

Alice wants to see how this setup works. Okay, let's see how Alice can set up and use passwordless authentication for her Schmoogle account. **Alice adds the krypton extension to her browser and downloads the Krypton app onto her phone from the google play store. Alice opens Krypton on her phone and Chrome on her laptop and scans the QR code with the app on her phone. Her phone is now paired with her browser.** She goes to the Schmoogle website and creates a new account. As usual, she enters her first name and her last name. Of course she also has to choose a username. The Schmoogle website explains to her that Schmoogle supports passwordless authentication with an **App**, and Alice does not have to set a password for registration or login when she creates her new account. The Schmoogle website instructs her to now use her **App.** Alice's **phone** is already connected to her computer and **a notification pops up** which allows Alice to log in by pressing a button. Now Alice has successfully registered her new Schmoogle account using her **phone** instead of a password. To login into her Schmoogle account she simply has to enter her username and when instructed by the website use her **phone** to authenticate. She has now successfully logged into her Schmoogle account Alice also wants to use passwordless authentication for a new Fakebook social network account. Like Schmoogle,

Fakebook supports passwordless authentication with a **phone.** Alice enters her first and last name as well as her email to register a new Fakebook account. When registering Alice is again instructed to use her **phone** by pressing the **Notification on the phone.** After successfully registering Alice can log into her Fakebook account by just entering her email address and then using her **phone.** To successfully log in she simply has to press the **notification on her phone.** If she would use a different **phone** than her own **phone** she could not login successfully. Since she is using her own **phone** she can access her Fakebook account and now start making new friends or following her existing friends. Now it's your turn to try out how passwordless authentication works

Appendix C

Themes from Qualitative Responses

Topic and Themes	
A.	Usability of Krypton
	A.1 Easy to use
	A.2 Fast
	A.3 Complicated
B.	Advantages of Krypton
	B.1 No need to remember password
	B.2 More secure
	B.3 Already carry phone
C.	Disadvantages of Krypton
	C.1 Lose account access with phone issues
	C.1.A Dead battery
	C.1.B Broken phone
	C.1.C Misplaced phone
	C.1.D New phone
	C.2 Always have to have your phone on you
	C.3 Doesn't work with non-paired computers
	C.4 Hard to share account access with family members
D.	Would you use Krypton?
	D.1 Yes
	D.2 No
	D.3 Maybe
	D.3.A If everyone uses
	D.3.B If account recovery was resolved
E.	What accounts would you use Krypton with?
	E.1 All
	E.2 Everywhere except email
	E.3 Non important/social media
	E.4 Would not use