User Study on Single Password Authentication

Devriş İşler, Alptekin Küpçü, and Aykut Coskun

Koç University
İstanbul, Turkey
{disler15,akupcu,aykutcoskun}@ku.edu.tr

Abstract. Single password authentication (SPA) schemes are introduced to overcome the challenges of traditional password authentications, which are vulnerable to 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 offline dictionary attacks in a provably secure manner. Several cryptographic SPA solutions were proposed in this decade, some based on cloud storage, and some employing a trusted personal mobile device. However, studies on usability of these novel SPA systems are rare, hardening their deployment and the validation of their practicality.

In this paper, we implement two very different SPA systems and assess their usability with the following two comparative experiments: one comparing the state-of-the-art cloud-based browser-extension SPA solution against traditional password-based authentication (where in both cases the user experience is simply entering a username and password), and another comparing the first mobile-application-based SPA solution against two-factor authentication (where, in both cases, in addition to the password, the user needs access to her mobile device). We obtain that the cloud-based SPA system is easier to use than the traditional approach, making it suitable for daily use deployment, and the mobile-based SPA system is as easy as, but less intimidating and more secure than two-factor authentication, making it a better alternative for online banking type deployments. Hence, SPA systems overall constitute a usable alternative to the existing solutions, while providing offline dictionary attack protection.

Keywords: Password authentication, usability, two-factor 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, it is common that server password databases are hacked, and millions of users are affected because their passwords are not complicated enough to resist offline dictionary attacks. The attacker aims to obtain a user password and impersonates the user on other services to perform unauthorized actions such as bank transfers. The damage of these attacks on the password becomes dramatically dangerous when the user reuses the same password for multiple sites, which is common in practice [16].

Because of the aforementioned attacks, cryptographic solutions called *single password authentication* (SPA) systems are proposed to create a secure authentication environment considering all accounts of a user and overcome the challenges of traditional password authentication system by ensuring *provable security* against these attacks.

Unlike other authentication systems, SPA systems *securely* enable a user to use *only a single password* (and a username) for all her accounts. Although SPA systems are similar to some other techniques (e.g., password managers) in terms of actions taken by users (e.g., using a single master password), the underlying cryptography employed and the security they provide are different. In SPA systems, when any one of the parties (i.e., storage provider and login server) is compromised, user's single password is provably kept secure from attackers. On the other hand, their alternatives are insecure when any one of the parties (e.g., storage in password managers) is corrupted; in such cases the user password is vulnerable to offline dictionary attacks.

The general idea of an SPA system is to generate a secret independent of the password (e.g., a random r or a key) and then store this secret protected by the user's single password at a separate storage provider (e.g., cloud storage or mobile device). The associated verification information (e.g., $hash(r||url)$ or verification key) is shared with the login server during the registration. Whenever the user wants to login to the server, the user communicates with both the storage provider and the login server. She securely retrieves the secret information from the storage provider, where the storage provider cannot learn the password, 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 reconstructed secret. SPA systems are secure unless the storage provider(s) and login server are corrupted by the same adversary.

In chronological order, [4] (with their patent application dating 2010 [7]), [9], [21], [30], and [20] are the known examples of single password authentication systems. For these cryptographically-elegant constructions to be widely deployed and accepted, their usability studies must be performed.

Until now, only the usability of Shirvanian et al. [30] mobile-phone-based password-manager-type solution was evaluated against traditional password-based authentication. In this paper, we study the usability of two other single password authentication proposals in a comparative manner. The first SPA system we study is the state-of-the-art cloud-based SPA solution proposed by İşler and Küpçü [20], since it can be simply implemented without any server-side changes and used via a browser extension. We compare their solution against traditional username-password authentication that is widely deployed today because both approaches simply require the user to follow the same steps (e.g., typing a username and password, and pressing the login button). The second SPA system we study is the first mobile-based SPA mechanism by Acar et al.

[4], since it can be implemented as a single mobile device application (unlike [30] that requires both a mobile phone application and a browser extension) and uniquely protects the user's single password against malware-infected computers. We compare it against two-factor authentication commonly used for online banking because both approaches similarly employ a random one-use challenge via the mobile device, in addition to the password.

We measure the usability considering various standardized aspects: **effort expectation** (percieved ease of use), **anxiety**, **behavioral intention to use the system**, **attitude towards using technology**, **performance expectancy**, and **perceived security** [33]. Our expectation is to observe significant benefits of SPA systems regarding effort expectation, attitude towards using technology, and perceived security compared to their counterparts. 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 two state-of-the-art single password authentication systems (cloud-based SPA solution of [20] and mobile-based SPA method of [4]).
2. We conduct a comparative usability study of these two SPA solutions for the first time in the literature against two commonly-employed authentication systems: traditional username-password authentication and two-factor authentication.
3. We provide our findings (based on both quantitative and qualitative data) on user perspective against the idea of using a single password securely. We discuss in what type of settings mobile- and cloud-based SPA solutions provide better usability.

2 Related Work

We explain various authentication systems and studies exploring their usability.

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, 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, whereas SPA systems ensure security even under server database compromise. The effect of these attacks increases dramatically if the user uses the same password for multiple servers, which is common in practice [16]. [34] discusses the traditional password authentication usability. [34] provides a quantitative point of reference for the difficulty of remembering random passwords, which is necessary to employ traditional solutions securely.

Two-Factor Authentication: These schemes generally employ any combination of two of what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric). Two-factor authentication aims to strengthen the security of traditional password authentication by deploying 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 two-factor authentication is perceived as usable, regardless of motivation or use. [18] showed that two-factor authentication provides more security but lower level of usability. [32] proposed a two-factor authentication solution, where they found their system is reliable and usable. [29] analyzed different communication channels in two-factor authentication (e.g., QR code, bluetooth). They concluded that their full bandwidth WiFi to WiFi system provides highest security and usability when a browser extension and radio interface exist.

Password Managers: In this setting, the user holds a master password to generate server-specific passwords (e.g., $hash(password||domain)$). The generated passwords are usually resistant to dictionary attacks and have high entropies. iPMAN [9] (where the master password is created based on objects), LastPass [13], PwdHash[28], Password Multiplier [19] are some examples of password manager type solutions where their usability studies are conducted as well. [12, 22, 23] compare the usability of some existing password managers, where they found that users were not comfortable with leaving the control of their passwords to a manager and did not feel that password managers provided greater security.[1] [23] also suggests that it is still a challenge for password managers to be secure. Indeed, SPA solutions remain secure even when the password-protected storage at the cloud or mobile device is compromised.

SPHINX [30] is a mobile-phone-based password-manager-type SPA solution that uses cryptographic tools to ensure password security against aforementioned attacks. It is efficient, relatively simple to use, and provides better security capabilities compared to many other 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 [30], we studied the Acar et al. [4] mobile-based SPA solution in this paper, which does not require client-side installation (useful for public terminal scenarios).

Other Techniques: Users create secure passwords based on objects (e.g., an image) using an object-based password authentication application (e.g., extension). [8, 10, 24] are some examples that provided usability studies on object-

[1] As 84% of our participants did not have any experience with password managers, we could observe the usability and security of cloud-based SPA (especially regarding user perspective on employing a single password) without being positively or negatively biased by previous password manager experience.

based passwords. [24] points that the user needs to keep the object (e.g., picture) with herself (e.g., via flash driver) to login to a site. In general, [10, 24] showed that creation of the password in object-based systems is easy to accomplish by users.

Password encoding strategies are proposed to make offline dictionary attacks ineffective [11]. Chatterjee et al. [11] introduce the notion of outputting decoy passwords to an attacker. Since the attacker does not have any idea about the correct password, any trial to login with the decoy passwords can be prevented and alerted. However, an attack presented in [17] showed that such a scheme seems to be vulnerable.

3 Usability Study

We compared the cloud-based SPA against traditional password-based authentication, and the mobile-based SPA against two-factor authentication. We implemented the cloud-based SPA solution of [20] as a Chrome browser extension that simply asks for username and password. Thus, experience-wise, this is similar to the traditional password-based authentication. We designed three email-branded websites and asked the user study participants to register with and login to these three websites using the browser extension and separately using the traditional approach. We implemented the mobile-based SPA protocol of Acar et. al [4] as an Android application that employs a challenge-response mechanism using a mobile device, where a short random string is sent by the server during authentication via SMS. This should be familiar to those who used two-factor authentication for online banking, where a bank employs such a random code for authentication purposes and a mobile device is the second factor (in addition to the password). The participants were presented with three online banking type websites, and were asked to register with and login to these websites using the mobile-based SPA technique and separately using the two-factor authentication. For two-factor authentication implementation, we used Google authenticator[2] to provide the smart codes the server asks for. Therefore, we conducted these two separate studies:

1. **Study I-** *cloud-based SPA with browser extension* and *traditional password authentication:* We implemented the protocol proposed by İşler and Küpçü [20] as a Chrome browser extension.
2. **Study II-** *mobile-based SPA* and *two-factor authentication with Google authenticator:* We implemented an Android application to represent the mobile-based SPA protocol in Acar et al. [4], and SMS is used for the challenge.

We measure the usability considering various standardized aspects: **effort expectation**, **anxiety**, **behavioral intention to use the system**, **attitude towards using technology**, **performance expectancy**, and **perceived security** [33]. We expect that both cloud- and mobile-based scenarios, SPA solutions would have significant advantages in terms of effort expectation, attitude

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

towards using technology, and perceived security compared to their counterparts. On the other hand, we do not expect to see a significant difference in behavioral intention to use the system and anxiety.

In our studies, the tasks were pre-determined as explained below (see Section 3.4), and these 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 users did not need any training to use the system as they will not in real life. Our user studies were reviewed and approved by the university ethics committee. We took precautions according to the European Union General Data Protection Regulation [1] and local data protection laws [3, 2] to protect personally-identifiable information of the participants.

3.1 Participants

We asked the participants to fill an online form to learn their demographic and technical information. Based on the information provided, there were 25 participants (12 male, 13 female) who attended Study I (browser extension vs. traditional) with a distribution to different age groups: 18-25 years (6 users), 25-35 years (13 users), 35-45 years (2 users), 45-55 years (3 users) and 55+ years (1 user). There were 25 other participants (11 male, 14 female) who attended Study II (mobile vs. two-factor) with similar 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).

For both of the studies, the participants had diverse educational backgrounds such as post-graduate, graduate, undergraduate, high-school, and primary school degrees. They were university students, faculty, and staff from various departments (both technical and non-technical). The full demographic and technical information can be found in Table 1 and Table 2, respectively. Despite the fact that deciding how many participants are needed for the user study remains vague, [15] justifies that even twenty users can be enough to have certainty on finding the usability problems in the testing.

3.2 Testing Environment

Our usability studies were conducted in the Koç University's Media and Visual Arts Lab. There was an observer in the room who observed the user actions and received feedback from each participant. As a token of appreciation, we gifted each participant with a mug with the logo of our research group on it.

We provided the participants with a ready setup: a pre-installed desktop computer[3] and an Android mobile phone[4]. We did not enforce the participants to install the browser extension and mobile applications (both mobile-based SPA

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

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

Table 1. Responses of the participants regarding demographic information.

	Study I	**Study II**
Sex		
Male	12	11
Female	13	14
Age Interval		
18-25	6	6
25-35	13	15
35-45	2	1
45-55	3	1
55+	1	2
Education Level		
Post-Graduate	10	10
Masters	7	7
Bachelor	5	6
High School	2	2
Primary school or under	1	0

application and Google Authenticator) from scratch, since mobile-based SPA mobile application setup is the same as a regular mobile application installation, and cloud-based SPA Chrome extension installation is the same as any other browser extension installation. 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.

We also created our own websites just for the purposes of the study, since mobile-based SPA solution require server-side changes and we wanted to keep logs of user actions. Three websites created for Study I were framed as *email sites*, and three websites for Study II were framed as *online banking sites*. These choices were intentional: traditional password authentication is commonly used for email type of daily purposes, whereas two-factor authentication is widely employed for 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 the purposes of this study. Each participant was allocated a 30 minute time slot.

3.3 Measures

Before conducting the study, participants were first asked to complete a 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 browser extensions and password managers, and whether or not they have prior knowledge of password security (see Table 2). We then as-

Table 2. Responses of the participants regarding technical information of Study I and Study II

	Study I	**Study II**
How often do you use your mobile device?		
So often (Daily)	23	24
Few times in a day	1	1
Weekly	1	0
How often do you use mobile banking?		
Daily	5	4
Weekly	11	11
Monthly	5	5
Rarely	0	0
Never	4	5
How often do you use online banking?		
Daily	4	4
Weekly	5	9
Monthly	10	7
Rarely	4	3
Never	2	2
How often do you change your password?		
Weekly	1	1
Monthly	2	4
Every 3 months	2	4
Every 6 months	5	2
Once a year	1	0
If I have to	14	14
Do you have prior knowledge of password security?		
I heard from news, social media etc.	18	16
I had a course	3	6
Not me but someone I know had experience	4	3
Have you ever used a browser extension?		
Yes	16	16
No	5	4
Never Heard	4	5
Have you ever used a password manager?		
Yes	4	4
No	16	17
Never Heard	5	4

signed the participants to two different studies, considering an even distribution across groups, i.e., age, sex, educational level. To collect the data for observation, we had two different methods:

Post-questionnaire: Measures from post-questionnaire were 4-point Likert-scale (strongly disagree, disagree, agree, strongly agree).[5] Participants answered 23 questions per phase (e.g., 23 questions for traditional password-based authentication and 23 questions for cloud-based SPA browser extension in Study I). We followed the standard questions in [33] 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 works on password usability [10, 12, 30]. 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 3 for questions and groups). 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)[6], which is common in usability studies on password authentication systems [12, 22, 25], is applied to compare the systems in each study, since each participant tested two systems per study (either cloud-based SPA and traditional passwords, or mobile-based SPA and two-factor authentication).

Comments to the observer: At the end of the study, the observer (the first author) had a discussion with the participants about each system they tested, where the users freely commented about their feelings and concerns such as what they felt about the systems and their password and systems security in general, their positive and negative feedback, and what they thought about using a single password.

3.4 Testing Procedure

Before the participants started the study, written signed consent of the participants were taken. We did not collect personally-identifiable information unnecessarily, and used the names only for the consent forms, which are not linkable to the anonymous post-questionnaires and comments.

Tasks of Study I: Each participant registered with three different websites (e.g., Mail A) separately using the traditional approach and the cloud-based SPA Chrome extension. The order of which password authentication system a participant started with was random, where either they began with the conventional approach and then continued with the SPA Chrome Extension, or vice versa. After registration, they logged in to the three websites in random order

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

[6] [27] discuss with various samples of testing that parametric statistics can be used with Likert data without coming to the wrong conclusion.

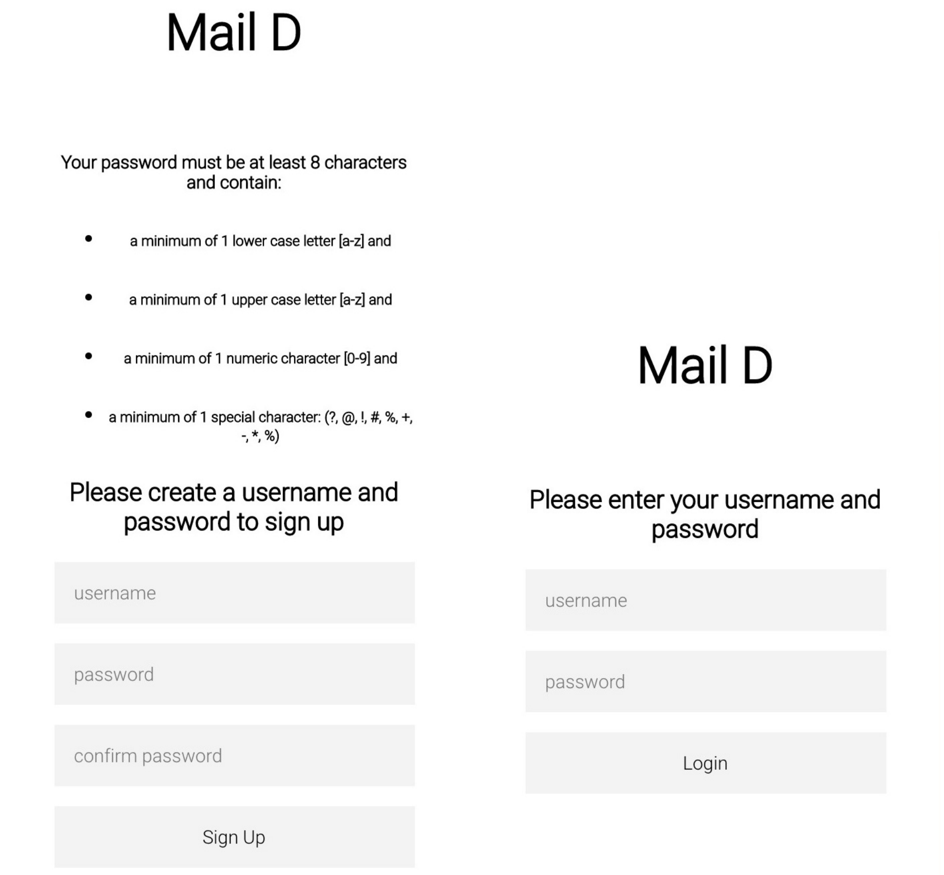
Table 3. Post-questionnaire form questions asked to the participants. The form employed a 4-point scale, where 1=Strongly Disagree, 2=Disagree, 3=Agree, and 4=Strongly Agree. The group names and questions' abbreviated numbering does not exist in the actual forms the participants filled; only the questions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

(as we pre-determined). If a participant failed to login to a website three times, we counted it as a login failure and asked the 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 users were explicitly told to behave as in their regular life as much as they could. For that reason, some participants wrote down each password they created during the test of traditional password authentication on a piece of paper (that they took away after the test), as they noted this is how they remember their passwords in their regular life. More specifically, the tasks of Study I are described as follows: **Traditional Password Authentication Registration:**

Fig. 1. Traditional authentication registration and login screenshots.



Mail D

Your password must be at least 8 characters and contain:

- a minimum of 1 lower case letter [a-z] and
- a minimum of 1 upper case letter [a-z] and
- a minimum of 1 numeric character [0-9] and
- a minimum of 1 special character: (?, @, !, #, %, +, -, *, %)

Please create a username and password to sign up

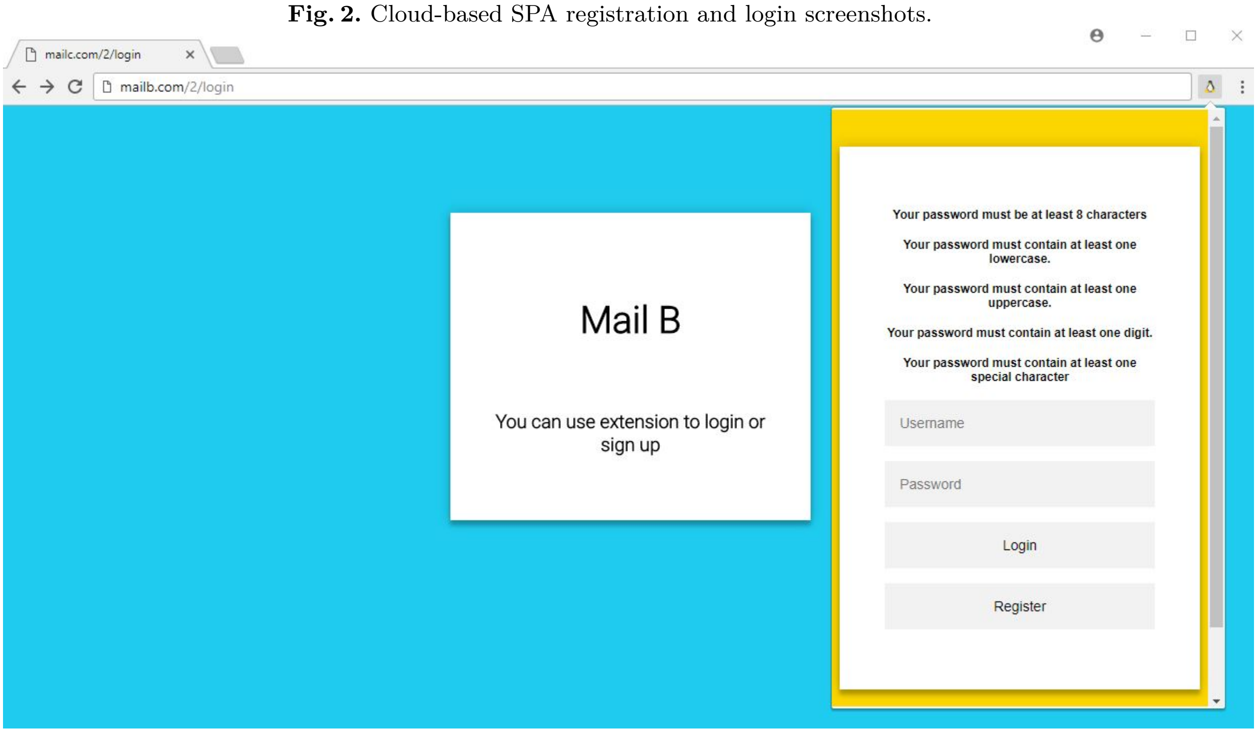
Mail D

Please enter your username and password

(a) Traditional password authentication registration page.

(b) Traditional password authentication login page.

Fig. 2. Cloud-based SPA registration and login screenshots.



You can use extension to login or sign up

Your password must be at least 8 characters

Your password must contain at least one lowercase.

Your password must contain at least one uppercase.

Your password must contain at least one digit.

Your password must contain at least one special character

The user

1. selects a strong password with at least eight characters containing at least one of each category: lower case and upper case letters, numerical character, and special character,
   Remark: The users are asked to choose a different password for each website. Ideally users are expected not to use a password for more than one website for security, 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 the password,
3. confirms the password (see Figure 2(a)),
4. presses the signup button,
5. is informed whether the registration is successful or not (e.g., password confirmation does not match).

Traditional Password Authentication Login: The user

1. types username and password (see Figure 2(b)),
2. presses the login button,
3. is informed whether the login attempt is successful.

SPA Chrome Extension Registration: The user

1. selects a strong password with at least eight characters containing at least one of each category: lower case and upper case letters, numerical character, and special character,

   Remark: The participant is told to use the same password during all three account registrations.
2. opens the extension by clicking its button next to the address bar,
3. types her username and the password into the extension (see Figure 2),
4. presses the registration button,
5. is informed whether the registration is successful.

SPA Chrome Extension Login: The user

1. opens the SPA extension,
2. types her username and password using the extension (see Figure 2),
3. presses the login button,
4. is informed whether the login attempt is successful.

Tasks of Study II: Each participant was required to separately register to three different websites (e.g., Bank A) using the two-factor authentication approach and the SPA mobile application. The order of which password authentication system a participant started with was random, where either they began with two-factor authentication and then continued with mobile-based SPA, or vice versa. After each registration, they logged in to the 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. More specifically, the tasks are described as follows[7]:

Two-Factor Password Authentication Registration: The user

1. selects a strong password with at least eight characters containing at least one of each category: lower case and upper case letters, numerical character, and special character,

   Remark: The users are asked to choose a different password for each website. Ideally users are expected not to use a password for more than one website for security[8], 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 (see Figure 4(a)),
3. presses the signup button,
4. opens Google Authenticator application on the phone (see Figure 4(b)),

[7] Note that the list of tasks were not given to the participants; instead, such instructions were clarified on the web pages, browser extensions, and mobile applications that we created (see, for example, Figure 6(d)). The users simply followed those instructions.

[8] Two-factor authentication 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 two-factor authentication. Such offline dictionary and impersonation attacks are prevented by SPA systems.

5. scans the QR code shown on the website (see Figure 4(c)),
6. types the application-generated six-digit numerical code to the site and clicks the send button,
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. opens the Google authenticator application on the phone,
3. types the application-generated six-digit numerical code to the site (see Figure 4(b)),
4. is informed whether the login attempt is successful.

SPA Mobile Registration: The user

1. selects a strong password with at least eight characters containing at least one of each category: lower case and upper case letters, numerical, and special characters,

   Remark: The participant is told to use the same password during all three account registrations.
2. types her username (see Figure 5(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,
6. scans the QR code shown on the website (see Figure 5(b)),
7. types her password on the mobile application (see Figure 5(d)),
8. clicks the register button on the mobile application,
9. is informed whether the registration is successful.

SPA Mobile Login: The user

1. types the username on the website (see Figure 6(a)),
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,
4. types the single password on the mobile application (see Figure 6(b)),
5. types the 8-digit alphanumeric code displayed by the mobile application to the website (see Figure 6(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(see Figure 6(c)).
6. is informed whether the login attempt is successful.

4 Results

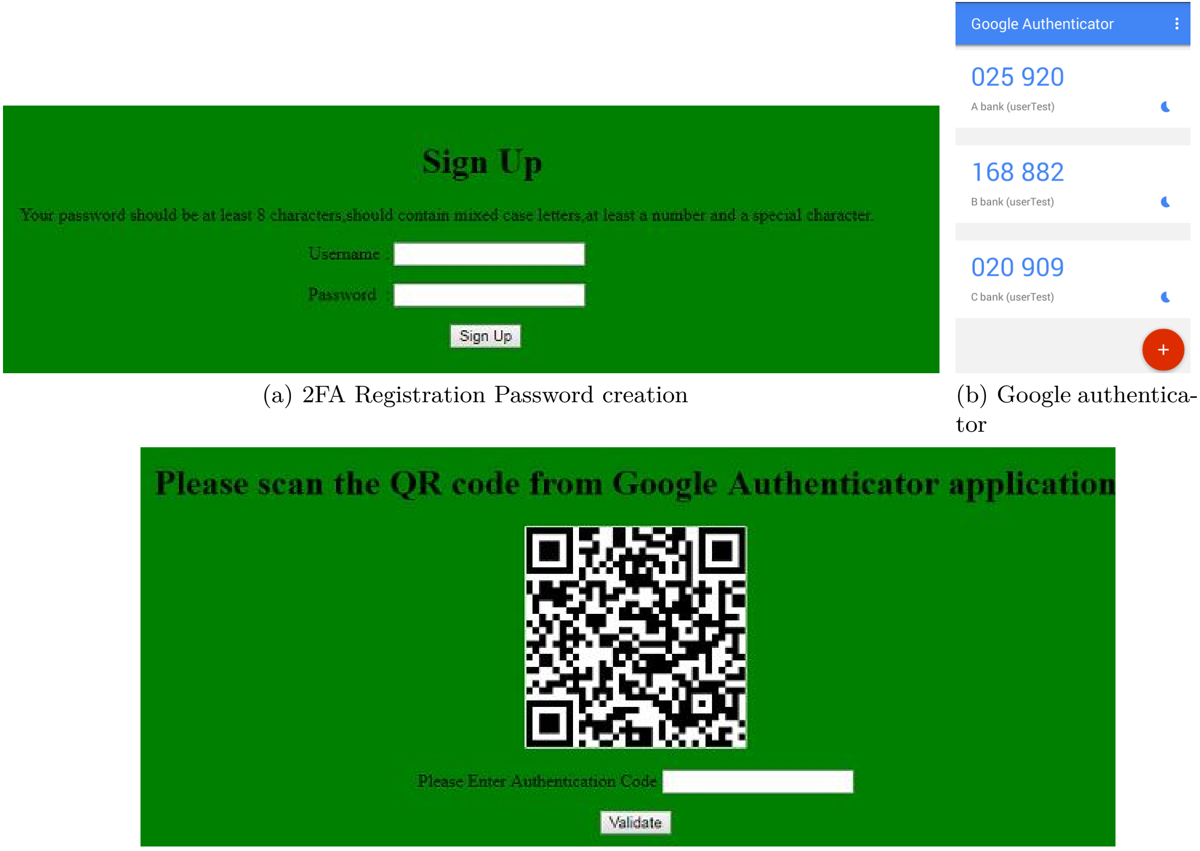
Below, we provide a comparative analysis for each study based on: 1) the statistical significance using t-test (Table 4), 2) quantitative response data such as mean and standard deviation values (Table 4) , 3) the range of responses (Table 7)[9] , 4) number of login attempts until success or failure (Tables 5 and 6), and 5) observations from users' comments.

[9] Anonymous individual responses can be found in the Appendix B for completeness.

Table 4. Post-Test Questionnaire and results for user studies on cloud-based SPA (SPA Cloud), traditional password authentication (Traditional), mobile-based SPA (SPA Mobile) and two-factor authentication (Two-Factor). Scores are out of the 4-point Likert scale employed. μ: mean, σ: standard deviation, t: t-statistic, and p: significance. Degrees of freedom are 24.

	SPA Cloud		**Traditional**		**t-test**		**SPA Mobile**		**Two-Factor**		**t-test**	
	μ	σ	μ	σ	t	p	μ	σ	μ	σ	t	p
EE	3.40	0.70	2.94	0.71	2.09	**0.04**	3.14	0.55	3.26	0.41	1.10	0.28
EE1	3.40	0.82	3.16	0.69	1.10	0.28	3.04	0.79	3.32	0.56	1.66	0.10
EE2	3.32	0.95	3.08	0.64	0.94	0.35	3.16	0.75	3.16	0.55	0.00	1.00
EE3	3.44	0.82	2.64	1.04	2.61	**0.01**	3.20	0.65	3.08	0.64	0.76	0.44
EE4	3.44	0.71	2.88	0.93	2.22	**0.03**	3.16	0.80	3.48	0.51	2.13	**0.04**
A	1.87	0.51	2.25	0.65	2.03	0.05	1.89	0.43	2.22	0.54	2.77	**0.01**
A1	1.76	0.78	2.04	073	1.13	0.27	2.00	0.71	2.24	0.60	1.29	0.20
A2	2.08	0.81	2.36	0.95	1.02	0.31	1.68	0.56	2.24	0.88	3.21	**0.003**
A3	1.84	0.75	2.32	0.82	2.21	**0.03**	1.88	0.60	2.12	0.67	1.23	0.22
A4	1.80	0.65	2.28	0.79	2.61	**0.01**	2.00	0.76	2.28	0.68	1.57	0.12
BIU	2.65	0.60	2.48	0.77	0.84	0.40	2.64	0.64	2.64	0.70	0.00	1.00
BIU1	2.80	0.65	2.56	0.77	1.00	0.32	2.72	9.68	2.72	0.74	0.00	1.00
BIU2	2.60	0.71	2.40	0.87	0.92	0.36	2.68	0.75	2.68	0.75	0.00	1.00
BIU3	2.56	0.71	2.48	0.92	0.73	0.34	2.52	0.77	2.52	0.77	0.00	1.00
ATUT	2.82	0.39	2.08	0.76	3.82	**0.0008**	3.08	0.66	2.55	0.78	2.71	**0.01**
ATUT1	3.08	0.70	2.40	0.82	2.88	**0.01**	3.12	0.73	2.64	0.70	2.61	**0.01**
ATUT2	2.52	0.59	1.92	0.91	2.68	**0.01**	3.12	0.78	2.40	0.96	2.97	**0.006**
ATUT3	2.76	0.52	1.84	0.90	3.99	**0.001**	3.00	0.76	2.52	0.92	2.00	0.05
ATUT4	2.92	0.57	2.16	0.94	3.26	**0.003**	3.08	0.76	2.64	0.91	1.74	0.09
PE	2.70	0.55	1.95	0.72	3.27	**0.003**	2.50	0.72	2.27	0.76	1.04	0.30
PE1	3.16	0.69	2.32	0.90	3.12	**0.004**	2.92	1.00	2.56	0.96	1.36	0.18
PE2	2.92	0.81	1.92	0.91	3.33	**0.002**	2.56	1.00	2.12	0.97	1.38	0.17
PE3	2.68	1.03	1.76	0.88	2.91	**0.007**	2.48	0.87	2.44	0.92	0.16	0.87
PE4	2.04	0.68	1.80	0.76	1.36	0.18	2.04	0.54	1.96	0.68	0.41	0.67
PS	2.73	0.72	2.57	0.81	0.64	0.52	3.12	0.64	2.48	0.81	3.25	**0.003**
PS1	2.84	0.94	2.76	0.93	0.30	0.76	3.12	0.60	2.40	0.91	3.39	**0.002**
PS2	2.72	0.95	2.64	0.86	0.31	0.75	3.12	0.60	2.64	0.81	2.38	**0.02**
PS3	2.64	0.84	2.48	1.05	0.51	0.60	3.12	0.78	2.60	0.87	2.31	**0.02**
PS4	2.72	0.75	2.40	0.91	1.01	0.31	3.12	0.78	2.28	1.02	3.67	**0.001**

Fig. 3. Two-factor authentication registration and login screenshots.



Sign Up

Your password should be at least 8 characters,should contain mixed case letters,at least a number and a special character.

Username

Password

(a) 2FA Registration Password creation

025 920
A bank (userTest)

168 882
B bank (userTest)

020 909
C bank (userTest)

(b) Google authenticator

Please scan the QR code from Google Authenticator application

Please Enter Authentication Code

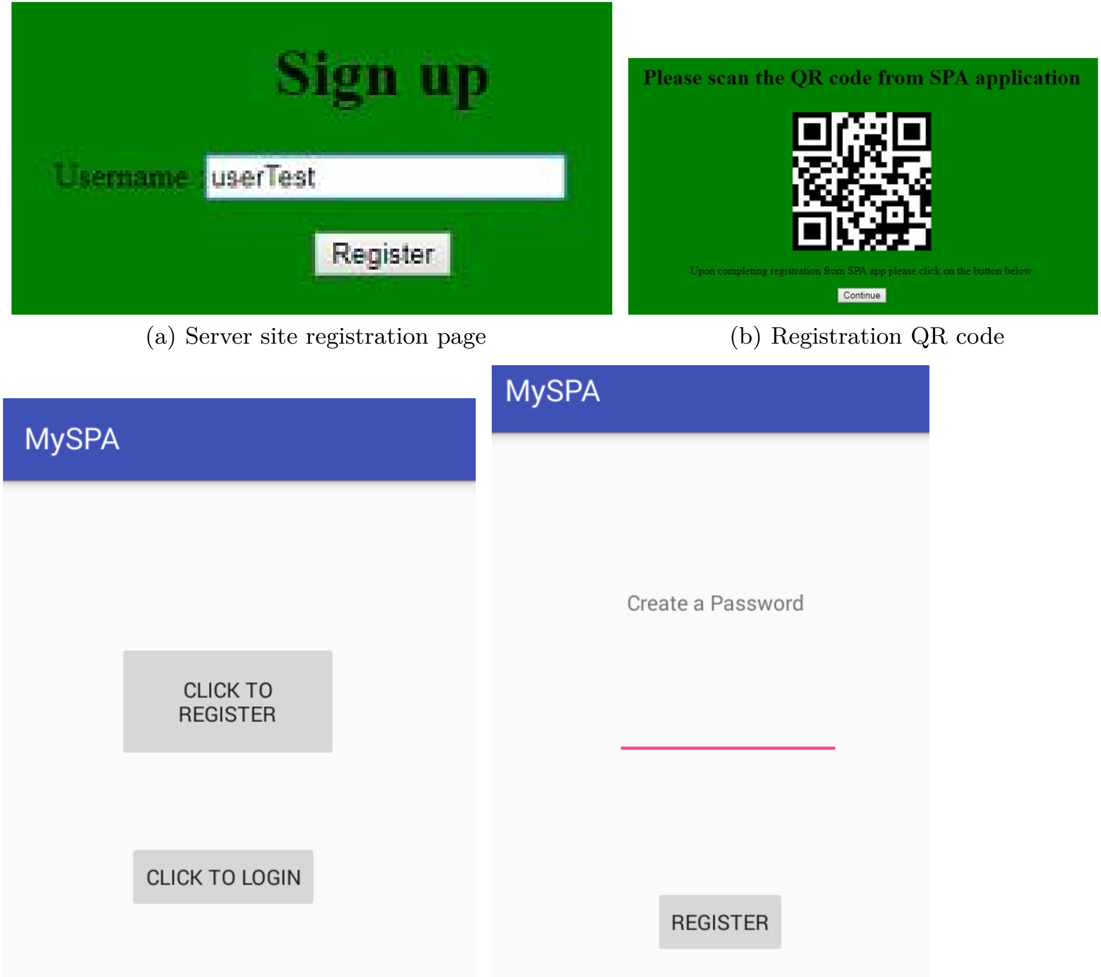
(c) Google authenticator registration via QR code

4.1 The Usability of Cloud-based SPA

Considering the range of responses, the majority of the participants agreed (or strongly agreed) that cloud-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. Indeed, this holds for every question except *"If I use the system, I will increase my chances of getting a raise"*, which received low agreement for all the systems we tested, as the participants did not link password security to their salaries.

As for the usability of cloud-based SPA compared to traditional password authentication, we found significant differences in terms of three dimensions: **effort expectancy**, **attitude towards using technology**, and **performance expectancy**. There is no significant difference between cloud-based SPA and traditional password authentication regarding **anxiety** ($t(24) = 2.03$ and $p =$

Fig. 4. Mobile-based SPA registration screenshots.



Sign up

Username : userTest

(a) Server site registration page

Please scan the QR code from SPA application

Upon completing registration from SPA app please click on the button below.

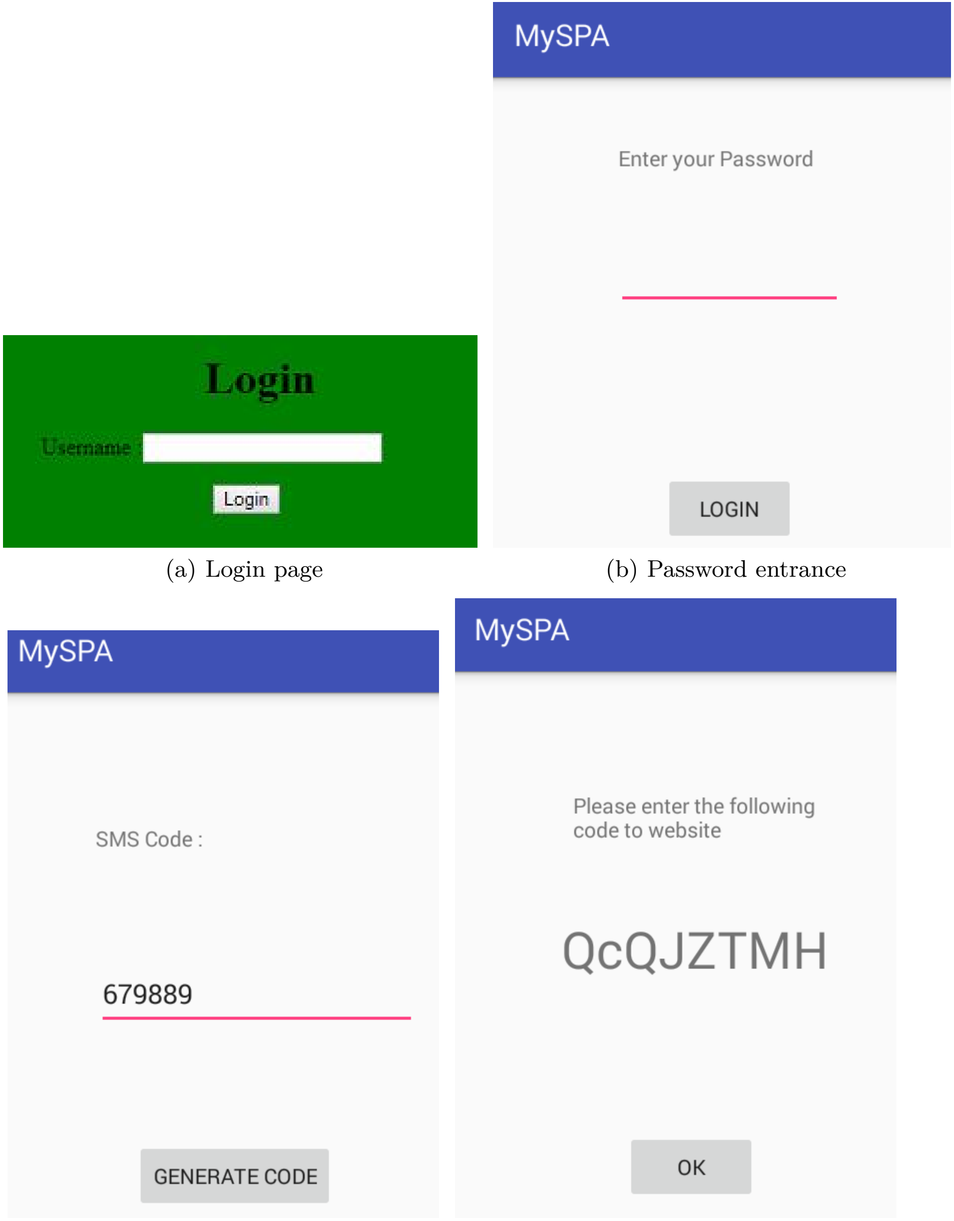
(b) Registration QR code

(c) Mobile application main page

Create a Password

(d) Password creation

Fig. 5. Mobile-based SPA login screenshots.



Enter your Password

SMS Code :

679889

Please enter the following code to website

QcQJZTMH

(a) Login page

(b) Password entrance

(c) SMS code

(d) Generated smart code

0.053), **behavioral intention to use the system** ($t(24) = 0.84$ and $p = 0.40$), and **perceived security** ($t(24) = 10.64$ and $p = 0.52$).

Effort Expectancy: SPA extension is easier to use (requires less effort) compared to traditional password authentication ($t(24) = 2.09$ and $p = 0.04$). Anecdotal observation supports this statistic, since the participants only needed to remember a single password, rather than several different passwords.

A participant said that she feels under pressure while creating a password requiring her to follow certain rules in her daily life. Consequently, she commented that she was using the same password for all her accounts (which is insecure in the traditional approach). She stated that this was because she would need to remember the passwords during login and it is hard for her to remember all these complicated passwords (see Section 4.3 for further observations).

Attitude towards using technology: Participants had a significantly more positive attitude towards cloud-based SPA compared to traditional password authentication ($t(24) = 3.82$ and $p = 0.0008$). 87% of the participants (21 out of 25 participants) wanted to use the cloud-based SPA system because of its functionality. A participant asked when we planned to launch the system publicly. The same participant stated that he generally reseted his password while logging in to a site because he always forgot or exceeded the number of attempts to enter the correct password in his daily life.

Performance Expectancy: Cloud-based SPA performed significantly better than traditional password authentication ($t(24) = 3.27$ and $p = 0.003$). The majority of the participants commented that cloud-based SPA system was very useful and they could use the system in their real life. These participants commented that they liked the idea of holding only one single password since recalling passwords took some time and it got worse if they tried to login to a site that they did not login for a while.

In the comments to the observer, the users stated that cloud-based SPA was too “simple” for online banking. They expected a second authentication factor and a more complex system for online banking. Interestingly, 63% of the comments stated that if it is hard for a user to login, it should be hard for attackers as well. This observation is also important to understand users’ point of view against cryptographic systems.

80% of the participants (20 out of 25) stated that they did not know if the extension was really performing as it was supposed to do (e.g., running the cryptographic protocols, not storing passwords). They commented that they trust this system more than traditional password authentication; however, they felt nervous because of the idea that the extension might have stored their passwords.

Another interesting point was that 52% of participants (13 out of 25)wanted to use the cloud-based SPA for their “unimportant” accounts, where they were okay if the password was compromised. These participants also stated that they had a hierarchy based on the sites they were creating account. They grouped the sites in categories and they created the password based on the category. For instance, they employ separate passwords for separate categories such as e-mail accounts (though the same password is employed for all email accounts), gaming accounts (the same password for all gaming accounts, but different from the email account password), banking accounts (different from email and gaming passwords), etc. This way, they commented, if the password used for gaming accounts was compromised, it would be fine since that password is not used for "important" sites.

Table 5. Cloud-based SPA (SPA Cloud) and traditional password authentication (Traditional):The percentage distribution of password attempts by the participants to login. μ: mean, σ: standard deviation.

	Login Trial		**Success Percent at Trial Number**			
	μ	σ	1	2	3	Failure (%)
SPA Cloud	1.09	0.38	88	4	3	5
Traditional	1.44	0.73	68	16	14	2

Success/Failure Rates: We measured that 88% of the time the participants successfully remembered their passwords at the first attempt using cloud-based SPA. 4% of the time they remembered their passwords at their second attempt and 3% of the time they remembered their password at their third trial. 5% of the time the participants participants did not remember their passwords within 3 trials and were counted as failed attempts. Overall, 95% of of the time the participants accomplished to login while 5% of the time the participants failed to login. The average number of attempts by a user is 1.09 (see Table 5).

In comparison, for traditional authentication, we measured that 68% of the time the participants successfully remembered their passwords at their first attempt. 14% of the time the participants remembered their passwords at their second attempt and 16% of the time the participants remembered their password at their third trial. 2% of the time the participants did not remember their passwords within 3 trials and were counted as unsuccessful login attempt. Overall, 98% of the time the participants accomplished to login while 2% of the time the participants failed to login. The average number of attempts by a user is 1.44 (see Table 5).

Thus, both systems had similar overall failure rates though surprisingly cloud-based SPA failure rate was slightly higher. We observed that the average number of attempts for cloud-based SPA (with an average of 1.09) is smaller than that of traditional password authentication (with an average of 1.44). This observation implies that that cloud-based SPA fulfilled what it promises about easier recall of passwords.

4.2 The Usability of Mobile-based SPA

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. Except the salary raise note as in Study I, the only other two questions that the majority did not agree were *"I plan to use the system in the next 6 months"* and *"Using the system increases my productivity"*, for both of which both the mobile-based SPA and two-factor authentication responses are almost identical.

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 two-factor authentication 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 participants (14 out of 20 who commented) stated that they 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 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 two-factor authentication ($t(24) = 3.25$ 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 mobile device (conceived as a personal item) made the user feel more secure, whereas they needed to type their passwords on websites in standard two-factor authentication.[10] One participant commented that seeing all works (computations) carried out on the mobile device made her feel more secure, and she felt to have the control of her password security, since she could see the steps (e.g., SMS challenge, smart code generated). Another participant pointed 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.

Furthermore, 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 independent sets of participants of both studies essentially agreed that a "simple" single password solution without the mobile device (i.e., cloud-based SPA) does not feel secure enough for banking

[10] [26] measures the usability and security of creating and entering textual passwords on mobile devices. [26] finds that users spend significantly longer time while creating textual passwords on mobile devices and creating passwords on mobile devices is more error-prone. Besides, passwords created on mobile devices are also weaker compared the passwords created on computers.

scenarios, but it is efficient for daily use, and a "complex" solution using the mobile device (i.e., mobile-based SPA) feels secure for banking since the password is typed on the phone, whereas it is inefficient for daily use (e.g., for e-mail and other frequently accessed sites).

Attitude towards using technology: Mobile-based SPA performed statistically significantly better compared to two-factor authentication ($t(24) = 2.71$ and $p = 0.01$), including all sub-statements. Similar to cloud-based SPA, 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 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 two-factor authentication 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 steps followed in mobile-based SPA were a little bit more complex (such as typing 8-character alphanumerical code to the site, while they type 6-digit numerical code in the two-factor authentication). Most of the users 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. 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.

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 6). 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 future systems and studies.

For two-factor authentication, 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 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 which resulted in a login failure. Overall, 91% of the time the participants accomplished to login while 9% of the time the participants failed to login. The average number of password attempts by a user is 1.17 (see Table 6).

We conclude that for both two factor authentication 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. Using two-factor authentication, 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.

Table 6. Mobile-based SPA (SPA Mobile) and two-factor authentication (Two Factor): The percentage distribution of password attempts by the participants 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

4.3 Common Single Password Authentication Observations

The participants mentioned valuable statements and discussed their habits while creating, securing, and recalling the passwords. [31] observes 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 (whether cloud-based or mobile-based) overcomes some of the challenges users face.

90% of the study participants (45 out of 50) were aware of password security. 85% of the comments (38 out of 45) 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 participants (25 out of 45) noted that they 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.

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. 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.

Another frustration shared by 52% of the users (26 out of 50) was 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. While this idea might require further research, users may feel more secure when a new system is collectively used.

Our user studies concluded that SPA systems provide usability benefits. The main reasoning is that it is not convenient to expect users to create different 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. Also, considering the discussions on security and usability, there might be an inverse relationship between the perceived security and ease of use, since cloud-based SPA was found better for daily use, whereas mobile-based SPA was found more secure for online banking. This interpretation is worth exploring for future research.

5 Conclusion

We implemented two single password authentication solutions (cloud-based SPA solution of [20] and mobile-based SPA method of [4]) and conducted their usability analysis for the first time. We compared cloud-based SPA against the traditional approach in a daily use scenario, and mobile-based SPA against two-factor authentication in an online banking scenario. Quantitative and qualitative results support that both SPA solutions have usability and security advantages compared to their counterparts. Based on the feedback reported by the participants, we suggest that cloud-based SPA solutions should be deployed for daily use, where users wish to login to a site frequently, and mobile-based SPA solutions 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 usability of SPA systems regarding their future deployment. Yet, to obtain more generalizable results, we plan to conduct future studies taking into account timing information, taking place in a natural settings instead of a lab environment, and increasing the number of participants. Our findings suggest that the smart code mechanism should be simpler, the SPA branding should provide more trust to the users, and SPA systems should also potentially be compared against password managers (that provide lower levels of cryptographic security).

Acknowledgements

We thank Arjen Kılıç and İlker Kadir Öztürk for their efforts on implementation. We acknowledge the support of TÜBİTAK (the Scientific and Technological Research Council of Turkey) under the project number 115E766, European Union COST Action IC1306, and the Royal Society of UK Newton Advanced Fellowship NA140464.

References

1. European Union General Data Protection Regulation 2016/679 (GDPR), 2016.
2. Turkish Personal Data Protection Law no. 6698, 2016.
3. Turkish Personal Data Protection Law 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, H. Gurbaslar, and B. Erdeniz. Towards usable solutions to graphical password hotspot problem. In *IEEE COMPSAC*, 2009.
9. 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.
10. K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, and N. Atalay. Graphical passwords as browser extension: Implementation and usability study. *Trust Management III*, 2009.
11. R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart. Cracking-resistant password vaults using natural language encoders. In *IEEE SP*, 2015.
12. S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, 2006.
13. L. Corporate. Lastpass-the last password you have to remember, 2016.

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. M. Golla, B. Beuscher, and M. Dürmuth. On the security of cracking-resistant password vaults. ACM SIGSAC, 2016.
18. 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.
19. J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In *ACM WWW*, 2005.
20. D. İşler and A. Küpçü. Threshold single password authentication. In *ESORICS DPM*. 2017.
21. S. Jarecki, H. Krawczyk, M. Shirvanian, and N. Saxena. Device-enhanced password protocols with optimal online-offline protection. In *ACM ASIACCS*, 2016.
22. A. Karole, N. Saxena, and N. Christin. A comparative usability evaluation of traditional password managers. In *ICISC*, 2010.
23. Z. Li, W. He, D. Akhawe, and D. Song. The emperor's new password manager: Security analysis of web-based password managers. In *USENIX Security Symposium*, 2014.
24. M. Mannan and P. C. van Oorschot. Digital objects as passwords. In *HotSec*, 2008.
25. 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.
26. W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek. Usability and security of text passwords on mobile devices. In *CHI Conference on Human Factors in Computing Systems*. ACM, 2016.
27. G. Norman. Likert scales, levels of measurement and the "laws" of statistics. *Advances in health sciences education : theory and practice*, 2010.
28. B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. In *USENIX Security Symposium*, 2005.
29. M. Shirvanian, S. Jarecki, N. Saxena, and N. Nathan. Two-factor authentication resilient to server compromise using mix-bandwidth devices. In *NDSS*, 2014.
30. M. Shirvanian, S. Jareckiy, H. Krawczykz, and N. Saxena. Sphinx: A password store that perfectly hides passwords from itself. In *IEEE ICDCS*, 2017.
31. E. Stobert and R. Biddle. The password life cycle. *ACM TOPS*, 2018.
32. 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.
33. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 2003.
34. M. Zviran and W. J. Haga. A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, 1993.

A Post-Questionnaire Percentage Distribution

Table 7. Post-Questionnaire Percentage Distribution

Cloud-based SPA																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
Strongly Disagree	4	8	4	4	40	20	36	32	4	8	8	0	4	0	0	0	4	16	20	4	8	12	12
Disagree	8	8	8	0	48	60	44	56	20	28	32	20	40	28	20	16	24	24	56	24	28	32	24
Agree	32	28	28	44	8	12	20	12	68	60	56	52	56	68	68	52	48	36	24	56	48	36	44
Strongly Agree	56	56	60	52	4	8	0	0	8	4	4	28	0	4	12	32	24	24	0	16	16	20	20
Traditional Password Authentication																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
Strongly Disagree	0	0	12	4	24	16	16	12	8	16	16	12	36	40	28	16	36	44	36	12	12	24	16
Disagree	16	16	40	36	48	48	40	56	36	36	32	44	44	44	36	48	44	44	52	20	24	20	40
Agree	52	60	20	28	28	20	40	24	48	40	40	36	12	8	28	24	12	4	8	48	52	40	32
Strongly Agree	32	24	28	32	0	16	4	8	8	8	12	8	8	8	8	12	8	8	4	20	12	16	12
Mobile- based SPA																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
Strongly Disagree	4	4	0	4	20	36	24	24	0	0	4	0	4	0	0	8	16	12	12	0	0	0	4
Disagree	16	8	12	12	64	60	64	56	40	48	52	20	12	28	24	28	32	40	72	12	12	24	12
Agree	52	56	56	48	12	4	12	16	48	36	32	48	52	44	44	28	32	36	16	64	64	40	52
Strongly Agree	28	32	32	36	4	0	0	4	12	16	12	32	32	28	32	36	20	12	0	24	24	36	32
Two Factor Authentication																							
	EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
Strongly Disagree	0	0	0	0	4	16	12	8	4	4	4	4	24	20	12	16	32	16	20	16	8	8	28
Disagree	4	8	16	0	72	56	68	60	32	36	52	36	20	16	28	28	32	36	68	40	32	40	28
Agree	60	68	60	52	20	16	16	28	52	48	32	52	48	56	44	40	28	36	8	32	48	36	32
Strongly Agree	36	24	24	48	4	12	4	4	12	12	12	8	8	8	16	16	8	12	4	12	12	16	12

B Participants Responses per Question

Table 8. Participants scores per question for two-factor authentication. Each row represents responses of one participant.

Two factor Authentication																						
EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
3	4	3	4	2	2	2	2	3	2	2	3	3	3	3	3	3	3	2	1	1	2	1
3	3	2	3	2	2	2	2	2	2	2	2	3	3	3	2	2	2	2	2	3	3	2
3	3	3	3	3	2	2	2	2	3	2	2	1	1	1	1	1	1	1	2	2	2	1
3	3	2	4	2	4	2	2	3	3	3	2	1	1	1	2	1	1	1	1	2	2	1
3	3	3	4	2	3	3	2	2	2	2	3	3	3	3	3	3	3	4	2	2	2	3
3	3	3	3	2	2	2	2	3	3	3	3	2	3	3	3	2	2	2	2	3	2	2
3	3	3	3	3	3	2	3	3	3	3	3	2	2	2	3	1	2	2	3	3	3	1
4	4	4	4	2	2	2	3	4	4	4	3	3	3	3	3	2	3	2	3	3	3	3
3	3	3	3	4	4	2	3	2	2	2	3	3	3	3	2	2	2	2	2	2	1	1
4	2	4	4	2	2	2	2	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3
3	3	3	3	3	2	2	3	4	3	4	2	1	3	4	2	1	3	2	3	3	3	2
4	4	4	4	2	1	2	2	2	2	2	2	3	3	2	3	3	2	1	1	1	1	1
3	4	4	4	2	3	3	2	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4
4	4	3	4	2	1	1	3	3	4	3	4	4	4	4	4	1	4	2	3	3	4	3
3	3	3	3	2	2	2	2	3	3	3	3	3	3	3	4	4	4	3	4	4	4	4
4	3	4	4	2	4	4	4	3	3	2	2	3	3	4	4	3	3	2	4	4	4	4
4	3	3	3	2	2	2	2	3	3	3	3	2	2	2	3	2	2	2	3	3	3	3
3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	3	2	3	2	2	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	3	3	3	2	2	2	2	3	2	2	3	3	3	3	3	3	3	2	3	3	2	3
4	2	2	3	3	3	3	3	2	3	2	2	1	1	2	1	1	3	2	2	3	3	3
4	3	3	4	2	2	2	2	3	3	2	3	3	3	3	2	2	2	2	2	2	2	2
4	4	4	4	2	2	2	2	3	2	2	3	3	3	3	3	3	3	2	1	2	2	3
3	3	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	3	3	2
2	3	3	4	3	1	1	1	3	3	3	3	1	1	2	1	1	1	1	2	3	3	1

Table 9. Participants scores per question for mobile-based SPA. Each row represents responses of one participant.

Mobile-based SPA																						
EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
4	3	3	4	1	1	2	2	3	2	2	3	3	3	3	3	3	3	2	4	4	4	4
3	4	3	3	2	2	2	2	3	2	2	3	3	3	3	3	3	3	3	4	4	4	4
4	4	4	4	2	2	2	2	2	3	2	3	4	4	4	4	3	3	2	4	4	4	4
3	3	3	3	2	2	3	2	2	2	2	3	3	3	3	2	2	2	2	3	3	3	3
4	4	3	3	2	1	1	2	2	2	2	3	1	2	2	2	2	1	1	3	3	3	3
3	3	3	3	1	2	2	1	3	3	3	4	3	2	2	1	1	1	1	3	3	2	3
3	3	3	3	2	2	2	2	2	2	2	4	4	4	4	4	4	3	2	3	3	3	3
4	3	4	4	2	2	2	2	3	3	4	4	3	3	3	4	4	3	3	3	3	3	3
3	3	2	2	3	3	3	3	2	2	1	2	3	3	3	2	2	2	2	3	3	3	2
2	4	4	4	1	1	1	4	3	3	2	3	4	4	4	2	2	2	2	3	3	3	3
3	3	3	2	2	2	2	3	3	3	2	2	3	2	2	3	2	2	2	2	2	2	2
4	1	4	4	3	1	1	1	4	4	4	4	4	4	4	4	4	2	2	3	3	3	3
2	3	2	3	1	1	1	1	2	2	2	4	4	4	4	4	2	1	2	4	4	4	4
4	4	4	4	3	2	2	2	3	3	3	3	3	3	3	3	3	3	2	3	3	2	3
4	3	3	4	2	1	1	3	3	4	3	4	4	4	4	4	1	4	2	3	3	4	3
3	4	4	3	2	2	2	2	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4
3	3	3	3	2	2	2	2	3	3	3	3	3	3	3	4	4	4	3	4	4	4	4
3	3	2	2	2	2	2	3	2	2	2	2	3	2	2	2	1	2	2	3	3	3	4
1	2	3	1	2	2	2	2	3	3	3	3	2	2	2	3	3	2	2	3	3	3	3
2	3	3	3	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	3	3	3	2	2	2	2	3	2	2	3	3	3	3	3	3	3	2	3	3	2	3
3	4	4	4	1	1	1	1	2	4	3	4	4	3	3	2	2	3	2	3	3	4	4
3	3	3	3	2	1	2	1	4	3	3	3	2	2	3	1	1	2	1	3	3	4	3
3	4	4	4	4	1	2	1	2	2	2	3	3	3	4	4	3	3	2	3	3	3	3
2	2	3	3	2	2	2	2	3	2	3	2	3	3	3	3	3	2	2	2	2	2	1

Table 10. Participants scores per question for traditional password authentication. Each row represents responses of one participant.

Traditional Password Authentication																						
EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
4	4	4	4	2	4	2	2	3	3	2	4	4	4	4	4	4	4	2	4	4	4	3
2	3	1	1	2	2	3	2	1	1	1	1	1	1	1	1	1	1	1	3	2	2	1
3	3	2	3	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1
3	2	2	2	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	2	1	2	2	4	4	4	2	1	1	2	1	1	2	2	1	1	1	1	1	1	2
3	3	3	2	2	2	2	2	3	3	3	3	2	2	3	3	3	3	2	3	3	3	3
4	4	4	4	1	1	1	1	4	4	4	4	1	1	1	3	1	1	1	3	3	3	2
2	3	3	3	1	1	1	1	3	3	3	3	3	4	4	4	4	4	4	4	3	4	2
4	4	4	4	2	2	2	2	3	3	3	3	2	2	3	2	2	2	2	3	3	3	2
3	2	1	2	1	1	1	4	3	3	3	2	1	1	1	1	1	1	1	4	4	3	3
4	4	4	4	2	2	2	3	3	3	3	3	2	3	3	3	2	1	1	4	3	3	3
3	3	2	3	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	2	2	2	2
3	3	3	3	1	2	1	2	3	3	3	3	2	2	3	3	2	2	1	1	1	1	1
3	3	4	4	3	4	3	2	3	2	1	3	3	2	3	3	3	2	2	3	3	3	3
3	3	3	2	3	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2
4	3	2	3	3	4	3	3	2	2	3	2	2	2	2	2	1	1	2	3	4	4	3
4	3	2	4	3	2	3	2	3	3	3	3	2	2	2	2	2	2	2	3	3	3	3
4	4	4	4	1	2	2	1	4	4	4	3	1	1	1	2	1	1	1	2	2	1	2
3	3	2	2	2	2	2	3	2	2	2	2	3	2	2	2	1	2	2	3	3	3	4
2	3	2	3	2	2	2	3	2	2	1	2	2	2	2	2	2	2	2	3	3	1	1
4	3	4	4	2	2	3	2	3	1	4	2	4	1	3	4	3	2	1	4	3	4	4
2	2	2	2	1	1	2	2	1	1	2	1	1	1	2	2	2	1	2	1	1	1	2
3	3	3	3	2	2	2	2	3	3	3	3	2	3	3	3	2	2	2	3	3	3	2
3	3	2	2	3	3	3	2	2	2	2	2	1	1	1	1	1	1	3	3	3	3	3
3	4	2	2	2	3	3	2	2	2	2	1	1	1	1	2	2	1	3	3	3	1	4

Table 11. Participants scores per question for cloud-based SPA. Each row represents responses of one participant.

Cloud-based SPA																						
EE1	EE2	EE3	EE4	A1	A2	A3	A4	BIU1	BIU2	BIU3	ATUT1	ATUT2	ATUT3	ATUT4	PE1	PE2	PE3	PE4	PS1	PS2	PS3	PS4
4	4	4	4	1	1	1	1	2	2	2	3	2	2	2	2	1	1	1	2	2	2	2
4	4	4	4	1	2	2	1	4	4	4	4	2	2	2	4	4	4	1	4	4	4	4
3	3	3	3	2	2	2	2	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3
3	4	4	3	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	4	4	3	2	4	3	2	3	2	2	4	3	3	3	4	4	3	2	3	3	1	2
2	3	2	3	2	2	2	2	3	3	3	3	2	3	2	3	2	2	2	3	3	3	3
4	3	3	3	2	2	2	2	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3
3	4	3	3	3	4	2	2	2	2	2	2	3	3	3	2	2	2	2	3	3	3	3
1	1	1	1	4	2	3	2	2	2	2	2	3	3	3	2	2	2	3	2	1	1	2
4	4	4	4	2	2	1	3	3	3	3	3	2	2	3	4	4	4	1	2	2	1	1
3	4	4	4	1	3	3	1	3	3	2	4	2	2	4	4	4	4	2	3	2	2	3
4	4	4	4	2	2	1	1	3	3	3	4	2	3	3	4	3	2	1	4	4	4	4
3	3	2	3	2	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	2	3	3	1	2	1	2	2	2	2	3	3	3	3	3	4	4	1	2	2	2	2
3	4	4	4	2	1	3	2	3	3	2	4	2	3	3	4	4	4	2	4	4	4	3
4	4	4	4	1	2	2	1	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3
4	4	4	4	1	1	1	1	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4
4	4	4	4	1	2	2	1	3	3	3	4	3	3	3	4	3	3	2	3	3	2	4
4	4	4	4	2	2	2	2	3	3	3	3	2	2	3	3	3	3	2	2	3	2	2
4	3	3	3	2	2	2	2	3	3	3	3	2	2	2	3	2	2	2	3	3	3	3
4	4	4	4	3	3	2	2	3	3	3	3	3	3	3	3	3	3	2	3	3	2	3
4	3	4	4	2	2	3	2	4	1	1	4	3	4	4	3	3	4	2	3	1	4	4
2	3	3	3	2	2	1	2	1	1	1	2	1	3	3	3	2	1	2	1	2	2	3
4	1	4	4	1	1	1	3	3	3	3	3	3	3	3	3	3	1	3	3	3	3	1
4	2	3	3	1	2	1	3	3	2	3	2	3	3	4	3	3	1	3	3	2	3	1