User Perceptions of Security and Usability of Mobile-based Single Password Authentication and Two-Factor Authentication

Devriş İşler[1]*, Alptekin Küpçü[2], and Aykut Coskun[2]

[1] imec-COSIC, KU Leuven, Leuven, Belgium
[2] Koç University, İstanbul, Turkey
{devris.isler@kuleuven.be,akupcu@ku.edu.tr,aykutcoskun@ku.edu.tr}

Abstract. Two-factor authentication provides a significant improvement over the security of traditional password-based authentication by requiring users to provide an additional authentication factor, e.g., a code generated by a security token. In this decade, single password authentication (SPA) schemes are introduced to overcome the challenges of traditional password authentication, which is vulnerable to the offline dictionary, phishing, honeypot, and man-in-the-middle attacks. Unlike classical password-based authentication systems, in SPA schemes the user is required to remember only a single password (and a username) for all her accounts, while the password is protected against the aforementioned attacks in a provably secure manner.
In this paper, for the first time, we implement the state-of-the-art mobile-based SPA system of Acar et al. (2013) as a prototype and assess its usability in a lab environment where we compare it against two-factor authentication (where, in both cases, in addition to the password, the user needs access to her mobile device). Our study shows that mobile-based SPA is as easy as, but less intimidating and more secure than two-factor authentication, making it a better alternative for online banking type deployments. Based on our study, we conclude with deployment recommendations and further usability study suggestions.

Keywords: Password-based authentication, usability, two-factor authentication, single password authentication.

1 Introduction

Password-based authentication that is widely deployed today is vulnerable to many attacks including offline dictionary, phishing, honeypot, and man-in-the-middle attacks. Unfortunately, the server password databases get hacked, and millions of users are affected because their passwords are not complicated enough to resist offline dictionary attacks or because of server misconfiguration that stores plaintext passwords [10, 11]. The damage of these attacks on the password

* Work done at Koç University

becomes dramatically dangerous when the user reuses the same password for multiple sites, which is common in practice [16].

Two-factor authentication (2FA) has emerged as a way to improve security by requiring the user to provide one more authentication factor in addition to the password. To be successful, the attacker has to exploit both authentication factors. 2FA has been employed mostly in finance, government and enterprise areas due to the sensitivity of the users' information. However, the servers employing 2FA still keep password databases as in the traditional password-based authentication systems. Therefore, the users' passwords are still vulnerable to offline dictionary, honeypot, phishing, man-in-the-middle attacks even when they employ 2FA. Even though such an attacker cannot gain access to the servers employing 2FA by attacking the password, password re-use is still problematic.

In this decade, another approach called single password authentication (SPA) based on cryptographic building blocks is presented. SPA systems (first shown by [4] (with their patent application dating 2010 [7]), [8], [20], [28], and [18]) ensure provable security even when the user re-uses the same password on multiple sites. SPA methods achieve this by introducing an additional party to store a secret (e.g., mobile device). A secret independent of the password (e.g., a cryptographic key) is generated and stored on this storage device protected by the user's single password. The associated verification information is shared with the login server during the registration. Whenever the user wants to log in to the server, the user communicates with both the storage device and the login server. She securely retrieves the secret information from the storage device in a way that only the legitimate user can reconstruct the secret using her single password. Then, the user signs in to the server with the reconstructed secret. For full cryptographic details, we refer the reader to the cited papers

In this setting, similar to 2FA, the attacker also needs to guess the user's password, and additionally access the secret storage device (e.g., the mobile device of the user). But, differently from 2FA, in SPA systems, when any one of the parties (i.e., storage provider and login server) is compromised, the user's single password is still kept secure from attackers. Compared to 2FA, SPA solutions provide provable security against all the aforementioned attacks.

In this paper, we study the usability of the first mobile-based SPA mechanism (where the storage device is the mobile device of the user) by Acar et al. [4] and compare it against 2FA commonly used for online banking because both approaches similarly employ a random one-use challenge via the mobile device, in addition to the password. Acar et al. [4] solution can be implemented as only a mobile device application (unlike [28] that requires both a mobile phone application and a browser extension) and is the *only* existing SPA proposal that protects the user's single password against malware-infected computers (e.g., at internet cafes or public computers at laboratories, libraries, etc.).

Conducting user studies on a new system is important for determining whether the system is suitable for its end users and its purpose. These studies ascertain any difficulties that the users may have while using the system in real life. In this work, we measure the usability considering various standardized

aspects [36]: **effort expectation**(perceived ease of use), **anxiety**, **behavioral intention to use the system**, **attitude towards using technology**, **performance expectancy**, and **perceived security**. Our expectation is to observe significant benefits of mobile-based SPA systems regarding effort expectation, attitude towards using technology, and perceived security compared to the 2FA counterpart. On the other hand, we do not expect to see a significant difference in behavioral intention to use the system and anxiety. While it is not the main goal of our usability study, we also provide some average success and failure metrics but leave precise timing-related measurements as future work. **Our contributions** can be summarized as follows:

1. We implement a unique and state-of-the-art mobile device based single password authentication system (mobile SPA method of [4], see also Appendix A).
2. We conduct a comparative usability study of this mobile-based SPA solution for the first time[3] in the literature against its commonly-employed counterpart authentication system: two-factor authentication.
3. We provide our findings based on both quantitative and qualitative data. We discuss the advantages that the mobile-based SPA system provides relative to an existing commonly-employed 2FA solution. While we did not observe any disadvantages, we include important recommendations for possible deployment of a mobile SPA system in practice.

Scope of the Work: SPA systems could be mobile-based and/or cloud-based depending on the employed storage provider(s). Their security guarantees were already analyzed in their respective papers. In our study, we focus on various usability aspects and the perceived security of a mobile-based SPA system. Additionally, our analysis ends up with some suggestions that can be applied to all SPA systems in general (e.g., password reset in SPA system, see Section 4.1).

Our study is conducted at a laboratory environment using fake websites because Acar et. al [4] method requires changes at the server-side, which makes it impossible to conduct the study on real online banking sites (see Section 3 for the details of our methodology and a discussion of the limitations).

This study is the first study comparatively analyzing a unique state-of-the-art mobile-based SPA solution (namely the Acar et al. [4] work) against a commonly-employed 2FA solution. Both constructions that we analyzed are similar in the sense that the users experiences are alike (e.g., a token generation via the mobile device in addition to the user's password).

2 Related Work

We explain studies exploring usability of various authentication systems.

Traditional Password Authentication: In these schemes, the username and the output of a deterministic function (e.g., hash) of the password is stored at the server. For authentication, the user types her username and password,

[3] The only previous work on mobile SPA usability compared SPHINX mobile-based SPA system against password managers [28], and hence their work is complementary and incomparable.

and the server compares this information against its database. The user has to remember the corresponding password for each server registered with. This approach is vulnerable to offline dictionary attacks and the effect of these attacks increases dramatically if the user uses the same password for multiple servers, which is common in practice [16]. SPA systems, on the other hand, ensure security even under server database compromise. [37] discussed the traditional password authentication usability. [37] provided a quantitative point of reference for the difficulty of remembering random passwords, which is necessary to employ traditional solutions securely.

Two-Factor Authentication (2FA): These schemes generally employ any combination of two of what you know (e.g., password), what you have (e.g., token), who you are (e.g., biometric), and who you know (see [12, 34]). 2FA aims to strengthen the security of traditional password authentication by deploying a secondary authentication token (e.g., SMS sent to mobile device). To pass the authentication, the user needs to provide a valid password and token. Despite the widespread use in banking, these systems still suffer from users' negative influence such as reusing the same password. [14] conducted a comparative study of the usability of two-factor authentication technologies, where they found that 2FA is perceived as usable, regardless of motivation or use. [17] showed that 2FA provides more security but lower level of usability. [33] proposed a 2FA solution, where they found their system is reliable and usable. [27] analyzed different communication channels in 2FA (e.g., QR code, bluetooth). They concluded that their full bandwidth WiFi to WiFi system provides the highest security and usability when a browser extension and radio interface exist. [21] proposed a different 2FA called Sound-Proof to reduce the communication between the user and device. It authenticates the user based on proximity to a mobile device. Their user study concluded that their new system was more usable than the Google Authenticator application. Another 2FA is the FIDO Alliance and the protocol proposed by them Universal 2nd Factor protocol (U2F) [30]. The U2F is currently implemented by security keys (a piece of hardware authenticating the user after pressing a button on the key [23]). [26] conducted a user study on a U2F security key called YubiKey comparing it with 2FA for non-experts. They discovered that the setup phase is unusable and suggested an improvement on the design.

Single Password Authentication (SPA): SPA systems (first shown by [4] (with their patent application dating 2010 [7]), [8], [20], [28], and [18]) ensure provable security even when the user re-uses the same password on multiple sites. SPA methods achieve this by introducing an additional party to store a secret (e.g., mobile device). Similar to 2FA, the attacker also needs to guess the user's password, and additionally access the secret storage device (essentially the mobile device of the user). But, differently from 2FA, in SPA systems, when any one of the parties (i.e., storage provider and login server) is compromised, the user's single password is still kept secure from attackers. Compared to 2FA, SPA solutions provide provable security against all the aforementioned attacks.

SPHINX [28] is a mobile-phone-based SPA solution that uses cryptographic tools to ensure password security against the aforementioned attacks, whose usability was analyzed in the same paper. It is efficient, relatively simple to use, and provides better security capabilities compared to password managers, such as security in the case of mobile device compromise. Similarly, Acar et al. [4] mobile-based SPA solution is also secure in such a case, but has a different design goal: SPHINX ensures that the password is input to the client computer and not the mobile device, whereas Acar et al. intentionally use the mobile device for inputting the password, rather than the computer (considering a potentially malware-infected public terminal scenario). Since the usability of SPHINX is already examined in [28], we studied the Acar et al. [4] mobile-based SPA solution in this paper, which does not require client-side browser extension installation that SPHINX requires (useful for public terminal scenarios). We compare it against 2FA commonly used for online banking because both approaches employ a random one-use challenge via the mobile device, in addition to the password.

[19] proposes an SPA framework and suggests various secure SPA systems based on different cryptographic building blocks. It would be useful to study if a low entropy password can be replaced with other authentication mechanisms such as biometrics. We leave such an analysis as future work.

3 Methodology

Our tests were conducted in the Koç University's Media and Visual Arts Lab, and the methodology was reviewed and approved by the university ethics committee (IRB). Written consent of the participants were taken, and the questionnaire data was kept anonymous. We took precautions according to the European Union General Data Protection Regulation [1] and local data protection laws [2, 3] to protect personally-identifiable information of the participants. We did not collect such information unnecessarily, and used the names only for the consent forms. We gifted each participant with a mug with the logo of our research group on it. Each participant was allocated a 30-minute time slot.

Demographics: Before conducting the study, participants were first asked to complete an online demographics and technical background questionnaire, whose data is kept anonymous, where they were given a general idea about single password authentication. In addition to sex, age interval, and education level, the users were also asked about their experience with mobile and online banking, password managers, and whether or not they have prior knowledge of password security (see Table 1). Based on the information provided, there were 25 participants[4] (11 male, 14 female) with an age distribution: 18-25 years (6 users), 25-35 years (15 users), 35-45 years (1 user), 45-55 years (1 user) and 55+ years (2 users). The participants had diverse educational backgrounds such as post-graduate (10 users), graduate (7 users), undergraduate (6 users), and high-

[4] Despite the fact that deciding how many participants are needed for the user study remains vague, [15] justifies that even 20 users can be enough to have certainty on finding the usability problems in the testing.

school (2 users) degrees. They were university students, faculty, and staff from various departments (both technical and non-technical).

Table 1. Responses of the participants regarding technical information

How often do you use your mobile device?		**Do you have prior knowledge of password security?**	
So often (Daily)	24	I heard from news, social media etc.	16
Few times in a day	1	I had a course	6
Weekly	0	Not me but someone I know had experience	3
How often do you use mobile banking?		**How often do you use online banking?**	
Daily	4	Daily	4
Weekly	11	Weekly	9
Monthly	5	Monthly	7
Rarely	0	Rarely	3
Never	5	Never	2
Have you ever used a browser extension?		**Have you ever used a password manager?**	
Yes	16	Yes	4
No	4	No	17
Never Heard	5	Never Heard	4
How often do you change your password?			
Weekly	1	Monthly	4
Every 3 months	4	Every 6 months	2
Once a year	0	If I have to	14

3.1 Study Design

At the beginning of the study, the participants were provided with a ready setup: a pre-installed desktop computer[5] and an Android mobile phone[6]. For mobile-based SPA, we used our own SIM card and configured our servers to send SMS messages to our number using NEXMO online service; hence, we did not need to collect participants' phone numbers. For the 2FA implementation, we used Google authenticator[7] to provide the smart codes the server asks for, as it is a commonly-employed and well-known app. We did not enforce the participants to install the mobile-based SPA application and Google Authenticator from scratch, since their setup is the same as a regular mobile application installation.

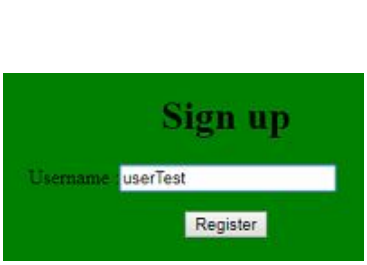
In our study, the pre-determined tasks were carefully constructed to preserve the reality as much as possible, though we accept that this is a lab study and therefore our findings should be interpreted as an important first step, rather than the final verdict. For our user study, the participants did not need any

[5] A desktop computer running 64-bit Windows 8 on Intel Core i7-3770 3.4 GHz CPU and 16 GB RAM.

[6] A Samsung Galaxy J1 with Android version 4.4.4.

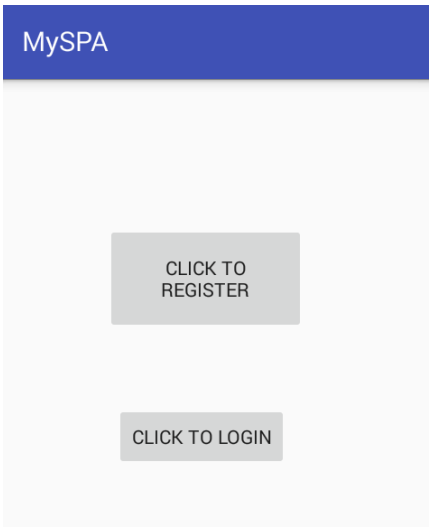
[7] Google Authenticator Android app. https://goo.gl/Q4LU7k

training to use the system as they will not in real life. Since the mobile-based SPA solution requires server-side changes, we created our own websites just for the purposes of the study. Three websites created were framed as *online banking sites*. This choice was intentional: 2FA is widely employed for online banking (among the participants 80% employed mobile banking and 92% employed online banking). No website had any data; we just created registration and login pages, and displayed success or failure messages. The only information these websites collected were usernames and (hashed) passwords (which were deleted after data evaluation was completed), and success/failure logs, for this study.

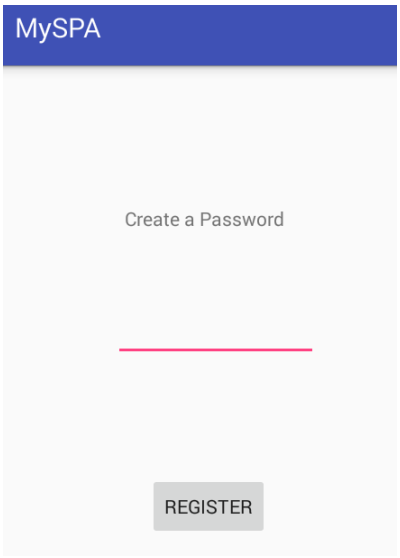


(a) Server site registration page

(b) Registration QR code



(c) Mobile application main page



(d) Password creation

Fig. 1. Mobile-based SPA registration screenshots.

The participants were presented with the aforementioned three online-banking type websites (e.g., Bank A), and were asked to register with and login to these websites using the mobile-based SPA technique and separately using the 2FA. The order of which password authentication system a participant started with was random, where either they began with 2FA and then continued with

mobile-based SPA, or vice versa. Per technique, after registering with the three websites in random order, they logged in to these websites in random order. If a participant failed to login to a website three times, we counted it as a login failure and asked user continue to login to the next website. This represented a realistic scenario where if a user enters an incorrect password three times, the user is asked to go through a CAPTCHA process or the user's account is blocked temporarily. The tasks followed by the participants in each authentication technique are described as follows:[8]

Two-Factor Password Authentication Registration: The user

1) selects a strong[9] password, where they are asked to choose a different password for each website, [**Remark:** Ideally users are expected not to use a password for more than one website for security[10], and previous studies show that an average user has approximately 7 unique passwords [16]. The username may be chosen the same or differently for each website.]
2) types her username and password, 3) clicks the signup button,
4) opens Google Authenticator app, 5) scans the QR code, 6) confirms 6 digit numerical code with the website,
7) is informed whether the registration is successful or not.

Two-Factor Password Authentication Login: The user

1) types her username and password on the server site,
2) is shown a message by the server site to type the code generated by Google Authenticator if the user types the correct username and password.
3) opens the Google authenticator application on the phone,
4) types the application-generated six-digit numerical code to the site,
5) is informed whether the login attempt is successful.

Mobile-based SPA Registration: The user

1) selects a strong[9] password, where the participant is told to use the *same* password during all three account registrations,
2) types her username (Fig. 1(a)), 3) presses the signup button,
4) opens mobile-based SPA application on the phone as it is told on the site,
5) clicks the register button on mobile-based SPA application (Fig. 1(c)),
6) scans the QR code shown on the website (Fig. 1(b)),
7) types her password on the mobile application (Fig. 1(d)),
8) clicks the register button on the mobile application,
9) is informed whether the registration is successful.

Mobile-based SPA Login: The user

1) types the username on the website (Fig. 2(a)),

[8] Note that the list of tasks were not given to the participants; instead, such instructions were clarified on the web pages and mobile applications that we created (see, for example, Figure 2(d)). The users simply followed those instructions.

[9] One with at least eight characters containing at least one of each category: lower case and upper case letters, numerical character, and special character.

[10] 2FA does not protect the user password against dictionary attacks when the password database is compromised. Therefore, such an attacker may impersonate the user on other websites that do *not* employ 2FA. Such offline dictionary and impersonation attacks are prevented by SPA systems.

2) is shown on the website that an SMS code is sent to the mobile phone and should open SPA mobile application,
3) opens the mobile application and clicks the login button (Fig. 1(c)),
4) types the single password on the mobile application (Fig. 2(b)),
5) types the 8-digit alphanumeric code displayed by the mobile application to the website (Fig. 2(d)), [**Remark:** The application automatically retrieves the SMS code and generates the code for the user; the user did not need to type SMS into the application (Fig. 2(c)).]
6) is informed whether the login attempt is successful.

3.2 Measures

We measure usability considering various standardized aspects from [36] as in various studies [14, 26, 28, 31] and added some SPA-specific questions. To collect the data for observation, we had two different methods:

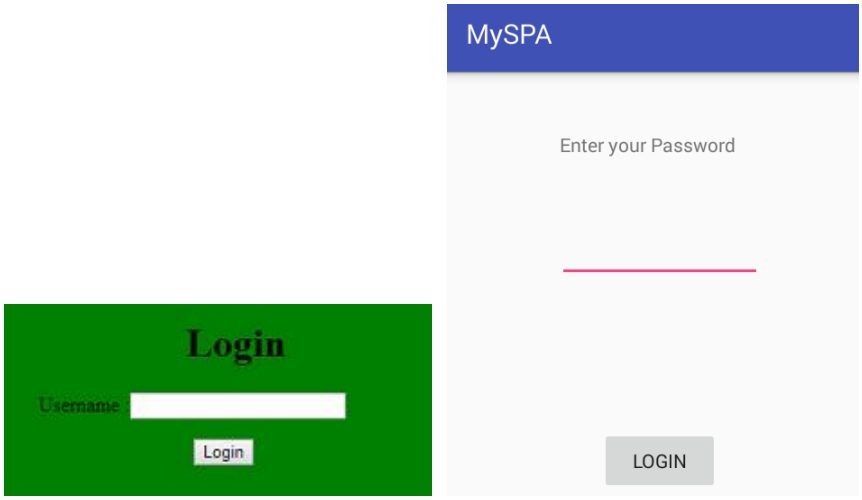
Post-questionnaire: Measures from the post-questionnaire were 4-point Likert-scale (strongly disagree, disagree, agree, strongly agree)[11]. Participants answered 23 questions per phase (e.g., 23 questions once they completed the two-factor authentication phase and 23 questions after completing the mobile-based SPA phase). We followed the standard questions in [36] because it is a commonly used standardized questionnaire measuring system usability, and added single-password specific questions ourselves to measure the perceived security, where we were inspired by previous work on password usability [9, 13, 28]. The questions in the post-questionnaire formed six sets that considered different aspects of the systems: **effort expectation**, **anxiety**, **behavioral intention to use the system**, **attitude towards using technology**, **performance expectancy**, and **perceived security** (see Table 2). For quantitative evaluation, we first converted the participants' responses to their numerical values from 1 to 4. For each aspect, we then calculated means, standard deviations, and t-test values based on the numerical values of users' responses. Dependent t-test (paired t-test)[12], which is common in usability studies on password authentication systems [13, 22, 24], is applied to compare the systems, since each participant tested both systems (mobile-based SPA and two-factor authentication).

Comments to the observer: There was an observer in the room who observed the user actions and received feedback from each participant. Since it is important not to give any additional information influencing the participants' actions, the observer provided the same standard information to all participants. At the end of the study, the observer had a discussion with each participant, where the users freely commented about their feelings and concerns about the studied systems, as well as password and system security in general.

Limitations: Our results were limited by the self-reported nature of surveys and natural selection bias. Since our experiments were held in a laboratory

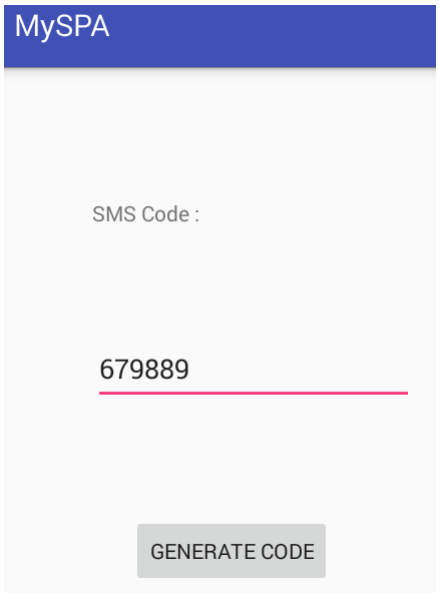
[11] We intentionally used 4-point Likert scale as it allows accounting for exact responses [5, 6].

[12] [25] argues that parametric statistics can be used with Likert data without reaching to the wrong conclusion.

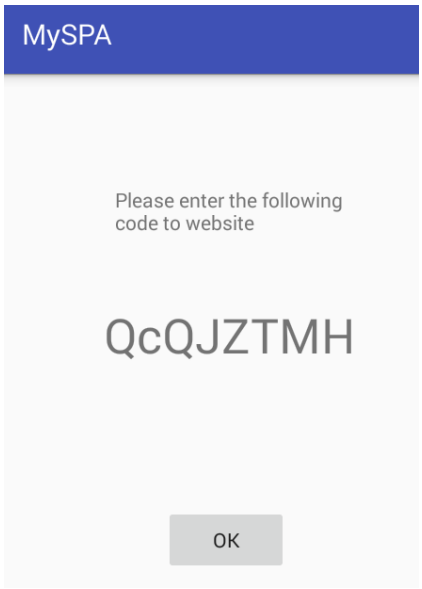


(a) Login page

(b) Password entrance



(c) SMS code



(d) Generated smart code

Fig. 2. Mobile-based SPA login screenshots.

setting using prototype implementation (mobile-based SPA Android application and the simple websites), the participants may not have behaved the same as they would in the real world. One would hope to obtain more realistic results if users could be examined in real-life, while connecting to real websites, and for a longer period of time rather than 30 minutes. Yet, this makes it very hard to conduct such a user study, especially because currently there is no deployed mobile-based SPA solution that is widely-used for online banking. Thus, we ex-

pect the reader to take our results as an important first step rather than the final verdict, and we hope to help future deployment of mobile-based SPA solutions with our discussion and suggestions based on user feedback.

Table 2. Post-questionnaire form questions asked to the participants. The form employed a 4-point scale, where 1=Strongly Disagree, 2=Disagree, 3=Agree, and 4=Strongly Agree. The group names and questions' abbreviated numbering does not exist in the actual forms the participants filled; only the questions were shown.

Effort Expectation (EE)
(EE1) My interaction with the system would be clear and understandable
(EE2) It would be easy for me to become skillful at using the system
(EE3) I would find the system easy to use
(EE4) Learning to operate the system is easy for me
Anxiety (A)
(A1) I feel apprehensive (worried) about using the system
(A2) It scares me to think that I could lose a lot of information using the system by hitting the wrong key
(A3) I hesitate to use the system for fear of making mistakes I cannot correct
(A4) The system is somewhat intimidating to me
Behavioral intention to use the system (BIU)
(BIU1) I intend to use the system in the next 6 months
(BIU2) I predict I would use the system in the next 6 months
(BIU3) I plan to use the system in the next 6 months
Attitude towards using technology (ATUT)
(ATUT1) Using the system is a good idea
(ATUT2) The system makes work more interesting
(ATUT3) Working With the system is fun
(ATUT4) I like working with the system
Performance Expectancy (PE)
(PE1) I would find the system useful in my job
(PE2) Using the system enables me to accomplish tasks more quickly
(PE3) Using the system increases my productivity
(PE4) If I use the system, I will increase my chances of getting a raise
Perceived Security (PS)
(PS1) I trust my password with this system
(PS2) I feel secure using this system for daily use
(PS3) I feel secure using this system for online banking
(PS4) I feel secure reusing the same password for multiple sites employing this system

4 Results

Below, we provide a comparative analysis based on: 1) the statistical significance using t-test, 2) quantitative response data such as mean and standard deviation

values, 3) the range of responses, 4) number of login attempts until success or failure (Table 3), and 5) observations from users' comments.

Considering the range of responses, the majority of the participants (more than 50% per question) agreed (or strongly agreed) that mobile-based SPA is easy to use, useful, trustworthy, and not intimidating to use, as well as they have a positive attitude towards and intention to using this system. This holds for all 20 questions out of 23 asked. The three questions that the majority did not agree were *"I plan to use the system in the next 6 months"* (**BIU3**), *"Using the system increases my productivity"*(**PE3**), and *"If I use the system, I will increase my chances of getting raise"* (**PE4**). This holds for both the mobile-based SPA and two-factor authentication responses, since the participants did not feel like an authentication system is tied to their salary or productivity.

As for the usability of mobile-based SPA compared to two-factor authentication, we found significant differences in terms of three dimensions: **anxiety**, **perceived security**, and **attitude towards using technology**. There was no significant difference between mobile-based SPA and 2FA regarding **effort expectancy** ($t(24) = 1.10$ and $p = 0.28$), **behavioral intention to use the system** ($t(24) = 0.00$ and $p = 1.00$), and **performance expectancy** ($t(24) = 1.04$ and $p = 0.30$).

Anxiety: Mobile-based SPA was less threatening than two-factor authentication ($t(24) = 2.77$ and $p = 0.01$). 70% of the comments (14 out of 20 participants who commented) stated that the participants were not worried while using mobile-based SPA because they typed the password on their mobile phone (conceived as a personal device) rather than the website. 96% of the participants (24 out of 25) were not scared to lose a lot of information by hitting the wrong key in mobile-based SPA. A participant explained that there was nothing to worry, since he did not give any important information to the websites.

Perceived Security: 80% of the participants (20 out of 25) felt secure while using mobile-based SPA based on the range of responses. The users trusted mobile-based SPA more than they trust 2FA ($t(24) = 3.25$ and $p = 0.003$), including all sub-statements. 80% of the comments (16 out of 20 participants who commented) stated that typing the password on the mobile device (conceived as a personal item) made the user feel more secure, whereas they needed to type their passwords on the websites in standard 2FA. One participant commented that seeing all works (computations) carried out on the mobile device made her feel more secure, and she felt as though she had the control of her password security, since she could see the steps (e.g., SMS challenge, smart code generated). Another participant pointed out that he was aware of the danger if he used the same password for multiple websites, just as 56% of participants (14 out of 25) agreed that they would feel insecure to use the same password for multiple websites in password-based authentication.

Attitude towards using technology: Mobile-based SPA performed statistically significantly better compared to 2FA ($t(24) = 2.71$ and $p = 0.01$), including all sub-statements. The users are required to remember only a single password and used it all the time, while they need to remember each one of the

Table 3. Mobile-based SPA (SPA Mobile) and 2FA (Two Factor): The percentage distribution of password attempts to login. μ: mean, σ: standard deviation.

	Login Trial		**Success Percent at Trial Number**			
	μ	σ	1	2	3	Failure(%)
SPA Mobile	1.00	0	100	0	0	0
Two Factor	1.17	0.5	82	5	4	9

passwords in the two-factor approach. One of the participants stated that she found two things she wanted at the same time, which are usability (easing her job by remembering one password) and more security (via employing a personal device and challenge).

Even though mobile-based SPA and 2FA did not have a significant difference regarding **effort expectation**, 80% of the participants (20 out of 25) agreed that mobile-based SPA was easy to use. The users reported a high satisfaction with mobile-based SPA, even though the tasks of the mobile-based SPA study were a little bit more complex (such as typing an 8-character alphanumerical code versus a 6-digit numerical code in the 2FA). 84% of the participants (21 out of 25) found that the mobile-based SPA is easy to learn, and they were fine with the steps they need to follow, since it was for online banking.

Success/Failure Rates: We measured that 100% of the time the participants successfully remembered their passwords without any trials using mobile-based SPA. Therefore, the average number of password attempts by a user is 1 (see Table 3). However, we measured a 20% overall login failure rate, due to the participants' inability to type the correct authentication code within 3 attempts. This indicates that simpler smart codes should be employed in the future.

For 2FA, we measured that 82% of the time the participants successfully remembered their passwords at the first attempt, out of which 91% of the time the participants could enter the authentication code (generated by the Google Authenticator) at their first attempt and 9% of the time at their second attempt. 5% of the time the participants remembered their passwords at their second attempt, out of which 80% of the time the participants could enter the authentication code at their first attempt and 20% of the time at their second attempt. 4% of the time the participants remembered their passwords at their third attempt, out of which 67% of the time the participants could enter the authentication code at their first attempt and 33% of the time at their second attempt. 9% of the time the participants did not remember their passwords within the first three attempts, resulting in a login failure. The average number of password attempts by a user is 1.17 (see Table 3).

We conclude that for both 2FA and mobile SPA, the participants had high login success rates. Using mobile-based SPA, the participants did not have problems with the password, but they had issues with the smart codes. On the other hand, using 2FA, the users did not have problems with the authentication codes, but they had issues remembering the password. We deduce that simpler smart

codes should be employed in such systems, as they may make things as bad as remembering passwords.

4.1 Further Discussion

The participants mentioned valuable statements and discussed their habits while creating, securing, and recalling the passwords. [16, 32, 35] observe how users manage, create, and secure their passwords and points out some challenges users face such as password creation (with the intent of reuse) and recall in traditional password authentication schemes. We observed how an SPA method overcomes some of the challenges users face.

Password Creation and Recall: 88% of the study participants (22 out of 25) were aware of password security. 85% of the comments (17 out of 20 participants who commented) stated that the participant always struggled while coming up with a password satisfying the requirements (e.g., at least one lowercase and one uppercase letter, a number, and a special character). The participants usually came up with a password after a number of trials. Once they created it, remembering the password was another struggle they bear. Thus, they created their own way to recall the passwords. More than 50% of comments (10 out of 20) noted that the participants wrote down their passwords to remember. One of the users commented that he stored password reminders (as hints helping him to recall the passwords) in a file, while he emphasized that anyone who obtained the file could not learn the passwords. When we questioned why he needed this storage, he responded that it is hard for him to remember the password for some sites he rarely used and he came up with this solution. However, even this solution did not stop him from re-using the same password for multiple sites.

Password Reset: While there is a functionality to reset a password in traditional approaches, a participant found it cumbersome, since the password reset procedure requires steps such as logging in to a backup e-mail, which requires remembering another password, or memorizing and entering all necessary information (such as security questions) to reset. Another participant shared his experience when he lost the paper where he noted a password for a site and wanted to reset the password. Unfortunately, he needed to follow a long official password reset procedure because of system requirements (e.g., personal application was required and he waited for a week). He stated that everything would be easier if he could use a secure SPA system that minimizes password remembering problems. As in password creation and recall discussion, similar comments support that SPA systems are easing the burden on users by requiring them to remember only one password (in addition to the cryptographic benefits they provide such as provable security against offline dictionary attacks). In the light of these comments, we recommend that the SPA systems should investigate how a secure single password reset can be efficiently carried out.

Widespread Use: While this idea might require further and detailed research all by itself, users may feel more secure when a new system is collectively used. 52% of the participants (13 out of 25) shared that they would use the SPA

system and trust it if it is commonly used and advertised by a "trusted" authority (rather than university researchers) such as Facebook, Google, etc. One of the participants said that *"I feel secure while I am using WhatsApp, since WhatsApp is employed for secure messaging. They use something like encryption."* The participant was not aware of the cryptographic scheme employed in WhatsApp and had no idea what it was, but stated that it "feels" secure since WhatsApp was widely advertised and employed.

Complexity of the Solution: We found some insights about online banking which is commonly used for financing [29]. 90% of the comments (18 out of 20 participants who commented) stated that mobile-based SPA provided a better security for online banking, and users felt secure in the online banking scenario because it was "complex" enough. Interestingly, the participants stated that a "complex" solution using the mobile device (i.e., mobile-based SPA) feels secure for banking since the password is typed on the phone. On the other hand, the mobile-based SPA system was found unproductive for email type daily purposes due to its complexity, while it was considered more secure by the participants. Considering such feedback on security and usability, there might be an inverse relationship between the perceived security and ease of use, since mobile-based SPA was found more secure for online banking. This interpretation is worth exploring for future research.

Our user study concluded that SPA systems provide usability benefits. The main reasoning is that it is not convenient to expect users to create different complex passwords for each website and remember them. While this approach would be secure, it is not usable. On the other hand, SPA systems enable single password re-use securely.

5 Conclusion, Recommendations, and Future Work

We implemented mobile-based single password authentication method of [4] and conducted its usability analysis for the first time. It has two unique properties apart from being the first such proposal: it can be implemented as only a mobile application, and it protects the user's password from malware-infected computers at public locations. We compared it against 2FA in a fake online banking scenario. Quantitative and qualitative results support that the mobile-based SPA solution has usability and security advantages compared to its counterpart.

Our findings suggest that the smart code mechanism should be simpler and the SPA branding should provide more trust to the users. Based on the feedback reported by the participants, we suggest that mobile-based SPA solution(s) should be deployed for online banking type of settings, where more complicated solutions are expected (at least seemingly more complicated, regardless of the underlying cryptography). Observations also indicate that there is potentially a trade-off between usability and perceived security, which is worth exploring as future work.

We believe our study constitutes an important step in understanding the usability of SPA systems regarding their future deployment. Yet, to obtain more generalizable results, we recommend to conduct future studies taking into account timing information, taking place in a natural settings instead of a lab

environment and examining other dimensions of user experience of SPA systems beyond usability such as emotional satisfaction, increasing the number of participants, and considering privacy of SPA systems.

Acknowledgements

We thank İlker Kadir Öztürk and Arjen Kılıç for their efforts on implementation. This work has been supported in part by TÜBİTAK (the Scientific and Technological Research Council of Turkey) under the project number 115E766, by the Royal Society of UK Newton Advanced Fellowship NA140464, by ERC Advanced Grant ERC-2015-AdG-IMPaCT, and by the FWO under an Odysseus project GOH9718N.

References

1. European Union General Data Protection Regulation 2016/679 (GDPR), 2016.
2. Turkish Personal Data Protection Law no. 6698 (KVKK), 2016.
3. Turkish Personal Data Deletion and Anonymization Regulation no. 30224, 2017.
4. T. Acar, M. Belenkiy, and A. Küpçü. Single password authentication. *Computer Networks*, 2013.
5. I. E. Allen and C. A. Seaman. Likert scales and data analyses. *Quality progress*, 2007.
6. K. C. Behnke, Andrew O. Creating programs to help latino youth thrive at school: The influence of latino parent involvement programs. *Journal of Extension*, 2011.
7. M. Belenkiy, T. Acar, H. Morales, and A. Küpçü. Securing passwords against dictionary attacks. 2015. US Patent 9,015,489.
8. K. Bicakci, N. B. Atalay, M. Yuceel, and P. C. van Oorschot. Exploration and field study of a browser-based password manager using icon-based passwords. In *RLCPS*, 2011.
9. K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, and N. Atalay. Graphical passwords as browser extension: Implementation and usability study. *Trust Management III*, 2009.
10. L. F. Bicchierai. Another day, another hack: 117 million linkedin emails and passwords. 2016. `https://bit.ly/2Nq1b9M`.
11. L. F. Bicchierai. Hacker tries to sell 427 milllion stolen myspace passwords for $2,800. 2016. `https://bit.ly/2GBnu9S`.
12. J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-factor authentication: somebody you know. In *ACM CCS*, 2006.
13. S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, 2006.
14. E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie. A comparative usability study of two-factor authentication. In *NDSS USEC*, 2014.
15. L. Faulkner. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behavior Research Methods, Instruments, & Computers*, 2003.
16. D. Florencio and C. Herley. A large-scale study of web password habits. In *ACM WWW*, 2007.

17. N. Gunson, D. Marshall, H. Morton, and M. Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 2011.
18. D. İşler and A. Küpçü. Threshold single password authentication. In *ESORICS DPM*. 2017.
19. D. İşler and A. Küpçü. Distributed single password protocol framework. Cryptology ePrint Archive, Report 2018/976, 2018. `https://eprint.iacr.org/2018/976`.
20. S. Jarecki, H. Krawczyk, M. Shirvanian, and N. Saxena. Device-enhanced password protocols with optimal online-offline protection. In *ACM ASIACCS*, 2016.
21. N. Karapanos, C. Marforio, C. Soriente, and S. Capkun. Sound-proof: usable two-factor authentication based on ambient sound. In *USENIX*, 2015.
22. A. Karole, N. Saxena, and N. Christin. A comparative usability evaluation of traditional password managers. In *ICISC*, 2010.
23. J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas. Security keys: Practical cryptographic second factors for the modern web. In *FC*, 2016.
24. D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot. Tapas: design, implementation, and usability evaluation of a password manager. In *ACSAC*. ACM, 2012.
25. G. Norman. Likert scales, levels of measurement and the "laws" of statistics. *Advances in health sciences education : theory and practice*, 2010.
26. J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons. A tale of two studies: The best and worst of yubikey usability. In *IEEE SP*, 2018.
27. M. Shirvanian, S. Jarecki, N. Saxena, and N. Nathan. Two-factor authentication resilient to server compromise using mix-bandwidth devices. In *NDSS*, 2014.
28. M. Shirvanian, S. Jareckiy, H. Krawczykz, and N. Saxena. Sphinx: A password store that perfectly hides passwords from itself. In *IEEE ICDCS*, 2017.
29. S. Smith. Digital banking users to reach 2 billion this year, representing nearly 40% of global adult population. 2018. `https://bit.ly/2GPRhdE`.
30. S. Srinivas, D. Balfanz, E. Tiffany, and A. Czeskis. Universal 2nd factor (u2f) overview. *FIDO Alliance Proposed Standard*, 2015.
31. E. Stobert and R. Biddle. The password life cycle: user behaviour in managing passwords. In *ACM SOUPS*, 2014.
32. E. Stobert and R. Biddle. The password life cycle. *ACM TOPS*, 2018.
33. H.-M. Sun, Y.-H. Chen, and Y.-H. Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE TIFS*, 2012.
34. S. Taheri-Boshrooyeh and A. Küpçü. Inonymous: Anonymous invitation-based system. In *ESORICS DPM*, 2017.
35. B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. "I added '!' at the end to make it secure": Observing password creation in the lab. In *USENIX SOUPS*, 2015.
36. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 2003.
37. M. Zviran and W. J. Haga. A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, 1993.

A Mobile-based Single Password Authentication Scheme of Acar et al. [4]

We briefly present Acar et al. [4] mobile-based SPA solution here for completeness. In their mobile-based SPA, there are three parties; a user holding a pass-

word *pwd*, a trusted mobile device of the user, and a server, with which the user wishes to register. The protocol is roughly as follows:

Registration:

1. The **user**:
   - generates a Message Authentication Code (MAC) key K.
   - sends the key K and her username UID to the server.
   - encrypts the MAC key K where the encryption key is derived using the hash of her password $H(pwd)$ as $ctext \leftarrow Encrypt(H(pwd), K)$. [**Remark:** The user also sends an identifier with ciphertext.]
2. The **trusted mobile device** stores the ciphertext $ctext$.
3. The **server** stores the username UID and the MAC key K.

Authentication:

1. The **user** sends her username UID to the server.
2. The **server** generates a random challenge *chal* and sends it to the mobile device. [**Remark:** The server can send the challenge in various ways such as via SMS, or via a QR code where the user scans the code with her mobile device.]
3. The **user** types her single password on the mobile device.
4. The **trusted mobile device:**
   - decrypts the ciphertext and retrieves the MAC key K as $K \leftarrow Decrypt(H(pwd), ctext)$.
   - generates a MAC $resp$ as a response to the challenge *chal* using the retrieved key K as $resp \leftarrow MAC(K, chal)$. [**Remark:** To resist man-in-the-middle attacks, as [19] notes, preferable usage is $resp \leftarrow MAC(K, chal||domain)$.]
   - applies trimming function $Trim$ on the generated response $resp$ to get a short one-time code/password $resp'$ as $resp' \leftarrow Trim(resp)$.
5. The **user** types the short one-time code $resp'$ on the user machine and sends it to the server.
6. The **server** checks if the $resp'$ is generated based on a valid MAC of the challenge *chal* with the corresponding user MAC key K in his database as $Trim(MAC(K, chal)) \stackrel{?}{=} resp'$.
7. The **server** informs the user whether the login attempt is successful or not.