Vision: I don't want to use my Phone! A Cognitive Walkthrough for YubiKeys

Claudia Bischoff
University of Bonn
Bonn, Germany
claudia.bischoff@uni-bonn.de

Eva Gerlitz
Fraunhofer FKIE
Bonn, Germany
gerlitz@cs.uni-bonn.de

Matthew Smith
University of Bonn, Fraunhofer FKIE
Bonn, Germany
smith@cs.uni-bonn.de

***Abstract*—Security keys can be used as a second factor when users aim at securing their online accounts or devices in addition to passwords. In this vision paper, we made the first step to identify common issues when registering a YubiKey as second factor on Google, Facebook, Windows 10 and Ubuntu 18.04.4 accounts by a cognitive walkthrough. We found the websites to be too phone-centered and the instructions for operating systems too complex and incomplete at the same time. We therefore plan to analyze further websites to identify the most usable implementation for each step of the registration process, in order to combine those into an improved overall solution.**

***Index Terms*—two-factor authentication, security key, YubiKey, cognitive walkthrough**

1. Introduction

A digital life without passwords is hard to imagine. However, many end users show an insecure password hygiene such as reusing their passwords or using commonly used passwords and thus make it easy for attackers to get access to their accounts [1], [2]. A secure solution is offered by using a combination of a password (*something you know*) and a different authentication method, for example biometric authentication (*something you are*) or authentication using a token or trusted device (*something you have*), known as two-factor authentication (2FA). An example for the latter one are YubiKeys, security tokens by the company Yubico. The tokens come in different sizes, resembling flash drives. The core of the registration process is as simple as plugging the key in the USB port and touching the button of the key. While according to Yubicos' website, "it only takes a few seconds to register a YubiKey with your personal accounts and favorite digital services" [3], this task is embedded into finding the appropriate place in each accounts' settings. Commonly, at login, the user will need to first enter their password, then plug in the key and touch its button when prompted.

Previous work which tested the usability of YubiKeys with end users found a number of issues when registering a key as second factor on different services [4]–[6].

We were thus interested in the differences of the setup process for different services and operating systems to answer the following questions:

- What are current issues when registering a key?
- Do all services show issues at the same stage of the process?
- Can different GUIs or approaches be combined to build a usable and more intuitive approach?
- Will this improved usability lead to a higher usage rate or are further steps necessary?

As in the nature of a vision paper, we present work that is still in progress.

The rest of the paper is structured as follows: First we outline literature that is related to our work. This is followed by our methodology and our preliminary results for two websites and two operating systems. We conclude by discussing our results and giving an outlook to upcoming work.

2. Related Work

In the following section, we discuss previous work concerning end users' usage as well as the usability of 2FA in general and YubiKeys in particular.

2.1. Overviews about different means of 2FA

Krol et al. [9] compared different second factors used for UK bank accounts (secure key, card reader, SMS, app, phone call). They interviewed 21 UK online banking customers and asked them to keep an authentication diary for 10 – 12 days. They found that users are dissatisfied with carrying around extra devices, but also that user satisfaction is lower when more information is needed for authentication tasks. Users themselves proposed biometric forms of authentication in order to ensure the high level of security needed for banking purposes.

Reese et al. [6] compared five methods of 2FA (SMS, TOTP app, pre-generated codes, push notifications and YubiKeys) in a two-week online study combined with introductory and exit interviews. The 72 participants completed online banking tasks every day, signing into the researchers simulated banking website with their assigned second factor. In this study, YubiKeys turned out to have the shortest median authentication time, but a lower SUS score ([8]) than other methods. Users' willingness to use a second factor for authentication for their real accounts depended on the value of the specific account. In particular, it was desired for financial accounts and opinions were mixed for email accounts, while for social media accounts, less protection was aimed for. In a separate lab study focusing on the setup process of the same 2FA methods, it was found that some users had problems setting up the

YubiKey. However, all five methods received a Single Ease Question (SEQ) score that was rather on the "easy" than on the "difficult" side.

Acemyan et al. [10] compared the 2FA methods offered for Google accounts (SMS, app, YubiKey, push notifications) in a lab study with 20 participants. They found that the setup process was neither very effective, nor obtained a satisfactory SUS score. Yet Login achieved a satisfactory SUS score. The differences between methods were not significant except in the case of satisfaction with the login process.

Ciolino et al. [11] compared three security keys (by different manufacturers) with SMS-based OTPs in a lab study with 15 participants. The participants used each of the four 2FA methods for one out of two web accounts, being asked to first set up the account for use with the method, then log in to the account and finally complete an SUS questionnaire. The resulting SUS scores were "acceptable" for all methods except one security key, measuring setup and login phase together. However, several major usability issues of the setup process were reported.

Ciolino et al. [11] also performed a diary study, during which 15 participants were using the SecureClick security key (which obtained only a "marginal" SUS score in their previous study) for some of their accounts (which are compatible with the Universal 2nd Factor standard) for one week. The security key now received an "acceptable" SUS score. They also found that the combination of password and security key was required in only 28% of the 643 overall login events. A huge drop in security key usage throughout the week resulted from authentication fatigue, "remember me" options and SMS codes being sent even when security key authentication was desired.

2.2. Studies about YubiKeys

Das et al. [4] performed two lab studies about the setup process of YubiKeys. Participants had to set up their personal Google account for use with a FIDO U2F Security key by Yubico. The stopping points of participants in the process were collected, i.e. when a participant came to a complete stop or believed they had completed their task while they actually had not. As such, stopping points involved a demo which was confused with the actual setup and the inability to verify success by logging in with the key, due to a default "remember me" option. After the first study with 21 participants, the results were forwarded to the manufacturer Yubico, and the study was repeated with 35 participants one year later, when some of the obstacles had been addressed. The second study revealed an improved usability, but no improvement in the acceptability of the process. The acceptability was mostly determined by risk awareness, knowledge of potential benefits and cognition about the importance of passwords.

Reynolds et al. [5] performed a lab study with 31 participants for the setup process of the YubiKey 4 on Google, Facebook and Windows 10 accounts. They found that the setup process has a "non-acceptable" SUS score (measured with a joint SUS questionnaire for all three account types). Many participants failed to correctly set YubiKey authentication up for the Facebook and Windows accounts, indicating that documentation needs to be updated and improved.

In order to also evaluate the day-to-day login experience, Reynolds et al. [5] performed a diary study with 25 participants, lasting four weeks. Participants used a YubiKey 4 NEO or Nano with their personal Facebook, Google and Windows accounts. In this second study, both YubiKey models attained an "acceptable" SUS score for day-to-day use. However, most users encountered errors when authenticating at the Windows account. Some users had practical concerns such as the very small shape of the Nano key model, the need for additional keys in order to share accounts and the risk of losing the security key.

3. Methodology

The goal for this part of our study was to evaluate the usability and learnability of the setup process of a YubiKey for an end user. As we focused on non-tech-savvy users, we also focused on account types that such users were likely to have. Thus, applications such as password managers or developer tools, which rather widely support YubiKeys, were not of our interest. Instead, one research assistant in usable security and privacy performed cognitive walkthroughs (CW) for a Google account and a Facebook account. Additionally, we wanted to evaluate accounts on common operating systems, choosing Windows 10, Ubuntu 18.04.4 and MacOS Catalina.

According to the current information by Yubico [12], [13], in MacOS Catalina the YubiKey cannot be required for login (using HMAC-SHA1 challenge-response) but can only be used as a Smart Card, which allows to log in using either the users' password or the YubiKey. Since the latter is not the technology of our interest, we decided not to test it.

For the cognitive walkthroughs, we followed the methodology of Wharton et al. [14]. We first defined who the users are, by making explicit assumptions about their situation and previous knowledge:

- The user has had their respective account for a longer time, but now decides to add a security key for the first time.
- The user is familiar with the sign-in process using a password, but has not been using 2FA before.
- They have seen the settings page of the respective account before, but haven't explored or used it a lot.
- This is the first account which they set up for use with the YubiKey.
- The user is working on a laptop or desktop computer with Windows 10 as operating system. (In particular, Google and Facebook accounts are not being accessed on a smartphone, as this would require additional considerations, such as the type of key used etc. This is in fact a restricting assumption.)
- The user is aware that using the YubiKey requires a change in the settings of the respective account (as opposed to browser settings or other places) and that they need to log into their account in order to access and change these settings. Furthermore, they associate the YubiKey with terms like *Login*, *Security* and *Two-factor authentication*.

Next we defined the task, namely setting up a given YubiKey as a second authentication factor for the respective account. The sequence of actions needed to accomplish

this task differs for each account type and is given in the beginning of the Results section for each account.

For each step listed in the necessary actions, we asked the following four questions:

1) Will the user try to achieve the right effect?
2) Will the user notice that the correct action is available?
3) Will the user associate the correct action with the effect they want to achieve?
4) If the correct action is performed, will the user see that progress is being made toward solution of their task?

If possible, the researchers should then justify answering each question with "yes", producing a credible success story. Otherwise, a so-called failure story explains why a user may fail at this step.

It has to be noted that cognitive walkthroughs are centered at the GUI of a system, as they can also be carried out using merely a description of the interface instead of a working implementation.

Google and Facebook offer wizards for setting up the YubiKey as a second authentication factor and could thus be tested with strict cognitive walkthroughs.

In contrast, the process for Windows 10 and Ubuntu 18.04.4 involved downloading and installing some software, then using the tools in the correct order and, in the case of Ubuntu, didn't even have a GUI. Therefore, instead of sticking to the questions of the cognitive walkthrough, which are centered at the user interface, we instead followed the instructions given on the Yubico homepage (see [15] for Windows and [16] for Ubuntu) and tried to identify stopping points or lack of clarity.

For our tests, we were using a ThinkPad running Windows 10, Version 1909 and Ubuntu 18.04.4 LTS. We used the YubiKey models YubiKey 5 NFC and YubiKey 5 Nano.

4. Results

In this section we focus on the challenges and problems that we discovered, since these mark the points which call for improvement.

The section consists of three parts: First, the cognitive walkthroughs for online accounts, second, the operating system tests, and third, physical issues which are independent of the account type. For the cognitive walkthroughs, we give the list of steps necessary to accomplish the task, and the chronological failure stories associated to the steps, if present.

The first issue, which applies to all online accounts, is the need to use Chrome or Opera as a browser for the set up of YubiKeys. Indeed, this is mentioned in the instructions by Google [17] and Facebook [18]. However, not using Chrome or Opera will lead to failure without helpful feedback.

4.1. Google

4.1.1. Steps for the CW.

1) Open google.com
2) Sign into account
   - Click on "Sign in" in upper right corner
   - Choose account
   - Enter password and confirm
3) Open account settings
   - Click on account symbol in upper right corner
   - Select "Manage your Google Account"
4) Open security settings in Left-hand side menu
5) Scroll down to "Signing in at Google" and click on "2-Step Verification"
6) Select "Get started"
7) Enter password
8) Select "Choose another option"
9) Select "Security Key"
10) Find physical key, press "Next"
11) Plug key into USB port
12) Press button on the key
13) Enter a name for the key and click on "Done"

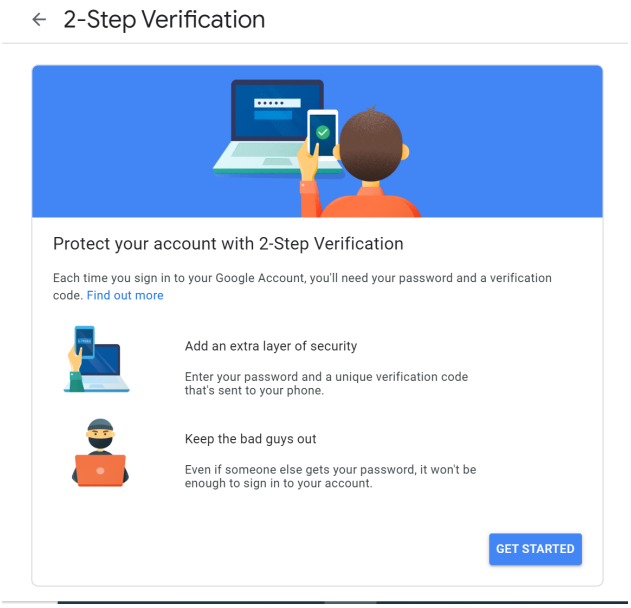

Figure 1. Screenshot of the introductory page for enabling 2FA in a Google account

4.1.2. Failure stories. We were able to identify several points during the setup process of a YubiKey for a Google account which might lead an end user to be confused or even interrupt the whole process.

First, we noticed a difference in the wording used by Google ("2-Step Verification") as opposed to, for example, the official website of Yubico ("Two-Factor authentication"). As we assume only basic knowledge, we imagine that some users might be confused by this.

Second, the intro page (Fig. 1) might be misleading by saying, "you'll need your password and a verification code". While this is technically correct for security keys, it is usually hidden to the user, who probably doesn't know the key generates codes.

Also, the page mentions "a unique verification code that's sent to your phone", which is another way of 2FA that our user doesn't want to use and which is also not necessary for the registration of a security key.

The "Choose another option" is hard to see, as the rest of the page (Fig. 2) is phone-centered. The item is

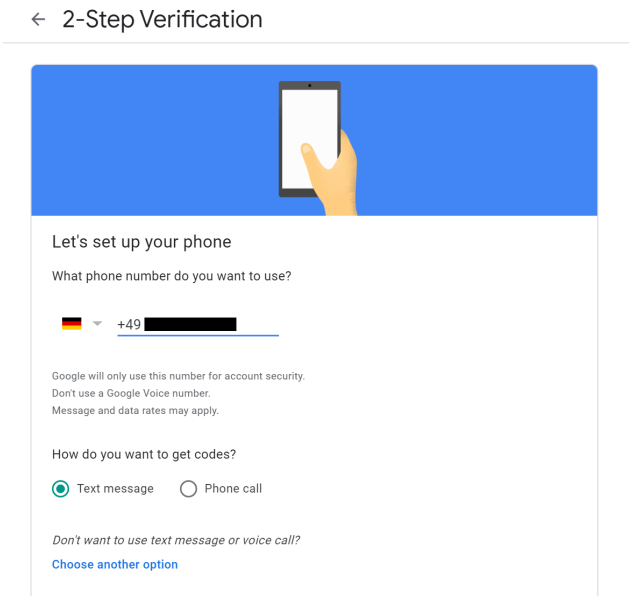

Figure 2. Screenshot of the first step for enabling 2FA in a Google account

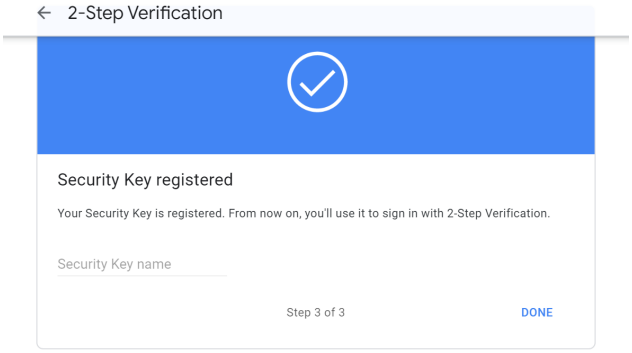

Figure 3. Screenshot of the success page after enabling 2FA in a Google account

kind of small, at the very bottom of the page and may thus be overlooked. Moreover, all other contents of the page are phone-related (e.g. heading "Let's set up your phone"), making the user believe they are on the wrong page overall. Finally, terms like "Security Key" are not used on this page.

After registering a key, the user is asked to enter a name for the key (Fig. 3). There is no explanation what the name is or what it will be used for and it is not obvious that text can be entered in the field. We assume that the user doesn't expect to be asked to enter a name for the key.

4.2. Facebook

4.2.1. Steps for the CW.

1) Open facebook.com
2) Sign into account
   - Enter Email
   - Enter Password
   - Click "Log In"
3) Open account settings
   - Click on "down arrow" in the top right corner to see menu
   - Select "Settings"
4) Select "Security and Login" in the left-hand side list
5) Scroll down to "Use two-factor authentication" and click on "Edit"
6) Setup any "Security method", for example an Authenticator App
   - Select "Authenticator App"
   - Re-enter password
   - Open App on Smartphone
   - Scan QR Code on the screen
   - Enter Code given in the App on Facebook page
   - Click "Done"
7) Select the option "Security Key", click on "Setup"
8) Plug Key into USB port
9) Tap button of the key
10) Confirm with "Ok"

4.2.2. Failure stories. When looking at Facebook, we only found one failure story for registering a YubiKey:

For Facebook, security keys can only be used as a "backup" means of 2FA. Hence another method (like an authenticator app) needs to be set up first. This is an effect the user doesn't want to achieve. Furthermore, the user needs to have access to a mobile phone (to receive SMS) or preferably a smartphone (to use an authenticator app).

4.3. Success stories for Google and Facebook

In the CWs for Google and Facebook, we found success stories for each of the steps which are not associated with one of the failure stories above. As the reasoning was similar for many of the steps, we summarise the positive answers to the questions of the CW, which we asked in 3. While answering them, we kept the assumptions about the user in mind (e.g. that the user is aware that using the YubiKey requires a change in the account settings.)

The user will try to achieve the right effect either because they are prompted to do so or because they know from general computer experience that simple steps such as clicking "Ok" or entering their password are required.

The user will notice the correct action, because they know from experience where common actions can be taken (e.g. accessing the account settings) or because they see well-visible UI elements like buttons (e.g. "Next") or explicit textual prompts. A reduced UI design oftentimes highlights where actions can be taken.

The user will associate the correct action with the effect they want to achieve due to meaningful labels such as "Log in", sometimes in combination with matching icons (e.g. of a security key in an overview of different 2FA methods).

If the correct action is performed, the user will see that progress is being made toward solution of their task because they see a new page which displays the next step (building on the previous one, which was thus successful). At the end of the registration processes, there is an explicit success page to highlight overall success.

4.4. Windows10

In order to register a YubiKey with Windows 10, users need to install the tool "Yubico Login for Windows", restart their computer and then run the tool "Login Configuration", which provides a wizard for the actual registration of the keys.

4.4.1. Failure Stories. The tool "Yubico Login for Windows" works only for local accounts. Thus, it would be necessary for the user to first switch from a Microsoft account to a local account. This step comes with its own perils, such as discontinuation of automatic backups. Instructions for this step need to be looked up in the Microsoft help and are not hyperlinked by Yubico.

A potentially unpleasant byproduct of the registration of a YubiKey is that for logging in, users will need to first enter their username (as opposed to just selecting it from a list), then their password (while the YubiKey is inserted in the USB port). Hence they need to know their usernames. Note that this applies to all users, even those who are not using a YubiKey for their accounts. However, this obstacle is mentioned sufficiently in the instructions.

The installation guide also mentions that "It is not necessary to press the button on the YubiKey to log in. In some instances, pressing the button actually causes the login to fail." This might be very confusing for users who use their YubiKey for multiple accounts and all but this one require the button to be touched.

After installing the tool "Yubico Login for Windows" and restarting the machine, users need to open a program called "Login Configuration" in order to register a YubiKey for their account. Each key has 2 slots in which challenge-response secrets can be stored. Slot 1 is pre-allocated with a secret, while slot 2 is empty on a new key. (If the key was already registered with other accounts, both slots may contain secrets.) In the setup process, the user can choose which slot to use and whether to use an existing secret or to generate a new secret. A new secret can be stored in the empty slot 2 or can overwrite an existing secret; the latter will break authentication at other accounts using the overwritten secret. Moreover, trying to use an existing secret can lead to the error message "Error programming device – Error in configure_yubikey_challenge_response_for_user: 0000004e". We do not know accurately which problem causes this error. Yet we can say that the message is not helpful in understanding the problem.

Beyond the actual setup process, a lot of other questions remain open or aren't thoroughly explained. For example, users can recover from loss of their key by entering the recovery code instead, but they can't recover from loss of their password (besides contacting an administrator) and it's also difficult for loss of username (other users of the computer who are able to log in can see all usernames). If an end user is the only administrator of the computer themselves, and they forgot their password, then they permanently locked themselves out of their account, to our knowledge. Hence the recovery from loss of the first authentication factor, the password, is hard, while for the second factor, the YubiKey, it is easy.

4.5. Ubuntu

The instructions guide the user through enabling the Yubico PPA, installing the tool "libpnam-u2f", associating a YubiKey (and optionally a backup key) with the account and finally configuring the system to require the YubiKey for login. Following through the instructions, everything seemed to work.

Yet the registration of one of our keys failed, but we only recognized this when we were not able to use it for authentication. There was no error message, and consequently we don't know what the actual reason for the failure was.

As the setup process is not intuitive and doesn't have a UI, we believe that it is not suited for average users. Lots of supplementary information is missing, for example how to deal with multiple user accounts or how to remove a key from an account. Only other keys can be used as a backup; there are no recovery codes or other second factors.

4.6. Physical issues

The YubiKey 5 NFC is flash drive-shaped and therefore easy to handle. In contrast, the YubiKey 5 Nano is very small, with only a tiny handle sticking out of the USB port when plugged in. This makes it hard to grip and pull it back out.

Furthermore, the handle is also the "button" of the key, i.e. it needs to be touched in order to confirm authentication. On the other hand, OTPs can also be generated while one touches the handle, actually trying to pull the key out. If a wizard is waiting for another input, this can cause unwanted behaviour. In the Windows 10 setup, we observed that the wizard was just cancelled when the Nano key was pulled out, leading to an incomplete registration of the keys and the inability to record the backup code that is automatically generated at the end of the registration process.

5. Discussion

5.1. Common issues

We were able to identify problems that occurred for both Google and Facebook or Windows and Ubuntu.

On the websites, it is noticeable that the focus lies on phone-based 2FA methods (SMS, app) in the wizards, while security keys are either hidden (Google) or only possible as second method of 2FA (Facebook) in addition to the phone. While currently the phone as a second factor is much more widespread than security keys [19], and websites might therefore prioritize it (e.g. for the sake of faster navigation), we think this should not lead to the invisibility of the other methods.

In the case of our tested operating systems, we found the setup process to be too complex to be mastered without instructions, not only due to the number of steps necessary to register a key, but also in regard to several obstacles which users need to be aware of in order to avoid losing access to their accounts. In the case of Windows 10, users need to enter their username in order to log in. While this

increases the security of the account, we recommend to leave the decision of whether or not to use this feature to the user. Additionally, the instructions for Ubuntu cover only the strictly necessary steps, which increases the risk of losing access to the account due to technical problems. Furthermore, more background information would be needed to master additional tasks.

5.2. Comparison to Related Work

We found that most of the issues with registering a YubiKey for Google accounts (reported in [4]) and Google, Facebook and Windows 10 accounts (reported in [5]) have been resolved by altered wizards, and entirely new tools in the case of Windows. However, some of the previously reported issues persist (such as Facebooks' requirement of using a phone-based 2FA method, and "remember me" options being enabled by default) and others have newly emerged.

We were primed by the related work about two physical issues: Inserting the key in the USB port upside down and not recognizing the button of the Nano key. However, we have not previously heard of issues due to the fact that the button of the Nano key needs to be touched in order to pull the key out. This caused a wizard to fail in our study.

6. Limitations

Cognitive walkthroughs are centered at the UI. It can be assumed that most of the shortcomings can be circumvented by use of the tutorials provided by the service provider. On the other hand, additional problems (beyond those mentioned in section 4) may not have been recognized.

With our assumptions for the CWs as stated in section 3, we tried to outline a non-tech-savy end user. However, we are aware that the group of those users is diverse, which makes it hard to capture the individual previous knowledge in such assumptions. We tried to assume only the most basic previous knowledge.

7. Conclusion and Future Work

Our long-term goal is to find ways to improve the situation when registering security keys on websites and different operating systems. For this purpose, we started by looking at the current setup process on Google, Facebook, Windows 10 and Ubuntu 18.04.4 to identify issues. We found that websites are too phone-centered and that instructions for operating systems are too long and complex, but leave too many questions open at the same time.

To get a full picture, we will continue to look at more sites or services (e.g. Dropbox, Twitter and further email providers) to further identify different implementations of the steps needed for key registration. By comparing the different approaches, we hope to be able to combine the best implementations to an improved whole setup process, which is service- or website independent. After doing so, we plan to conduct a user study to evaluate our approach and see whether the wizards are self-explanatory, or if users seek help. For this step, we want to include participants with various background and ages, as previous work [4], [5] showed that university students do often not value their data enough to take further steps to protect them.

References

[1] Most hacked passwords https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security, last accessed on march 16, 2020.

[2] E. Stobert, R. Biddle, "The password life cycle: user behaviour in managing passwords", 10th Symposium On Usable Privacy and Security (SOUPS 2014), 2014.

[3] YubiKey – Fast and Simple Two-Factor Authentication https://www.yubico.com/why-yubico/for-individuals/, last accessed on march 13, 2020.

[4] S. Das et al., "A Qualitative Study on Usability and Acceptability of Yubico Security Key", Proceedings of STAST 2017, Florida, USA.

[5] J. Reynolds et al., "A Tale of Two Studies: The Best and Worst of YubiKey Usability", 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 872-888.

[6] K. Reese et al., "A Usability Study of Five Two-Factor Authentication Methods", USENIX Symposium on Usable Privacy and Security (SOUPS) 2019, pp. 357 – 370.

[7] E. De Cristofaro, H. Du, J. Freudiger, G. Norcie, "A Comparative Usability Study of Two-Factor Authentication", USEC '14, 23 February 2014, San Diego, CA, USA.

[8] J. Brooke, "SUS: A 'Quick and Dirty' Usability Scale". In: I.L. McClelland, B. Weerdmeester, B. Thomas, P. W. Jordan, "Usability Evaluation in Industry", London: Taylor and Francis, 1996.

[9] K. Krol, E. Philippou, E. De Cristofaro, M. A. Sasse, ""They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking", USEC '15, 8 February 2015, San Diego, CA, USA.

[10] C. Z. Acemyan, P. Kortum, J. Xiong, D. S. Wallach, "2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-Factor Authentication (2FA) Methods", Proceedings of the Human Factors and Ergonomics Society Annual Meeting vol. 62, no. 1 (September 2018), pp. 1141 – 1145.

[11] S. Ciolino, S. Parkin, P. Dunphy, "Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling", USENIX Symposium on Usable Privacy and Security (SOUPS) 2019, pp. 339 – 356.

[12] Getting Started with the YubiKey on macOS https://support.yubico.com/support/solutions/articles/15000006478-getting-started-with-the-yubikey-on-macos, last accessed on march 13, 2020.

[13] macOS Logon Tool Configuration Guide https://support.yubico.com/support/solutions/articles/15000015045-macos-logon-tool-configuration-guide, last accessed on march 13, 2020.

[14] C. Wharton, J. Rieman, C. Lewis, P. Polson, "The Cognitive Walkthrough Method: A Practitioner's guide", https://www.colorado.edu/ics/sites/default/files/attached-files/93-07.pdf, last accessed on march 14, 2020.

[15] Yubico Login for Windows Configuration Guide https://support.yubico.com/support/solutions/articles/15000028729-yubico-login-for-windows-configuration-guide, last accessed on march 14, 2020.

[16] Ubuntu Linux Login Guide – U2F https://support.yubico.com/support/solutions/articles/15000011356-ubuntu-linux-login-guide-u2f, last accessed on march 14, 2020.

[17] Use a security key for 2-Step Verification https://support.google.com/accounts/answer/6103523?hl=en, last accessed on march 16, 2020.

[18] What is a security key and how does it work? https://www.facebook.com/help/401566786855239, last accessed on march 16, 2020.

[19] State of the Auth: Experiences and Perceptions of Multi-Factor Authentication. Duo Security. https://duo.com/assets/ebooks/state-of-the-auth-2019.pdf, last accessed on april 20, 2020.