A User Study of Keystroke Dynamics as Second Factor in Web MFA

Ahmed Anu Wahab
Department of Electrical and Computer Engineering
Clarkson University
Potsdam, NY, USA
wahabaa@clarkson.edu

Daqing Hou
Department of Electrical and Computer Engineering
Clarkson University
Potsdam, NY, USA
dhou@clarkson.edu

Stephanie Schuckers
Department of Electrical and Computer Engineering
Clarkson University
Potsdam, NY, USA
sschucke@clarkson.edu

ABSTRACT

As account compromises and malicious online attacks are on the rise, multi-factor authentication (MFA) has been adopted to defend against these attacks. OTP and mobile push notification are just two examples of the popularly adopted MFA factors. Although MFA improve security, they also add additional steps or hardware to the authentication process, thus increasing the authentication time and introducing friction. On the other hand, keystroke dynamics-based authentication is believed to be a promising MFA for increasing security while reducing friction. While there have been several studies on the usability of other MFA factors, the usability of keystroke dynamics has not been studied. To this end, we have built a web authentication system with the standard features of signup, login and account recovery, and integrated keystroke dynamics as an additional factor. We then conducted a user study on the system where 20 participants completed tasks related to signup, login and account recovery. We have also evaluated a new approach for completing the user enrollment process, which reduces friction by naturally employing other alternative MFA factors (OTP in our study) when keystroke dynamics is not ready for use. Our study shows that while maintaining strong security (0% FPR), adding keystroke dynamics reduces authentication friction by avoiding 66.3% of OTP at login and 85.8% of OTP at account recovery, which in turn reduces the authentication time by 63.3% and 78.9% for login and account recovery respectively. Through an exit survey, all participants have rated the integration of keystroke dynamics with OTP to be more preferable to the conventional OTP-only authentication.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

Two-Factor Authentication, Multi-Factor Authentication, Usability, User Study, Keystroke Dynamics, Web

CODASPY '23, April 24–26, 2023, Charlotte, NC, USA

ACM ISBN 979-8-4007-0067-5/23/04…$15.00
https://doi.org/10.1145/3577923.3583642

ACM Reference Format:
Ahmed Anu Wahab, Daqing Hou, and Stephanie Schuckers. 2023. A User Study of Keystroke Dynamics as Second Factor in Web MFA . In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (CODASPY '23), April 24–26, 2023, Charlotte, NC, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3577923.3583642

1 INTRODUCTION

In today's world of universal access where technologies such as computers and mobile devices are in the homes and hands of the majority of individuals, improving security is imperative. Malicious attacks against organizations, companies and individuals are rampant and on the rise. Passwords, the conventional means of authentication, although ubiquitous and easy to use, are still vulnerable to attacks owing to the fact that they can be easily shared, stolen, sold or falsely recovered [5, 7, 14]. As a knowledge-based (what you know) authentication factor, passwords are expected to be unique. Therefore, users are often mandated to meet password constraints / requirements that involve the combination of uppercase and lowercase letters, digits, and symbols, which makes passwords difficult to remember and thus hated by users. Despite its security drawbacks and dislikes among users, passwords appear to continue to dominate other authentication methods [4, 5].

The rise of cybercrime requires stronger security and multi-factor authentication (MFA) such as fingerprint recognition, face recognition, one-time password (OTP) and mobile push are commonly used to bridge the security gap in password authentication. These MFA factors are used as secondary authentication factors to further strengthen the primary factor (passwords). These additional factors can be physiology-based (who you are) or possession-based (what you have) and have been widely used in commercial, banking and education websites, and by tech giants like Google, Amazon and Microsoft. OTP and mobile push-based authentication are two examples of the most commonly used MFA. Many of these MFA factors require the user to perform extra activities outside of the primary authentication activity, which takes more time from the user and adds friction.

Improving security often comes at the expense of usability. There is usually a trade-off between security and usability/convenience, as a completely secure system may not be usable and a fully usable system may pose serious security concerns. Authentication time is a good way to measure usability, as an average user will become frustrated if it takes too long to complete authentication.

A more applicable way of improving security, usability and reducing friction is to integrate keystroke dynamics into the regular password authentication process. Keystroke dynamics involves

analyzing a user's typing rhythm and patterns to identify the user [3, 18, 21]. This factor is behavior-based (what you do). It requires no extra activities other than the regular password typing activity, no additional hardware cost and non-intrusive. The focus of many keystroke dynamics research has been on creating better algorithms [1, 2, 8, 10, 12], datasets [9, 15, 16, 19] and improving performance [1, 8]. However, unlike other MFA factors such as fingerprint recognition, face recognition, OTP, mobile push etc. [4], the public acceptance and usability of keystroke dynamics has yet to be studied.

We performed a user study of keystroke dynamics in the context of a real-world web authentication system built with three standard features, i.e., signup, login, and account recovery. The website uses keystroke dynamics as a second factor with OTP as an alternative during enrollment and when a user was rejected by keystroke dynamics. Keystrokes data are captured as users interact with the website and stored in a remote database. Each participant completed at least 100 genuine login attempts and 20 genuine account recovery attempts. To simulate imposters, each participant also attacked 10 times each of randomly selected five other participants with their shared authentication credentials. As in any biometric authentication, keystroke dynamics requires that each user completes an enrollment process, where K samples from a user are used to build the user's profile. In general the larger K is, the better the authentication decision, but a smaller K reduces the time taken at enrollment and friction. The user completed an exit survey in the end.

To our knowledge, this is the first work on the user acceptance and usability of keystroke dynamics-based authentication system. The main contributions of this work include:

(1) We perform a user study on keystroke dynamics-based authentication system using a real-world style website with the standard features of signup, login and account recovery.
(2) We propose and evaluate a novel approach for completing enrollment which avoids additional steps outside of the regular authentication activities and thus reduces friction and time taken at enrollment (Section 3).
(3) We propose a novel authentication system that uses keystroke dynamics as the second factor and OTP as an alternative factor when keystrokes authentication is not ready for use or when the user is rejected by keystroke authentication.
(4) We show that integrating keystroke dynamics with OTP is usable and helps reduce authentication time and friction while maintaining a high level of security.
(5) Through an exit survey, we show that study participants prefer our novel integration of keystroke dynamics with OTP over the conventional OTP-only setting.

The rest of this paper is structured as follows. Section 2 presents related work. Section 3 describes the methodology of our study. We present the results of the study in Section 4. Lastly Section 5 concludes the paper.

2 RELATED WORK

The ineffectiveness of passwords in securing the user against several malicious cyber-attacks has been well known for decades [14]. Although there are many works on replacing passwords with other methods of authentication which are known to provide better security, passwords remains evergreen. Bonneau et al. [4] presented their work on the quest to replace passwords where thirty-five (35) other authentication factors went head-on against the passwords. The comparison was based on twenty-five usability, deployability and security benefits of each factor. Their work shows that some factors provided significant security benefits over passwords but they can also be costly to deploy or difficult to use, while others only provided minor security benefits beyond passwords but also lack in deployability, making it difficult to replace passwords. Similarly, Bošnjak and Brumen highlighted the weaknesses of passwords and argued that the users will eventually be unable to keep track of their passwords [5]. They also examined a set of user-generated passwords, comparing them to the passwords collected by Morris and Thompson [14], and showed that passwords remain as weak as they were decades ago. Although they showed that passwords are weak, yet they disputed the claim that passwords should be replaced by exposing the weaknesses of password alternatives.

Perhaps these password alternatives could be integrated with passwords to defend against its drawbacks instead of going head-on against it, which is the thought behind MFA. It is known that other authentication factors provide security benefits but are they usable? Reese et al. [17] had an extensive study on the usability of five common MFA factors (SMS, TOTP (Time-based OTP), pre-generated-codes, push notification, and U2F security keys). They collected quantitative and qualitative data from 72 participants while completing assigned tasks on a simulated banking website. They also conducted a laboratory study with 30 participants to learn the usability of the enrollment procedure for these five MFA methods. They reported that the U2F devices had the fastest median authentication time, followed by push notifications but the TOTP was the highest scored second-factor method. About one-third of the participants reported on times of not having their second-factor device immediately available when they needed it. Two-thirds of the participants using TOTP had problems entering the six-digit code before it timed out, and a few participants experienced difficulty setting up U2F and TOTP as second factors.

Towards bridging the security gap in passwords, Wiefling et al. [20] used risk-based authentication (RBA) analysis on a real-world online service. The RBA is the estimation of a user's login activity as either genuine or impostor attempt while recording all available data at login, such as IP address, login time etc. RBA calculates a risk score related to the login attempt and compares it against a threshold. A low threshold requests re-authentication at every login attempt, making the system identical to the classical 2FA. When set too high, it never requests re-authentication and considers all attempts as coming from the genuine user, and so does not provide any security benefit. The RBA is unpopular because it lacks open resources and online community support for research and development. A major challenge with RBA is that it requires at least six months login history to work effectively in blocking out targeted attackers. A six-month login history is expensive (time-wise) to have and the temporal use of alternative MFAs while building the login history will result in added friction and time to authenticate.

Karola et el. [13] investigated users perceptions and expectations of few MFA mechanisms and exposed users' unmet requirements in state-of-the-art solutions. They carried out survey on

both experienced and inexperienced MFA users, asking them of their experiences, preferences, and problems using MFAs. Based on the findings and feedback from the participants, they provided ten recommendations for the adoption of MFA-based authentication schemes towards transitioning from current solutions with lot of user frustration to novel 2FA solutions.

Crawford and Ahmadzadeh conducted a study on the impact of user movement during typing on the performance of keystroke dynamics authentication [6]. The research involved 36 participants typing on an Android device and collecting their gyroscope and free-text keystroke data. The data was then utilized for authentication using decision tree and logistic regression classifiers. First, they classified the typing behavior without considering the typing position of the participants (sitting, standing, or walking). The results showed an Area Under the Curve (AUC) of 66.9% for decision tree and 66.2% for logistic regression. However, when they used a two-phased approach of determining the user's position (seated, standing or walking) before classifying their typing behavior, they reported an AUC of over 93%, a 30% improvement compared to classification of typing behavior without considering typing position. This study differs from ours as it only focuses on the effect of the user's typing position on the performance of keystroke dynamics on mobile devices, not on its usability and security as an additional authentication factor in web multi-factor authentication.

While previous studies have investigated the usability of various MFA factors, the impact of typing position on keystroke dynamics, and the improvement of keystroke dynamics performance [1, 18] there has been no research on the usability of keystroke dynamics as a secondary authentication factor in web multi-factor authentication. Our work is the first to study the usability and security of keystroke dynamics-based authentication, using four metrics of usability (authentication time, security, convenience, and feedback from participants). Additionally, we surveyed our participants for their opinion of the usability merit of keystroke dynamics against the conventional OTP.

3 USABILITY STUDY METHODOLOGY

In this section, we describe the details of our user study: the design of the web authentication system, the study procedure, the enrollment process, the exit survey, and the statistics of our data.

3.1 The Web Authentication System

For the purpose of this study, we developed a web-based authentication subsystem supporting signup, login and account recovery as commonly seen in real-world websites. We captured users' typing pattern as they type information into the website. Due to Covid-19 restrictions and the desire to encourage more participation and completely natural user behavior, the website was hosted in the cloud and the study was conducted completely online in the participant's own environment. The details of the web pages throughout the user journey are described as follows.

3.1.1 The Signup Page. As the custom of every online system, the user journey begins at the account creation page. This page helps build the identity of the user using their personal information. Figure 1 shows the signup page and the information collected from the user, including full name, date of birth, full address, phone number, email, username and password. Participant's keystroke data are captured on this page and used as the first sample in building the user's profile. While consumer websites often collect varying amounts of information from users during account creation, more information can be required for added security.

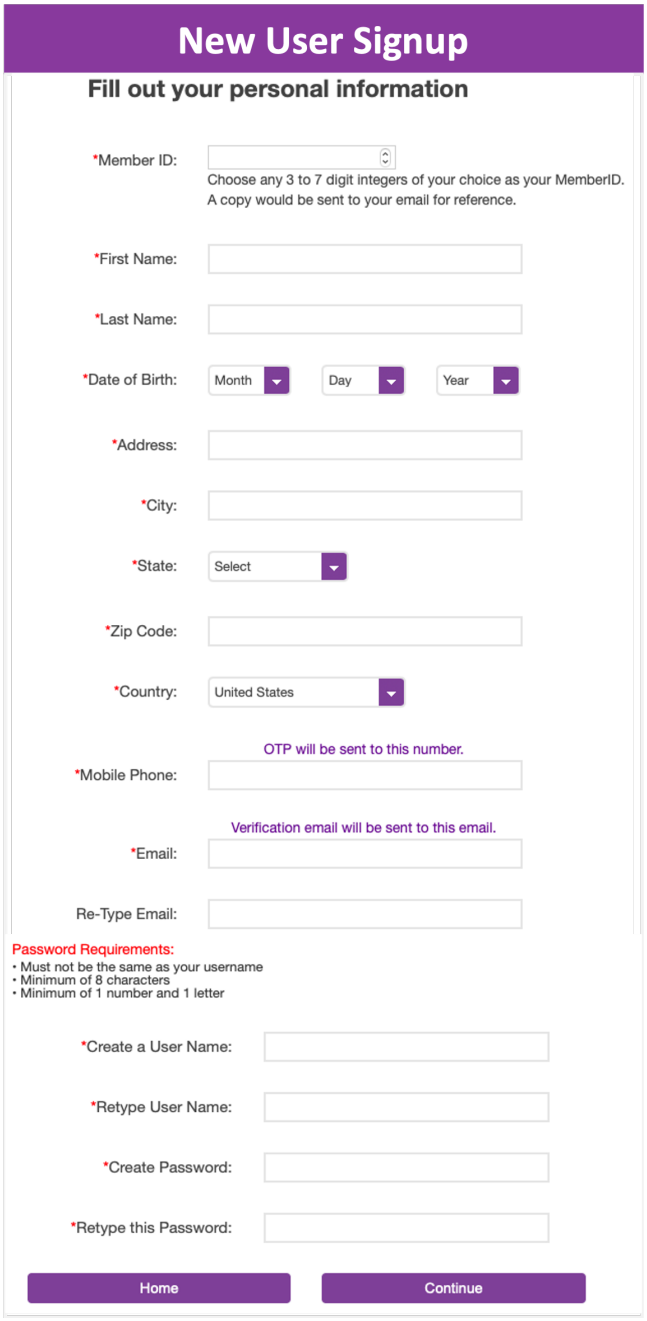

Figure 1: The user Signup page for new account creation. Keystroke data are captured as the user completes the form, which serves as the first profile sample.

Figure 2: The user Login page. The highlighted parts are for user login and buttons to redirect to the signup and account recovery pages.

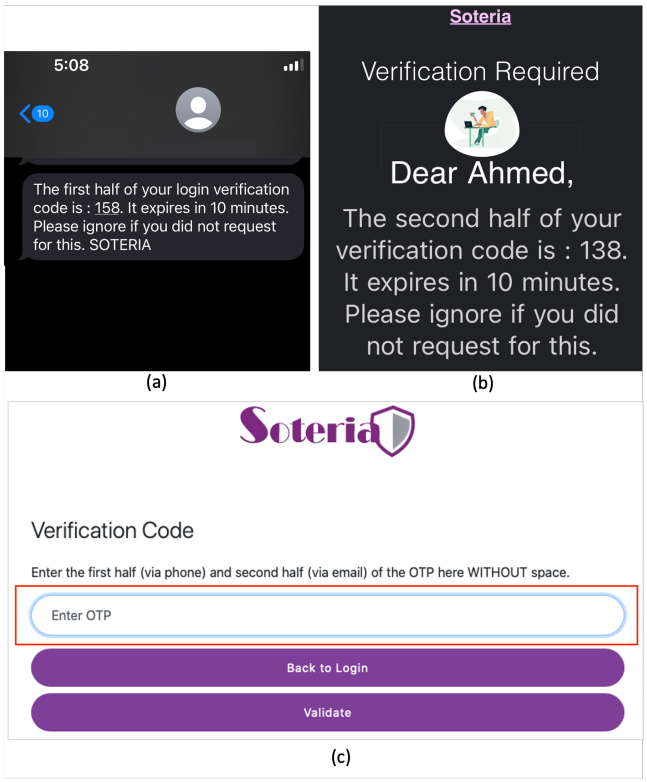

Figure 3: The escalation process when a user fails keystroke dynamics authentication. (a) The first half of the OTP sent to the legitimate user's phone. (b) The second half of the OTP sent to the legitimate user's email address. (c) The screen on the web application where both OTPs are entered.

3.1.2 The User Login Page. Next on the user journey is gaining access to the just created account. This page (Figure 2) captures not just the username and password but also the participant's keystrokes data which will later be used for authentication. This page also has a redirecting button to create a new account and a button for account recovery that the user can use to regain access to their account in case that they forget their password.

3.1.3 The User Home Page. Upon a successful login into the web system, the participant is greeted with a home screen that mimics the standard consumer website (Figure 4). Since the goal of this study is focused on studying the usability of keystroke dynamics, we limited the clickable buttons on the user home page to just the "logout" button.

3.1.4 Account Recovery Page. The account recovery option is ubiquitous in standard consumer website because the complexity around the choice of passwords makes it easy to forget them. Therefore, account recovery is designed to provide users with the opportunity to regain access to their accounts. A common and simple recovery method implemented in many consumer websites requires users to enter their verified email where the recovery link would be sent. This is considered a low security approach since the verified email can be stolen, rendering the account vulnerable. In contrast, we collected multiple information from users for improved security. As shown in Fig. 5, our account recovery is divided into three steps. Step 1 captures the participant's personal information. In Step 2, participants are required to type the following declaration text, *"I declare that I am (Full name) and everything I type here is true"*, after which the keystroke authentication is triggered. If the authentication is successful, the participant is required to choose a new password in Step 3. Otherwise OPT is triggered. A confirmation screen is displayed upon a successful password change.

3.2 Study Procedure

After IRB approval, advertisement was made in our university's daily email newsletter inviting students and faculty to participate in the web user-study. Intending participants showed their interest via email and we responded with the link to the study website alongside the instructions detailing the tasks to be completed. The study was fully remote and all participants who completed the study were compensated. All participants carefully read and signed the online consent form which contains the terms and condition of the study, study overview and purpose, tasks to be completed, participants' rights, and compensation. A proof of the signed consent form was mailed to all participants. The study lasted for about 4 months. A total of 20 participants, who were students of our university, participated. All participants were asked to complete an exit survey at the end of the study. We used keystroke dynamics as the second factor and OTP as an alternative factor in case when keystroke dynamics is not ready for use or the user fails the keystroke dynamics authentication. Also, the web user-study website captures and stores keystrokes data to a remote database. The tasks to be completed by all participants were divided into two categories: First is the genuine user tasks and the second is the impostor tasks.

3.2.1 Genuine User Tasks. In genuine tasks, each participant is required to go through the three stages of the user journey - user signup, login and account recovery - and to complete the necessary sub-tasks in each. Beginning with the user signup, the participant will complete the signup form with their personal information and

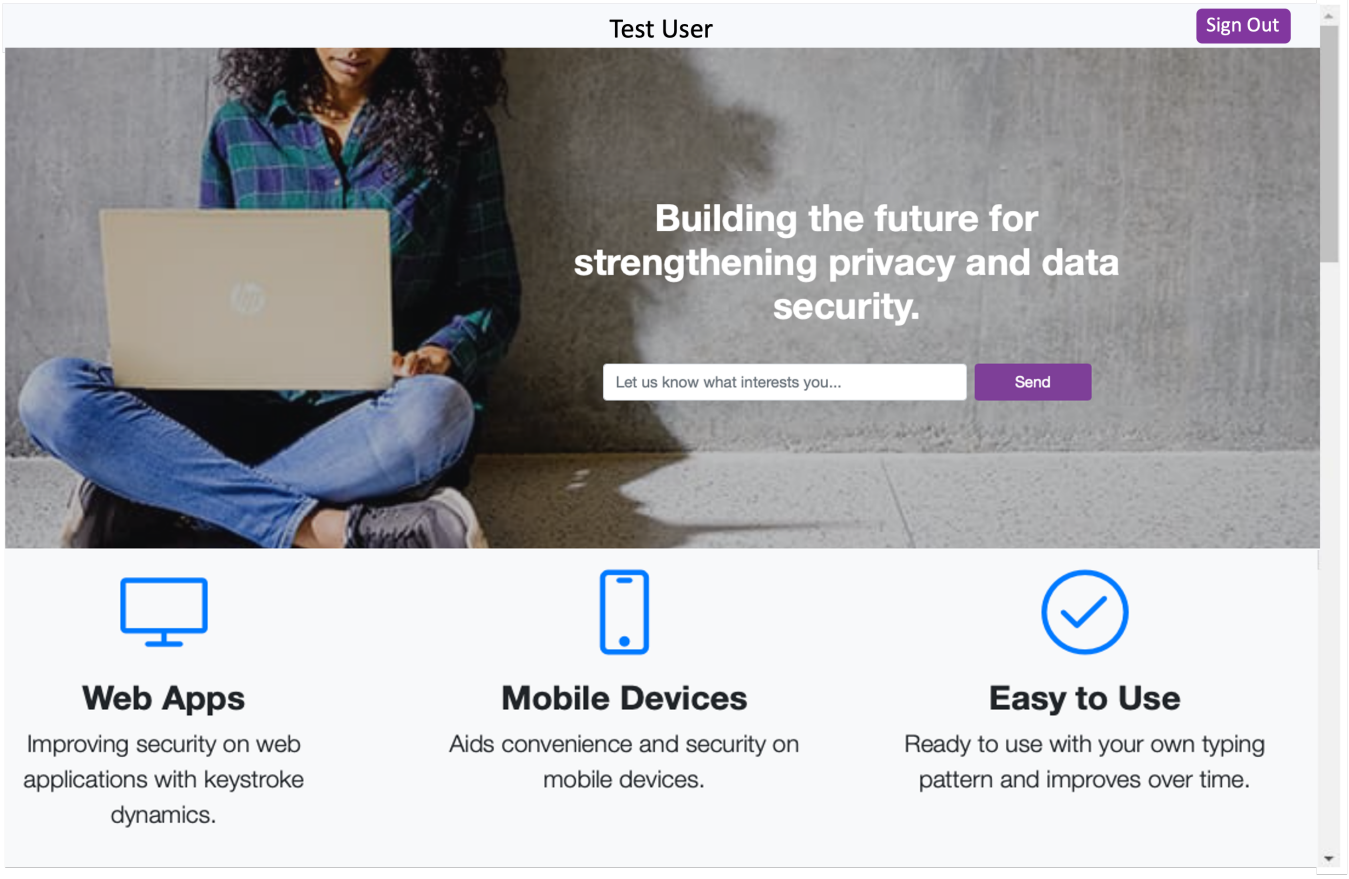

Figure 4: The user home page. User can exit the page by clicking the "Signout" button at the top

set up a username and password of their choice. A verification email is sent to the participant so as to ensure the validity of the email address provided. After the email is verified, the participant will then proceed to the user login stage. The participant attempts to login using the same credentials used at account creation. At this point, OTP is used as the initial authentication factor until the user has completed the K login attempts required by the enrollment process. Once the enrollment process is completed, the system will automatically default to using keystroke dynamics authentication.

The credentials (username and password) are first verified and validated before the default keystroke dynamics authentication factor is being triggered. If the user fails the keystroke dynamics authentication (after the enrollment process is completed), the system escalates the authentication process as shown in Fig. 6. We chose to escalate by sending half of an OTP to the genuine user's phone and the other half to the genuine user's email address as shown in Figure 3. It is expected that the genuine user has access to both the email and phone where the OTP is sent, while an imposter would not. In the case of false reject (genuine user was denied access), the system updates the user's keystroke profile with the new keystrokes sample after the OTP authentication has been passed. In the case of true reject (imposter was denied access), the keystrokes sample can be discarded or kept for future analysis. In this study, we decided to store these samples as "imposter samples" for further experimental analysis. A similar procedure is followed for the account recovery stage. The participant will complete the account recovery form using their personal information. The OTP is also used until the enrollment process is completed, after which the system defaults to keystroke dynamics authentication. The account recovery process is escalated should the user fail the keystroke authentication.

All participants were required to complete at least a 100 login attempts and 20 account recovery attempts. Generally, a user's typing behavior may change based on their mood, time of day (morning, afternoon or evening), past activities, health condition etc. To simulate actual user behavior and capture user's typing pattern in varying scenarios and across different mood, day and time, we ensured that all attempts are spread out with a maximum of 20 logins and 5 account recoveries per week. The user can only proceed to the next category (impostor tasks) after completing all tasks in this category. The system automatically keeps a record of all completed genuine tasks and if they are true accepts or false rejects.

3.2.2 Impostor Tasks. In this category of tasks, the credentials and information of 5 other random participants are shared, one at a time, with the participant to attack with. This is done in order to simulate the impostor attack scenario and observe how keystroke

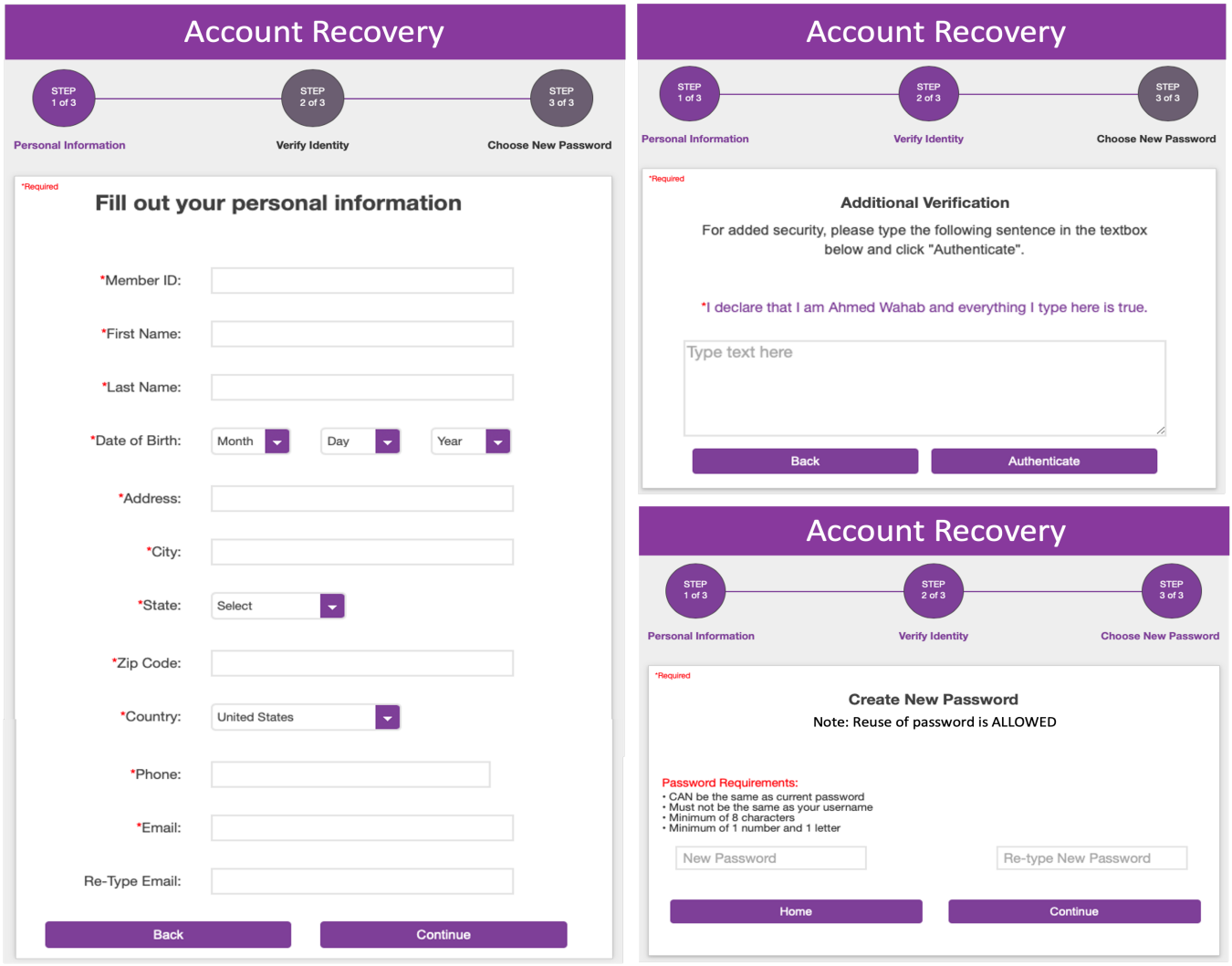

Figure 5: The account recovery pages. In Step 1 the participant types personal information (left). In Step 2 the participant declares the authenticity of their information (top right). Step 3 sets up a new password (bottom).

dynamics authentication responds to this kind of attack. The participant is required to complete 10 impostor logins and 10 account recoveries for each of the 5 participants he/she is to impersonate. To motivate imposters, additional compensation is given to the participant that successfully gain access into the account of the person he/she impersonated. The web system keeps record of all impostor tasks completed and the authentication status (true rejects or false accepts).

3.3 Enrollment

The user enrollment process of any biometric authentication is one of the important factors that determine the user acceptance and usability of the authentication factor. This process builds/creates the user's profile template which requires that the user contributes K samples, where K typically ranges from 1 to 10 in most keystroke literature. Authentication scores are calculated by comparing a query/test sample with the profile template. The choice of the approach for completing the enrollment process and the value for K are highly critical, as a less efficient approach can introduce a high enrollment friction to the overall authentication process. A simplistic and naive approach is to enforce the completion of the enrollment process (K samples) at once during signup but before user-login. Although keystroke authentication will be immediately available for use as the main and default authentication factor in this approach, it is more likely to cause an enrollment friction because the repeated typing of the same password is new and unnatural to the user. This naive approach toward enrollment will negatively affect the user acceptance of keystroke dynamics.

Instead, we approached the enrollment process differently. In our approach, we collected all enrollment samples without requesting the users to perform any extra activity outside of their regular authentication activities. Specifically, the first enrollment sample is

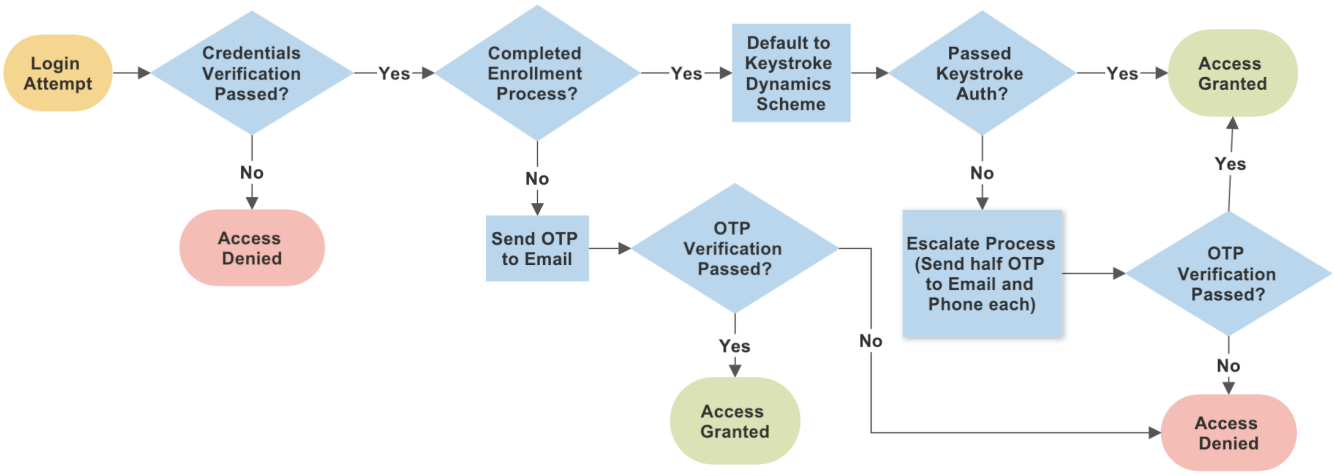

Figure 6: The flow chart of the user login procedure. The flow chart for account recovery follows a similar procedure.

collected at signup, and the remaining $K-1$ samples are collected after a successful user login and/or account recovery attempts. We used the OTP as the temporary authentication factor until the K profile samples are complete. After which, the system defaults to keystroke dynamics authentication. This approach reduces the initial enrollment friction.

We experimented with finding the optimum value of K by varying it from 1 to 10 with an increment of 1. The optimum value is the value that reduces both the initial false reject and authentication friction. For example, a value of 10 significantly reduces the initial false reject but increases the authentication friction, meaning that the system would use the temporary OTP authentication factor 9 times (i.e, $K-1$) before defaulting to the keystroke authentication factor. On the other hand, a value of 1 would significantly reduce the authentication friction but would increase the system's initial false reject because one profile sample is not sufficient to capture the user's typing behavior. We empirically set the optimum value for K to be 5.

For this study, we have implemented a statistical metric known as the Scaled-Manhattan distance, which is commonly used for fixed-text keystroke dynamics [11]. The Scaled-Manhattan distance measures how far apart the test and profile samples are. Hence, the closer the distance score is to 0, the more likely the test and profile samples belong to the same user.

3.4 Exit Survey

Participants were asked to complete an exit survey (see Table 6) to capture their password practices, experiences with password authentication, and their perception and ratings on keystroke authentication compared to other MFA factors.

3.5 Data Statistics

Table 1 and 2 shows the data statistics of the number of keys contributed per field and across all participants for login and account recovery respectively. As seen from the tables, the average total number of keys contributed at login is 17, which is much lesser than the total average total number of keys contributed at account recovery (117).

Table 1: Statistics for numbers of keys contributed per field across all subjects at Login. The average number of keys contributed at login is 17.

Fields	Avg	Min	Max
Username	8	6	12
Password	9	5	15
Total	**17**	**11**	**27**

Table 2: Statistics for numbers of keys contributed per field across all subjects during Account Recovery. The average number of keys contributed at account recovery is 117.

Fields	Avg	Min	Max
Full name	7	4	10
Address	14	7	19
City	7	5	10
Zip	5	4	6
Phone	10	10	12
Email	19	15	22
Declaration	65	60	70
Total	**117**	**105**	**149**

4 STUDY RESULTS

The results of the web user-study are sectioned based on these four usability metrics: security, convenience, authentication time, and participants feedback.

4.1 Security and Convenience

The security of a system is measured based on its false acceptance/positive rate (FPR), which is the percentage of times an impostor is falsely granted access to an account by the system. The lower the FPR, the more security the system provides. Convenience, on the other hand, is measured by the true acceptance/positive rate (TPR), which is the percentage of times a legitimate user is granted access to his account. A convenient system has a high TPR. An ideal system is expected to have 0% FPR and 100% TPR. However, there is always a trade-off between security and convenience and the preferred operating point depends on the specific use-case. Table 3 shows the FPR and TPR for login and account recovery respectively based on different operating thresholds. The receiver operating characteristic (ROC) curve of the login and account recovery is shown in Figure 7. Operating the keystroke dynamics-based authentication with utmost security (FPR of 0%) gives a TPR of 66.3% for the login and 85.8% for the account recovery. Therefore, for every 66 out of 100 logins and 85 out of 100 account recoveries, the user will not have to use other MFA (such as OTP) that increases authentication friction and adds extra steps to the authentication activities. Furthermore, as seen in the table, withstanding some FPR can give better TPR, but the preferred operating point depends on the application - either to favor security or convenience. For example, operating the keystroke dynamics-based authentication to favor convenience (threshold set to 1.23) gives 0.2% FPR and 76.9% TPR for the login, and 1.9% FPR and 95.4% TPR for the account recovery. However, in this paper, our focus is geared towards studying the performance of keystroke dynamics at utmost security (0% FPR), which shows that it reduces authentication friction by 66.3% at login and 85.8% at account recovery, without sacrificing security. Overall, account recovery has better performance compared to the login. This is because the average length of text at account recovery is much longer than that of login (see Table 1 and 2), and better performance is usually observed for longer text than for shorter text.

4.2 Authentication Time

To illustrate the authentication time for each user, we selected 2 random users and showed their total authentication time for the four enrollment attempts with OTP only, as well as the first four attempts with keystroke dynamics only (as shown in Table 4). Note that the timing were captured for both login/account recovery. The "Typing" column is the time it takes the user to type his credentials/information (i.e., username and password in the case of login) while the "Authentication" is the authentication time for the specific authentication type - keystroke-only or OTP-only. Finally, the "Total" is the overall time it takes to authenticate the user, beginning from when the user starts typing till access is granted. The system is not responsible for the typing time as it is completely dependent on how fast the user types, familiarity with the content and

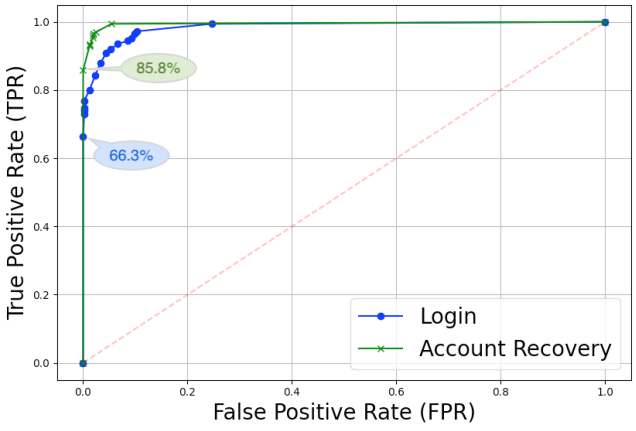

Figure 7: ROC for both login and account recovery. The respective TPR at 0% FPR is marked.

the length of the credentials/information. In the case of keystroke-only authentication, the authentication time depends on how fast the system makes the authentication decision. However, for the OTP-only authentication, the authentication time is dependent on both the system (how quick the OTP was sent to the user and how fast to make the authentication decision) and the user (how fast the user enters the OTP back into the system correctly). As a result, the keystroke-only authentication is far more time conserving compared to the conventional OTP-only case.

To have a general overview of the authentication time for each authentication method, we calculated the time it takes to authenticate with OTP only, keystroke dynamics only, and lastly the time it takes for credential typing across all users and showed the statistics in Table 5. Note that it took slightly longer time to authenticate the user with keystroke dynamics at account recovery than at login. This is because keystroke dynamics authentication processes more text (information/data) at account recovery than at login. On the average, at login, it takes 7.77 secs for credential typing, 13.53 secs to authenticate with OTP only, and 0.4 secs to authenticate with keystroke dynamics only. However, our authentication system is neither keystroke-only nor OTP-only but a combination of both - keystroke dynamics as second factor and OTP as alternative factor should in case the user fails keystroke authentication. Hence, there is a need to calculate the actual authentication time for this system. Since keystroke dynamics authentication saves 66.3% of OTP at login and 85.8% of OTP at account recovery (from Table 3), we can calculate the system's authentication time ($T_{keystroke+OTP}$) using Equation 1, where T_{OTP} is the OTP-only authentication time, $T_{keystroke}$ is the keystroke-only authentication time, and TPR is the true positive rate for login and account recovery from Table 3. The system average authentication time is 4.96 secs and 3.37 secs for login and account recovery respectively. Therefore, our system with keystroke authentication as second factor and OTP as alternative factor (compared with the OTP-only system) significantly reduces the average authentication time by 63.3% (from 13.53 to 4.96 secs) at login and 78.9% (from 15.98 to 3.37 secs) at account recovery.

Table 3: The FPR and TPR for the login and account recovery from five different operating thresholds across all users.

	Login		Account Recovery	
Threshold	FPR(%)	TPR(%)	FPR(%)	TPR(%)
1.1	0.0	66.3	0.0	85.8
1.18	0.2	72.9	1.2	92.8
1.19	0.2	74.1	1.2	93.3
1.2	0.2	74.8	1.3	93.3
1.23	0.2	76.9	1.9	95.4

Table 4: The total authentication time for two random users, which includes the time for each of the four enrollment OTPs and the time for the keystroke dynamics authentication between the browser and the server. Note that times for Typing and Authentication are captured for both login and account recovery separately (i.e. login/account recovery)

			Duration (secs)		
User	Auth Type	Attempt	Typing	Authentication	Total
1103	OTP-Only (Enrollment)	1	3.87 / 54.02	7.22 / 25.12	11.09 / 79.14
		2	4.36 / 40.37	9.33 / 22.11	13.69 / 62.48
		3	4.11 / 48.97	10.32 / 15.20	14.43 / 64.17
		4	4.45 / 41.60	9.52 / 17.30	13.97 / 58.90
	Keystroke-Only	5	3.64 / 51.21	**0.19 / 1.23**	3.83 / 52.44
		6	3.28 / 39.79	**0.22 / 2.32**	3.50 / 42.11
		7	4.08 / 43.23	**0.24 / 2.51**	4.32 / 45.74
		8	3.35 / 36.53	**0.30 / 2.92**	3.65 / 39.45
100	OTP-Only (Enrollment)	1	6.99 / 72.08	12.62 / 16.16	19.61 / 88.24
		2	6.31 / 54.34	9.24 / 15.13	15.55 / 69.47
		3	6.23 / 57.92	9.12 / 24.11	15.35 / 82.03
		4	6.70 / 49.55	10.16 / 22.54	16.86 / 72.09
	Keystroke-Only	5	6.86 / 51.16	**0.13 / 1.51**	6.99 / 52.67
		6	6.84 / 53.59	**0.17 / 2.08**	7.01 / 55.67
		7	6.57 / 50.44	**0.20 / 2.20**	6.77 / 52.64
		8	6.66 / 48.66	**0.22 / 2.25**	6.88 / 50.91

Table 5: Authentication time statistics for all users at login/account recovery. Compared with the conventional OTP-only approach, our novel approach of combining keystroke dynamics and OTP reduces the authentication time by 63.3% and 78.9% at login and account recovery respectively (on average).

	Duration (secs)				
Method	Min	Q1	Mean	Q3	Max
Typing	3.28 / 40.37	4.05 / 53.83	7.77 / 66.1	10.00 / 74.73	22.36 / 106.3
OTP-Only Auth	5.11 / 8.62	9.31 / 12.12	13.53 / 15.98	16.10 / 18.40	20.20 / 25.21
Keystroke-Only Auth	0.11 / 0.52	0.19 / 0.75	0.40 / 1.10	0.54 / 1.37	1.12 / 2.31
Keystroke+OTP Auth	1.83 / 1.74	3.33 / 2.47	4.96 / 3.37	5.97 / 3.98	7.93 / 5.89

$$T_{keystroke+OTP} = T_{keystroke} + ((1 - TRP) \cdot T_{OTP}) \quad (1)$$

4.3 Participant Feedback

Table 6 shows the feedback from participants. Questions 1 and 2 help to understand the background of the participants in relation to password attacks. Generally, older adults may have trouble keeping track of their passwords than younger adults, hence Question 3 captures the age range of our participants. All of our participants are 40 years old or younger.

Since passwords are advised to be unique and not repeated across multiple websites, we use Question 4 to gauge the range of the numbers of passwords our participants have. 80% of them have more than three passwords. Similarly, keeping track of passwords could be a daunting task, especially with multiple unique passwords. Question 5 asks if our participants use password managers and why they do. 35% of them report that they keep track of their passwords with a password manager while others either do not see a need to or are concerned about its security.

Questions 6, 7 and 14 are related to account recovery. Question 6 is intended to survey our participants if forgetting password is something they suffer from and to understand the primary reason for this. 60% of them acknowledge having had trouble remembering their passwords mainly because they have too many of them. Question 7 requires participants to rate the importance of account recovery, and 90% of them considered it to be important while the remaining 10% do not care. We hypothesize that participants who use the account recovery option often are more likely to rate it as important, while those who have fewer passwords, use password managers or write down their passwords are more likely to not care. For improved security, we required participants to enter multiple personal information items during the account recovery process, so Question 14 was used to capture the condition at which the participants would accept this design. The survey showed that, while all participants agree to accept our design of collecting multiple information for account recovery, they also agree that this is only necessary when security is of utmost importance.

Questions 9 and 10 asked the participants to evaluate our integration of keystroke dynamics with OTP to improve usability and reduce friction. In Question 9, we asked the participants if our system with keystroke dynamics as the second factor and OTP as alternative factor is more convenient compared to the conventional OTP-only case, to which all participants agree that integration of keystroke dynamics made our system more convenient. Question 10 further expands on this by weighing participants' preference on replacing other two-factor authentication factors (such as token-based only or mobile app push notification only) with our keystroke dynamics system, and all participants agree to prefer the idea.

Questions 11 and 12 ask if the participants were ever falsely rejected and the frequency of these false rejects. Although half of the participants (50%) expressed to have experienced false rejects at some point (very few times) in the study, only a quarter (25%) were truly wrongly rejected by the system, and others agreed to have intentionally changed their typing pattern, perhaps to test the robustness of the system (Q11). All of those who experienced a false reject agreed that the false rejects were rare (less than 10%) (Q12).

Question 13 is used to understand the improvement of our system on convenience (both for login and account recovery) and how important this improvement is to the participants. A total of 90% of the participants agree that our system with keystroke dynamics improves convenience, out of which 20% consider the improvement to be "very" important, while the remaining 70% consider it to be "somewhat" important. Finally, Question 15 asks if participants used their true username and password during the study, to which 90% of them do, while the remaining 10% do not.

Keystroke dynamics relies on the users to type out their credentials or information and would stop working when features such as auto-fill or copy-paste is used. With Question 8, we observe that about 50% of the participant uses auto-fill outside of this study.

Overall, participants rated the keystroke dynamics-based authentication (when integrated with OTP) more preferable, convenient and time saving than the OTP-only authentication.

5 CONCLUSION

We conducted a web-based user study of keystroke dynamics-based authentication where keystroke dynamics was integrated with OTP to improve usability and reduce friction while maintaining security. Using a standard consumer website that we built for this study, a total of 20 participants completed tasks related to signup, login and account recovery. The study was completely remote and natural where each participant completed, in their settings, 100 genuine logins and 20 genuine account recoveries, after which 5 other random participants' credentials were shared with the participant to impersonate with. We also implemented a new enrollment process approach for building the user's profile without introducing enrollment friction. More specifically, the OTP-based authentication was used as the initial authentication factor until the enrollment process is complete, and subsequent login or account recovery attempts uses the keystroke dynamics-based authentication factor. We analysed the usability of keystroke dynamics-based authentication using the following measures: authentication time, security, convenience and participants feedback. Overall, our study shows that while maintaining strong security (0% FPR), adding keystroke dynamics-based authentication significantly reduces authentication friction (by 66.3% for login and 85.8% for account recovery), leading to reduction in authentication time (average reduction of 63.3% for login and 78.9% for account recovery). Through the exit survey, all participants rated our novel integration of keystrokes with OTP to be more preferable to the conventional OTP-only authentication.

ACKNOWLEDGMENTS

This work was supported by US NSF award TI-2122746.

REFERENCES

[1] Alejandro Acien, Aythami Morales, John V Monaco, Ruben Vera-Rodriguez, and Julian Fierrez. 2021. TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 4, 1 (2021), 57–70.

[2] Blaine Ayotte, Mahesh Banavar, Daqing Hou, and Stephanie Schuckers. 2020. Fast free-text authentication via instance-based keystroke dynamics. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 2, 4 (2020), 377–387.

[3] Salil P Banerjee and Damon L Woodard. 2012. Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition*

Table 6: Exit survey and results.

Questions	Options	Results
1. Has anyone accessed your account without your consent before?	Yes my credentials were phished or stolen somehow	10%
	No, not what I am awared of	90%
2. Have you ever shared your account credentials with any family member or friends before?	Yes	45%
	No	55%
3. What is your age range?	40 or Below	100%
	Above 40	0%
4. How many passwords do you use now?	Less than 3	20%
	Between 3 and 7	55%
	8 or more	25%
5. Do you use a password manager and why?	Yes, because I have too many passwords, they are difficult to remember, or BOTH	35%
	No, because I am concerned about its security	25%
	No, I do not see the need to	40%
6. Do you suffer from the difficulty of remembering passwords and why?	No, I have no problem remembering them	25%
	No, as I write them down somewhere	15%
	Yes, as I tend to create too many of them for sake of security	15%
	Yes, as the slightly different password rule from every website forced me to create too many	45%
7. Is account recovery (also known as forgot password) important to you ?	Yes, definitely	80%
	Yes, somewhat	10%
	I do not care	10%
8. Generally (outside this study), do you use auto-fill to store your username and password or do you type it out each time?	I almost always type it out	20%
	I type it out when the password is important to me. Otherwise I use auto-fill	30%
	I use auto-fill every time	25%
	I use auto-fill only occasionally	25%
9. Our system uses the OTP only for the first 4 initial logins, after which only the username and password were required from you. In contrast, conventional OTP-based authentication requires OTP for every login. Do you feel our new authentication is more convenient than the conventional?	Yes, definitely	30%
	Yes, somewhat	70%
	No	0%
10. Our current system optimizes the user experience of OTP-based authentication with the IMPLICIT keystroke dynamics. This design can also be used to replace any other 2-factor based authentication such as token-based or mobile app push notification. Will you prefer this idea?	Yes, definitely	65%
	Yes, somewhat	35%
	No	0%
11. Are there instances you were confident that you have entered the correct username and password but the system rejects you (in such cases, you should have received OTP). Select the best option that applies to you.	Yes, and I have changed my typing behavior	25%
	Yes, but I have typed as usual	25%
	No	50%
12. If your answer to the previous question is NO, ignore this question. Otherwise, how often do you think our system has falsely rejected you?	0% (never)	0%
	Less than 10% (very few times)	100%
	More than 10% but not every time	0%
	100% (every time)	0%
13. Do you agree that the studied system has improved user experience and offers convenience? How important is such improvement in user experience to you?	I agree and the improvement is very important to me	20%
	I agree and the improvement is somewhat important to me	70%
	I do not know (hard to tell)	10%
14. Our account recovery asks you to enter multiple personal information items. In contrast, the simplest account recovery requires only a single email address. Under what condition will you accept our design?	When security is of utmost importance to me, for example when SSN or bank account are involved	100%
	I do not care as I do not have anything that requires that high a level of security	0%
15. In this study, did you use your true username and password?	Yes	90%
	No	10%

Research 7, 1 (2012), 116–139.

[4] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE symposium on security and privacy*. IEEE, 553–567.

[5] Leon Bošnjak and Boštjan Brumen. 2019. Rejecting the death of passwords: Advice for the future. *Computer Science and Information Systems* 16, 1 (2019), 313–332.

[6] Heather Crawford and Ebad Ahmadzadeh. 2017. Authentication on the go: Assessing the effect of movement on mobile device keystroke dynamics. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association Santa Clara, 163–173.

[7] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. 2010. Password strength: An empirical analysis. In *2010 Proceedings IEEE INFOCOM*. IEEE, 1–9.

[8] Yunbin Deng and Yu Zhong. 2013. Keystroke dynamics user authentication based on gaussian mixture model and deep belief nets. *International Scholarly Research Notices* 2013 (2013).

[9] Vivek Dhakal, Anna Maria Feit, Per Ola Kristensson, and Antti Oulasvirta. 2018. Observations on typing from 136 million keystrokes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[10] Jiaju Huang, Daqing Hou, Stephanie Schuckers, Timothy Law, and Adam Sherwin. 2017. Benchmarking keystroke authentication algorithms. In *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 1–6.

[11] Kevin S Killourhy and Roy A Maxion. 2009. Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, 125–134.

[12] Saket Maheshwary, Soumyajit Ganguly, and Vikram Pudi. 2017. Deep secure: A fast and simple neural network based approach for user authentication and identification via keystroke dynamics. In *IWAISe: First International Workshop on Artificial Intelligence in Security*, Vol. 59.

[13] Karola Marky, Kirill Ragozin, George Chernyshov, Andrii Matviienko, Martin Schmitz, Max Mühlhäuser, Chloe Eghtebas, and Kai Kunze. 2022. " Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Transactions on Computer-Human Interaction* (2022).

[14] Robert Morris and Ken Thompson. 1979. Password security: A case history. *Commun. ACM* 22, 11 (1979), 594–597.

[15] Christopher Murphy, Jiaju Huang, Daqing Hou, and Stephanie Schuckers. 2017. Shared dataset on natural human-computer interaction to support continuous authentication research. In *2017 IEEE International Joint Conference on Biometrics, IJCB 2017, Denver, CO, USA, October 1-4, 2017*. IEEE, 525–530. https://doi.org/10.1109/BTAS.2017.8272738

[16] Kseniia Palin, Anna Maria Feit, Sunjun Kim, Per Ola Kristensson, and Antti Oulasvirta. 2019. How do people type on mobile devices? Observations from a study with 37,000 volunteers. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*. 1–12.

[17] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 357–370.

[18] Pin Shen Teh, Andrew Beng Jin Teoh, and Shigang Yue. 2013. A survey of keystroke dynamics biometrics. *The Scientific World Journal* 2013 (2013).

[19] Ahmed Anu Wahab, Daqing Hou, Mahesh Banavar, Stephanie Schuckers, Kenneth Eaton, Jacob Baldwin, and Robert Wright. 2022. Shared Multi-Keyboard and Bilingual Datasets to Support Keystroke Dynamics Research. In *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy*. 236–241.

[20] Stephan Wiefling, Paul René Jørgensen, Sigurd Thunem, and Luigi Lo Iacono. 2022. Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. *ACM Transactions on Privacy and Security* (2022).

[21] Yu Zhong and Yunbin Deng. 2015. A survey on keystroke dynamics biometrics: approaches, advances, and evaluations. *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics* 1 (2015), 1–22.