User perceptions and use of authentication methods: Insights from youth in Mexico and Bosnia and Herzegovina

Abstract

Purpose: This paper aimed to address the user perspective about usability, security and use of five authentication schemes (text and graphical passwords, biometrics, and hardware tokens) from a population not covered previously in the literature. Additionally, we explored the criteria users apply in creating their text passwords.

Methodology: An online survey study was performed in spring 2019 with university students in Mexico and Bosnia and Herzegovina. 197 responses were collected.

Findings: Fingerprint-based authentication was perceived as usable and secure the most frequently. However, text passwords were the predominantly used method for unlocking computer devices. Our participants preferred to apply personal criteria for creating text passwords, which, interestingly, coincided with the general password guidelines, e.g., length, combining letters and special characters.

Originality: Research on young adults' perceptions of different authentication methods is driven by the increasing frequency and sophistication of security breaches, as well as their significant consequences. This study provided insight into the commonly used authentication methods among youth from two geographic locations, which have not been accounted for previously.

Keywords: authentication schemes, usability, security, memorability, text passwords

1. Introduction

The rising cybersecurity issues, stringent data privacy requirements, and necessity to regularly access a plethora of web services and computing devices are increasing demands for user authentication. A wide range of authentication schemes has been proposed and grouped as text-based and graphical passwords, biometrics, cognitive and token-based methods (Zimmermann and Gerber, 2020).

Research advances in this area have mainly focused on the design of biometric schemes (Abuhamad *et al.*, 2020) and applications of the latest machine learning models for these purposes (Ryu *et al.*, 2021). This has been supported by the proliferation and accessibility of mobile devices and embedded tools, such as cameras and microphones. In practical use, text password-based authentication continues to prevail (Zimmermann and Gerber, 2020). Nevertheless, opinions of users remain understudied (Zimmermann and Gerber, 2020; Ryu *et al.*, 2021). What is lacking is a more comprehensive understanding of user adoption and perspective on usability and security of the different authentication schemes.

Perceived usability refers to the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO, 2018). Memorability, an aspect of usability, addresses the cognitive load dedicated to memorizing something (Zimmermann and Gerber, 2020; Woods and Siponen, 2019). Perceived security, on the other hand, assesses an authentication method's perceived protection against or resilience to different security attacks, including, e.g., guessing, phishing and theft (Zimmermann and Gerber, 2020). Moreover, studies have shown that user perception of authentication methods is associated with their adoption (El-Abed *et al.,* 2010; Bhagavatula *et al.,* 2014).

Therefore, this paper aims to explore the perception and use of password-based (text and graphical), biometric (fingerprint and face recognition) and token-based authentication methods among youth in Mexico and Bosnia and Herzegovina (B&H), as two previously unaddressed geographic locations. We will attempt to answer the following research questions:

RQ1. What is the perceived usability of each of the five authentication methods?

RQ2. What is the perceived security of each of the five authentication methods?
RQ3. Which methods are used for authentication on different computer devices?
RQ4. What are the preferred criteria for creating text passwords?

The paper is structured as follows. Related work is reviewed in Section 2, while Section 3 reports on the research design and survey methods. Section 4 presents the quantitative and qualitative findings about the perceived usability and security of the five authentication schemes, and text password creation criteria. The results are discussed in Section 5, which concludes the paper with future work indications.

2. Related work review

Authentication methods are classified into: knowledge-based, which employ something a user knows; possession-based, derived from something a user has; and identity-based, i.e., methods that exploit what a user is (Shafique *et al.,* 2017). Commonly, these methods have been evaluated for: deployability (Bonneau *et al.,* 2012); user preferences (Mirza *et al.,* 2018; Zimmermann and Gerber, 2020); and usability and security, from a technical (Bonneau *et al.,* 2012; Ferrag *et al.*, 2020), as well as user perspective (Andriotis *et al.,* 2016; Zimmermann and Gerber, 2020).

Text password authentication is still among the most popular approaches. Katsini *et al.*'s (2016) review of knowledge-based methods showed that online service providers were mainly using text passwords. Moreover, users' preferences for passwords persist (Zimmermann and Gerber, 2020). Bonneau *et al*. (2012) evaluated 35 password-replacement schemes. However, none of the alternative schemes - including biometrics, graphical passwords and hardware tokens - scored better than passwords on usability, deployability and security criteria. According to a systematic literature review of 515 single-factor and 442 multi-factor authentication (MFA) methods, text passwords continue to also be heavily researched (Velásquez *et al.,* 2018).

While text passwords' popularity owes to their easy recovery, simplicity and high deployability (Bonneau *et al.,* 2012), they nevertheless have multiple drawbacks, e.g., questionable security (Katsini *et al*., 2016; Li *et al*., 2021), and usability and memorability issues (Mackie and Yıldırım, 2018; Woods and Siponen, 2019). Hence, various studies have given attention to password creation guidelines and policies. The commonly suggested ones in the related literature include:

g1. Avoiding words that reference personal life (Abbott *et al.,* 2018);
g2. Using a combination of upper and lowercase letter, numbers, and special characters (Zhang-Kennedy *et al*., 2016; Abbott *et al.,* 2018);
g3. Setting the minimum length to eight characters (Zhang-Kennedy *et al*., 2016; Abbott *et al.,* 2018);
g4. Using different passwords for each online account and computer device (Grawemeyer and Johnson, 2011);
g5. Changing passwords every 1-3 months (Zhang-Kennedy *et al*., 2016);
g6. Avoiding password reuse (Zhang-Kennedy *et al*., 2016);
g7. Using password generators for randomization (Guo *et al.,* 2019);
g8. Using password manager software (Alkaldi and Renaud, 2019);
g9. Not writing passwords on post-it notes (Zhang-Kennedy *et al*., 2016).

Graphical passwords alleviate some of the text password memorability issues. They take advantage of the picture superiority effect (Nelson *et al.,* 1979), i.e., their easier recall than words (Biddle *et al.,* 2012). However, graphical passwords' design overlooks potential visual perception issues and higher motor effort, which could represent a hindrance for some users. A user study for Android pattern lock screen found that graphical passwords' usability outweighs their security, due to, for example, susceptibility to shoulder surfing attacks (Andriotis *et al.,* 2016). Nevertheless, recent security improvements have been achieved with gamified approaches (Raptis *et al.,* 2021).

In terms of perceived security, **biometric** methods show superior performance. Bhagavatula *et al.* (2014) in their study of iPhone fingerprint and Android face recognition methods, showed that biometrics were generally considered secure. Similarly, Zimmermann and Gerber's (2017) findings implied that users could be grouped into two camps – pro-biometrics or pro-passwords, depending on what they valued more, security or privacy, respectively. Among the biometric methods, fingerprint and iris recognition were preferred for their perceived security (Zimmermann and Gerber, 2017). Fingerprint authentication was also well adopted in sensitive online services, as is mobile banking (Mirza *et al.,* 2018). Zimmermann and Gerber (2020) further observed users' interaction with twelve authentication schemes. They confirmed that fingerprint recognition and passwords were preferred the most, perceived as the most usable, and expected to result in the fewest problems. The limitation of Zimmermann and Gerber's (2020) approach was a small sample of 41 psychology students from a single location.

The convenience of biometrics depends on the scenario in which they are used (Bhagavatula *et al*., 2014). For example, only two of eight device and service providers (including banks, operating systems, smartphones and browsers) adopted biometric-based schemes (Al Abdulwahid *et al.,* 2016). Recently, however, fingerprint and face recognition can be seen more in computer devices, especially smartphones (Al Abdulwahid *et al.,* 2016). **Token-based** methods were also not frequently employed (Al Abdulwahid *et al.,* 2016), although these methods meet most of the objective security criteria (Bonneau *et al*., 2012; Zimmermann and Gerber, 2020), and are hence among the top ranked in terms of actual security levels.

Current research and commercial efforts are directed towards a wider exploration and adoption of **MFA**, i.e., combining knowledge-, possession-, and identity-based methods. The findings from a usability study of five two-factor authentication (2FA) methods for a simulated banking website indicated positive user perception and interest in 2FA adoption for personal accounts (Reese *et al*., 2019). However, reviews of five leading 2FA schemes (Wang *et al*., 2020) and MFA for online banking (Sinigaglia *et al*., 2020) showed that MFA still faces major challenges, e.g., security flaws, vulnerabilities, lack of user anonymity.

In summary, previous related work identified and categorized various authentication schemes (Bonneau *et al.,* 2012; Ferrag *et al*., 2020; Li *et al.,* 2021). They highlighted the persisting prevalence of text passwords (Abbott *et al.,* 2018; Zimmermann and Gerber, 2020). There were attempts to address the common text password issues with 2FA, which indicated improvements in usability and security (Bhana and Flowerday, 2020). The state-of-the-art explored MFA for Internet of Things (Lee *et al*., 2020) and behavioral biometric methods - motion, keystroke, touch gesture, voice and multimodal (Abuhamad *et al.,* 2020; Ryu *et al.,* 2021). Similarly, knowledge-driven methods were proposed for virtual reality (Mathis *et al.,* 2020). However, a comprehensive exploration of user perceptions of the different authentication methods remains understudied (Velásquez *et al.,* 2018; Ryu *et al.,* 2021) and is thus the focus of our paper.

Furthermore, the use of authentication schemes in different contexts needs further consideration (Velásquez *et al.,* 2018). The limited number of countries (often West-dominated) covered by prior research includes: user attitude toward biometric schemes in India, South Africa and the United Kingdom (Riley *et al*., 2009); effect of gender on perceptions of biometrics in Saudi Arabia (Al-Harby *et al.,* 2009); user opinions about graphical passwords in the UK (Andriotis *et al.,* 2016); user acceptance of biometrics for mobile banking in Bahrain (Mirza *et al.,* 2018); lab-based study in Germany evaluating 12 biometric and non-biometric schemes (Zimmermann and Gerber, 2020).

Therefore, our paper **contributed** by exploring university students' perceptions of usability and security of five authentication methods, and their use on different computer devices. Moreover, we addressed the gap in the literature by sampling young population from two geographic contexts which were not previously accounted for – B&H and Mexico. Given the prevalence of text passwords' use and the lack of successful replacement schemes (Zimmermann and Gerber, 2020), we also studied the existing and personal criteria users employ for creating memorable and secure text passwords.

3. Methodology

In line with Riley *et al.'s* (2009) cross-continental approach, this study was performed in two locations – a small private university in Bosnia and Herzegovina (English used for medium of instruction; students are local Bosnian and international) and a larger public university in Mexico (Spanish language; students are predominantly Mexican). We aimed at recruiting 200 students, with balanced representation from both locations. Previous authentication scheme evaluations reported a similar sample size (Furnell and

Evangelatos, 2007; Mackie and Yıldırım, 2018; Zimmermann and Gerber, 2020). Convenience **sampling** (Zimmermann and Gerber, 2017; 2020) was used in order to recruit students from different academic fields.

The data collection instrument was an online **survey questionnaire** (Appendix) as in (Furnell and Evangelatos, 2007; Mackie and Yıldırım, 2018). Google forms were used to create two survey versions – English (B&H) and Spanish (Mexico), which were pilot tested in both locations. Students completed the survey during a lecture or lab session, while overseen by one of the researchers. Participants were: explained the usability and security scales; informed in which cases to select “I am not familiar with this method”; asked to read the instructions and response options carefully, avoid random responses, and skip or select N/A for the questions they were unsure or unwilling to answer. Finally, they were asked to remain quietly seated, after submitting the survey, not to disturb other participants.

The first survey section was a consent form that informed participants about the study’s aim, their rights to withdraw, which data would be collected, process for ensuring confidentiality and anonymization, and collected their agreement to take part in the study. The rest of the survey sections gathered:

- Demographic information (age, gender, nationality, academic major/department).
- Usability and security (Appendix: Q1 and Q2), measured on a 5-point Likert scale (1 - strongly disagree to 5- strongly agree, and 6 - I am not familiar with this method). Usability and security items were adopted from (Zimmermann and Gerber, 2017; 2020). Five commonly studied (Sasse, 2005; Bonneau *et al.,* 2012; Zimmermann and Gerber, 2020) and currently used authentication methods were evaluated: text, i.e., alphanumeric passwords, graphical passwords, fingerprint, face recognition, and hardware tokens. Participants were given examples (illustrations in Appendix: Q1 and Q2) of each of the five authentication methods.
- Use of the five authentication methods for unlocking five computer devices, as a multiple answer question, including the not applicable option, if a device was not used (Appendix: Q3 and Q4).
- Text password guidelines (Appendix: Q5-Q7), comprising a multiple answer question listing nine commonly prescribed guidelines (Section 2: g1-g9), and two open-ended questions for participants to justify if and why the guidelines were not used, and to state personal text password creation criteria.

The average survey completion time was 20 minutes. Data was gathered over four weeks in May and June 2019. The total responses collected were 113 in B&H and 165 in Mexico.

Data preparation. The two questionnaire versions were combined into one dataset. Responses in Spanish (open-ended questions) were translated into English. Data was cleaned of extreme age outliers (30 years and above) and invalid responses (e.g., straight-lining, inconsistent answers, or if none of the open-ended questions were answered). We preserved missing values, given that they comprised only 0.5% of the data. Authentication methods’ usability and security items were transformed into a 1-5 scale, with a missing value for the “I am not familiar with this method” response. Answers to open-ended questions were organized into categories according to coinciding mentions and ordered by frequency. Text data cleaning included removal of: numbers, special characters, stopwords, common words (e.g. “password”, “make” and “can”), and participants’ examples of passwords. Finally, lemmatization was applied and word frequencies calculated.

Data analysis tools. Descriptive and quantitative data analyses for RQ1-RQ3 were performed in Excel and IBM SPSS. RQ4 was processed in R; for word frequency and text mining, *tm* and *SnowballC* packages were used.

4. Data analysis and results

4.1. Descriptive statistics

Data analysis was performed on 197 responses, 97 from B&H and 100 from Mexico. Participants’ average age was 20.2 years, and a slightly higher proportion were male. As shown in Table I, there was unbalanced representation of nationalities and academic majors.

Table I. Participants' demographics

Age	Mean ± SD: 20.2 ± 1.6		Range: 18-27
Gender (%)	Male 55.3	Female 43.2	Prefer not to say 1.5
Nationality (%)	Mexican 50.3	B&H 37.6	Other* 12.2
Academic major (%)	Information Technology** 44.1	Social Sciences# 30.5	Health Sciences¥ 25.4

*Syrian, Bangladeshi, Croatian, French, German, Greek, Iranian, Jordanian, Norwegian, Pakistani, dual nationalities

** telematics, computer science and information systems;

# psychology, economics, political science, marketing, linguistics;

¥ medicine, dentistry

4.2. Perceived usability and security of authentication methods (RQ1/RQ2)

Perceived usability and security of the five authentication methods are compared in Figure 1 and 2, respectively. The largest percentage of participants perceived fingerprint authentication as usable (88.3%), followed by text passwords (70.1%). Interestingly, these two methods were also perceived as secure the most frequently. On the other hand, the majority of our participants had a negative or neutral opinion about the graphical passwords' security and hardware tokens' usability. However, most were not familiar with the token-based method, while all the participants were familiar only with text passwords.

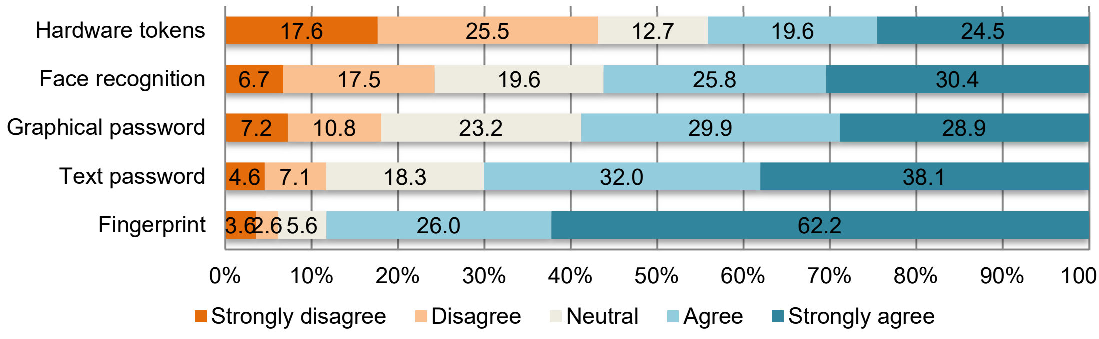


Figure 1. Perceived usability of five authentication methods

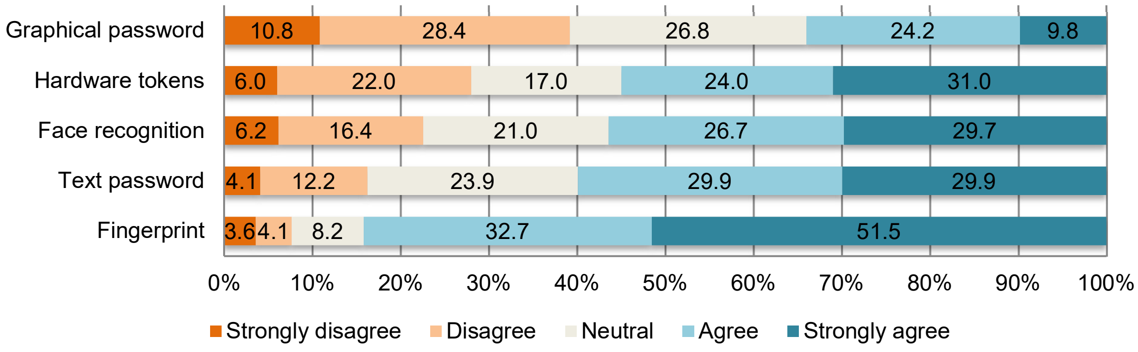


Figure 2. Perceived security of five authentication methods

The five authentication methods differed significantly in how usable (N=98, $\chi 2(4) = 66.6$, p = .000) and how secure (N = 97, $\chi 2(4) = 47.6$, p = .000) they were perceived. Post-hoc comparisons using Wilcoxon signed-ranks tests with Bonferroni corrections (p = 0.05/5 = 0.01) indicated the following significant results:

- *Fingerprint methods* had higher mean perceived **usability** (e.g., vs. text passwords, Z = -3.99, p = .000), and were also perceived significantly more **secure** (e.g., vs. face recognition, Z = -6.77, p = .000), than any of the other four methods.

- *Text passwords* were perceived significantly more **usable** than graphical passwords (Z = -2.71, *p* = .007), face recognition (Z = -3.48, *p* = .001) and hardware tokens (Z = -5.06, *p* = .000). However, they were only perceived significantly more **secure** than graphical passwords (Z = -6.26, *p* = .000).
- *Graphical passwords* were perceived more **usable** than hardware tokens (Z = -3.13, *p* = .002), however, less **secure** than face recognition (Z = -4.11, *p* = .000).

There was *no significant difference* in perception about usability or security of the five authentication methods between the observed *genders* or *academic majors*. Interestingly, students in B&H and Mexico only had a significantly different perception about the **usability** of *graphical passwords* (Mann-Whitney independent samples test: N=194, U=3880.0, Z = -2.2, p = .03), with participants from Mexico agreeing more strongly about the usability of this method (Figure 3: Mexico N = 100, mean rank = 105.7; BiH N = 94, mean rank = 88.8). Potential difference was also seen for fingerprint security, which students in Mexico perceived more positively (Mexico: N = 99, mean rank = 105.6; BiH: N = 97, mean rank = 91.3; U=4103.5, Z = -1.932, *p* = .053).

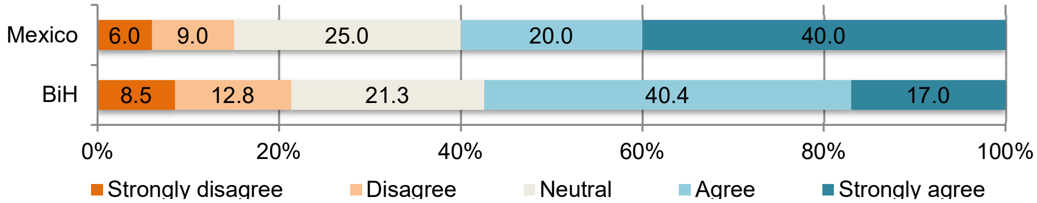
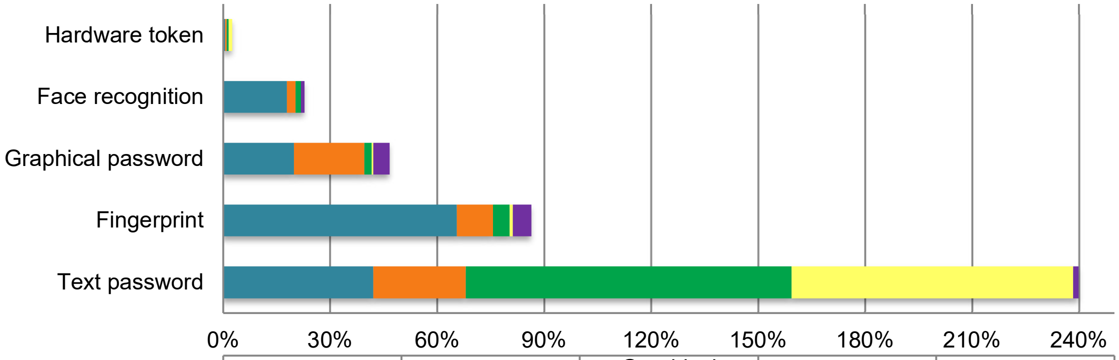


Figure 3. Graphical passwords' usability: Location-based comparison

4.3. Authentication methods' use on computer devices (RQ3)

We inquired about which of the five authentication methods our participants used for unlocking the common computer devices (Figure 4). Text passwords were by far the most frequently used method for accessing laptops (91.4%), desktops (79%), and tablets (25.9%). Fingerprint-based authentication, however, prevailed for unlocking smartphones (65.5%) and smartwatches (5.1%).



	Text password	Fingerprint	Graphical password	Face recognition	Hardware token
■ Smartphone	42.1%	65.5%	19.8%	17.8%	0.5%
■ Tablet	25.9%	10.2%	19.8%	2.5%	0.5%
■ Laptop	91.4%	4.6%	2.0%	1.5%	0.5%
■ Desktop	79.0%	1.0%	0.5%	0.0%	1.0%
■ Smartwatch	1.5%	5.1%	4.6%	1.0%	0.0%

Figure 4. Authentication methods used for unlocking computer devices

Previous studies (El-Abed *et al.,* 2010; Bhagavatula *et al.,* 2014; Zimmermann and Gerber, 2020) indicated that user perception of and adoption, or preferences for, authentication schemes are associated. We, therefore, tested the association between users' perception of a method's usability or security and its use on computer devices, in the context of Mexico and B&H. Our results showed a significant correlation between the prevalence of use across different devices (number of devices) and perceived usability for text passwords (N = 197, rho = .146, *p* = .041), graphical passwords (N = 194, rho = .192, *p* = .007), face recognition (N = 194, rho = .298, *p* = .000), as well as face recognition's perceived security (N = 195, rho = .205, *p* = .004), however, not for other methods.

4.4. Preferred criteria for creating text passwords (RQ4)

4.4.1. Prescribed text password guidelines and policies

The text password guidelines that were prescribed by literature and service providers, as presented to our participants, are in Appendix: Q5. The guidelines that the participants favored the most (Figure 5), in descending order, were: combining lower and uppercase letters, numbers and special characters (g2), minimum length of 8 characters (g3), and avoiding words that reference personal life (g1). The highest ranked guidelines were relatively equally used by participants in Mexico and B&H (Figure 6).

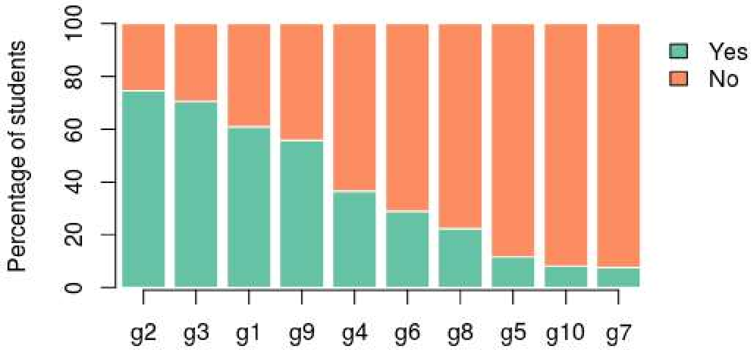


Figure 5. Use of prescribed guidelines

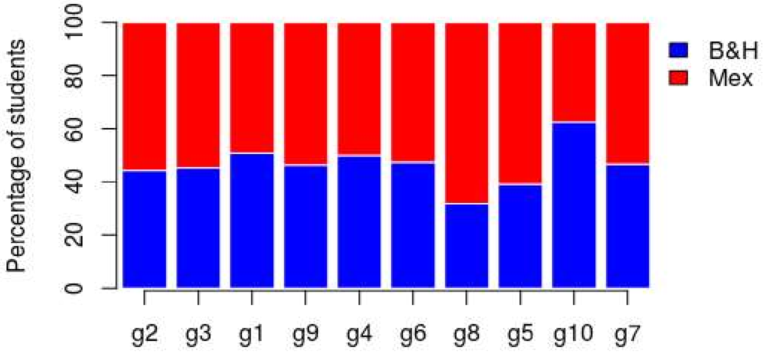


Figure 6. Location-based comparison of prescribed guidelines' use

4.4.2. Reasons for not adopting prescribed guidelines

The vast majority of participants (76.6%) claimed not to use one or more of the prescribed guidelines and reported their reasons. Similar reasons were aggregated into categories r1-r10, as shown in Table II. Interestingly, the main reason (r8) was having personal criteria for creating text passwords, mainly reported by participants in Mexico (71.4%).

The lack of trust in password generators/managers (r3) and lack of familiarity with these security and memory aids (r6) partially explains why our participants did not follow guidelines g7 and g8. The next most frequent rationale was the tendency to forget passwords when having to change them often (r2). This can explain why the guidelines to frequently change passwords (g5) and avoid password reuse (g6) were commonly not adopted.

Table II. Participants' reasons for not adopting the prescribed guidelines

Reason	Description	Mentions (%)
r1	Difficult to memorize too many passwords	13.1
r2	Forget passwords after multiple changes	13.6
r3	Lack of trust in password generators/managers	14.0
r4	Lazy to change/update different device	9.1
r5	No previous bad experience	1.8
r6	Lack of familiarity with password generators/managers	9.1
r7	Not important/necessary/relevant	12.7
r8	Use my own guidelines	22.2
r9	No particular reason	4.1
r10	Not suitable for me	0.5

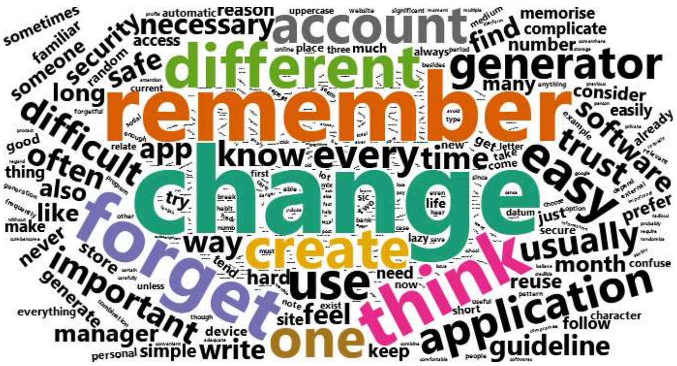


Figure 7. Word cloud of reasons for not adopting prescribed guidelines

Participants' reasons for not abiding by the prescribed guidelines are also presented in a word cloud (Figure 7). The most frequent words - change, remember, forget and think - confirm the previously mentioned text password memorability issues.

4.4.3. Participants' criteria for making memorable and secure text passwords

Most of our participants claimed they used their own criteria for creating text passwords. Table III ranks the 24 mentioned criteria according to frequency. 15 criteria were only security-related, three memorability-related and six related to both. Figure 8 shows how frequently the 10 highest ranked criteria were mentioned by participants in B&H versus those in Mexico.

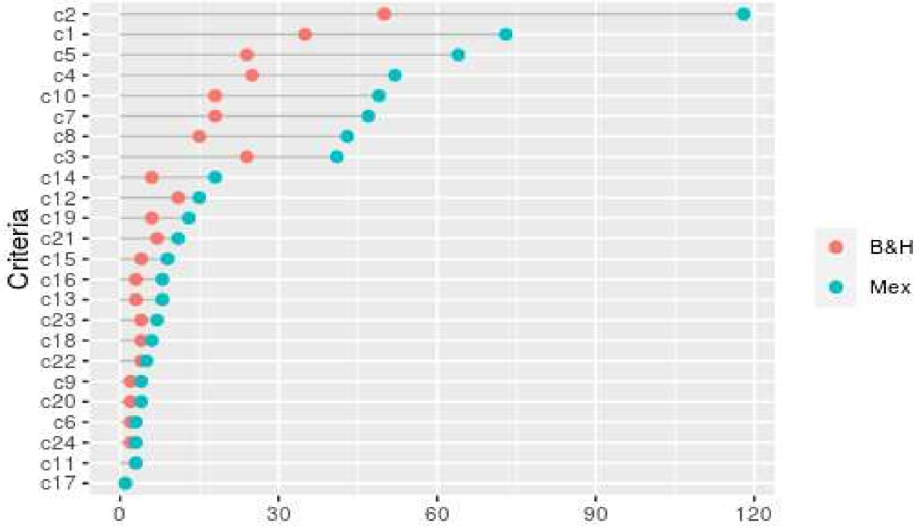


Figure 8. Frequency of mentioned criteria in B&H vs. Mexico

Table III. Participants' criteria for creating text passwords

Participants' criteria	Security/ Memorability	Related guidelines	Mentions (count)
c2. Numbers	S	g2	**118**
c1. Uppercase and lowercase letters	S	g2	**73**
c5. Long passwords	S	g3	**64**
c4. Special characters	S	g2	**52**
c10. Personal meaning words unknown to others	S, M	none	**49**
c7. Avoid reference to personal life/information	S	g1	**47**
c8. Real words	M	none	**43**
c3. Random letters	S	g2	**41**
c14. Use different passwords for different accounts	S	g4	**18**
c12. High complexity	S	g2, g3	**15**
c19. Hide passwords and do not share them	S	none	**13**
c21. Avoid writing them down	S	g9	**11**
c15. Group passwords according to importance of site	S, M	none	**9**
c13. Change often	S	g5	**8**
c16. Make passwords similar to others	S, M	none	**8**
c23. Use password managers	S, M	g8	**7**
c18. Avoid reusing old passwords	S	g6	**6**
c22. Use password generators	S	g7	**5**
c9. Translate random words or sentences	S, M	none	**4**
c20. Write on paper for backup	M	vs_g9	**4**
c6. Short passwords	M	vs_g3	**3**
c11. Creative	S, M	none	**3**
c24. Use two-step authentication	S	none	**3**
c17. Make password different from username	S	none	**1**

The highest ranked criteria correspond to the most popular guidelines from Section 4.4.1. That is, participants often reported the existing prescribed guidelines as their personal password creation criteria. 13 of the participants' personal criteria were directly related to a specific prescribed guideline (Table III). For example, uppercase and lowercase letters (c1), numbers (c2) and special characters (c4) correspond to the guideline for combining upper and lowercase letter, numbers, special characters (g2). High complexity (c12) was the only criterion related to more guidelines - g2 and g3. Importantly, two criteria - writing on paper for backup (c20) and short passwords (c6) – contradicted the guidelines, and nine criteria were newly introduced by our participants, e.g., using words of personal meaning that others do not know (c10).

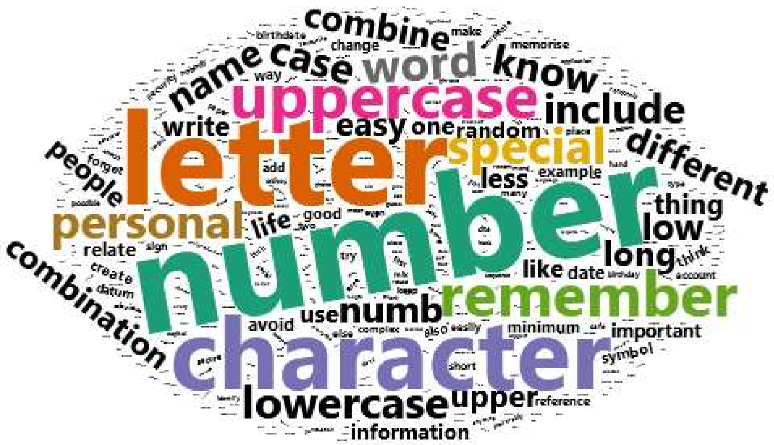


Figure 9. Word cloud of participants' criteria for text passwords

Figure 9 visualizes the personal criteria for secure and memorable passwords in a word cloud. Perhaps the most notable word is "remember" - pointing to the memorability aspect of passwords. The most frequent words - number, letter, character, remember, uppercase, etc. – stemmed from the highest ranked criteria (Table III), coinciding with the highest ranked guidelines (Section 4.4.1).

5. Discussion and conclusion

Research on user perspective about authentication schemes is limited (Velásquez *et al.,* 2018; Ryu *et al.,* 2021) and previous studies mainly focused on certain Western European, Asian or African countries (Section 2). To address these gaps, *we recruited participants from two previously unaccounted countries in South-East Europe and Latin America to gather user opinions about five authentication schemes*.

Unlike some prior studies which indicated differences in user attitude toward authentication methods, e.g., in the UK and India (Riley *et al.,* 2009), perceptions of participants in B&H and Mexico did not differ significantly. A slightly more positive perception of graphical passwords' usability and fingerprint security was noticed among students in Mexico, possibly as Mexican culture is more characterized by optimism and positive attitude (Hosftede Insights, 2021).

As seen in prior research (Zimmermann and Gerber, 2017; 2020), users in B&H and Mexico also mainly use text passwords for unlocking their computer devices. Our study further suggests that the prevalence of text passwords' use is associated with their perceived usability. Based on our results, authentication methods can be ranked by their perceived usability in descending order, as follows: fingerprint, text passwords, graphical passwords, face recognition, and hardware tokens. The two methods perceived to be the most usable by youth in B&H and Mexico were also perceived as the most secure. However, there could have been positive bias towards the familiar methods, particularly text passwords.

Although not explicitly studied in this paper, noteworthy is that the perceived security of some of the five authentication methods does not match their objective security levels. Zimmermann and Gerber (2020) pointed out a similar finding. Contrary to our findings about perceived security, hardware tokens satisfy most of the objective security criteria specified in (Bonneau *et al*., 2012; Zimmermann and Gerber, 2020). Moreover, token-based authentication's security outperforms most of the other methods, including fingerprints and text passwords. Graphical passwords have some security advantages over text passwords and fingerprints. While fingerprint-based authentication is better than passwords in only two of the 11 objective security criteria (Bonneau *et al.,* 2012).

The rest of this section discusses our results, grouped around the four research questions. The first two questions (**RQ1** and **RQ2**) explored user perception of usability and security of the five authentication methods. The vast majority of youth in B&H and Mexico agree that fingerprint-based authentication is usable and secure. In fact, the perceived usability and perceived security of *fingerprint* authentication is significantly higher than of the other methods assessed in our paper, which is in line with Zimmermann and Gerber's (2017; 2020) results. Although in fewer numbers, our participants also predominantly perceive *text passwords* as usable and secure. Text passwords outperform face recognition, graphical passwords and hardware tokens, however, primarily in terms of perceived usability. These text password usability results coincide with (Zimmermann and Gerber, 2020). Several prior studied (Bonneau *et al*., 2012; Katsini *et al*., 2016; Zhang-Kennedy *et al*., 2016) also indicated that text passwords' perceived usability and security were superior to some biometrics, graphical passwords and hardware tokens.

Face recognition's perceived usability and security are above average, which coincides with Bhagavatula *et al.* (2014), who highlighted high perceived security of face authentication. In comparison, *graphical passwords'* usability is favored by slightly more of our participants. Nevertheless, this method is the lowest ranked of the five on perceived security; the majority of youth in B&H and Mexico are neutral or disagree about its security. Furthermore, our participants are largely unfamiliar or do not use *hardware tokens* as an authentication method, and appear to perceive it as the least usable and among the least secure. Hence, our results need confirmation in further research, particularly as this method has among the highest objective security levels.

In **RQ3** we explored which of the five authentication methods youth in Mexico and B&H prefer to use for unlocking common computer devices. Our findings suggest that *text passwords* are the most frequently used authentication method, as shown in prior studied (Zimmermann and Gerber, 2017; 2020), and particularly for unlocking *laptop*, *desktop* and *tablet*. In line with (Zimmermann and Gerber, 2020), we saw a positive correlation between text passwords' use and their perceived usability, while an absence of correlation with perceived security. Hence, the prevalence of this scheme could likely be explained by its familiarity, general usability - ease of use (Zimmermann and Gerber, 2020) and personal information privacy (Zimmermann and Gerber, 2017), irrespective of the perceived security level. Moreover, as Al Abdulwahid *et al.* (2016) showed, service providers continue to rely on password authentication, and are slow in adopting alternative methods, although a rise in the use of biometrics is noticeable.

The other notable method, in terms of preference for use, is *fingerprint* authentication, as seen in (Zimmermann and Gerber, 2020). Importantly, fingerprints are the most frequently used method for accessing *smartphones* and *smartwatches*, which aligns with prior findings for online banking devices (Mirza *et al.,* 2018). Interestingly, the two schemes – text passwords and fingerprints - that most of our participants perceive as usable and secure, are also the ones they use the most for accessing their computer devices.

Youth in Mexico and B&H appear to use to some extent *graphical passwords* for *tablets* and *smart watches*, while *face recognition* for *smartphones* (likely due to the availability of integrated cameras). However, our correlation results for the latter method indicate that its low frequency of use is linked with its low perceived usability and security. The least used method for accessing computer devices among the youth population we focused on are *hardware tokens*, which coincides with findings for tokens in (Al Abdulwahid *et al.,* 2016).

The last research question (**RQ4**) aimed to identify the preferred criteria for creating text passwords. Given the popularity of text password use (Zimmermann and Gerber, 2020), including among our participants, we followed the earlier studies' recommendations to evaluate this method's memorability (Mackie and Yildirim, 2018) and security issues (Katsini *et al*., 2016; Zhang-Kennedy *et al*., 2016). Youth in Mexico versus those in B&H are not significantly different in how they adopt or perceive text password guidelines that literature and service providers prescribe (Section 2 and 4.4.1). Students in Mexico are somewhat more inclined to frequently change passwords and use password managers, while those in B&H tend more to avoid the use of any guidelines, unless explicitly required. The inclinations of the homogenous Mexican student group could be ascribed to it cultural factor of uncertainty avoidance, i.e., transferring responsibility, and ensuring known outcomes (Hofstede Insights, 2021).

Overall, in creating their passwords, the majority of our participants: combine lower and uppercase letters; use numbers, special characters, and more than 8 characters; avoid using words that reference their personal life; and keep them out of sight from other people. Transferring password generation or management to automated tools is, however, not well accepted. Lack of trust in or familiarity with such tools is one of the main reasons for not using the latter guidelines. Other common reasons for not abiding by the different guidelines include memorability-related issues, e.g., use of different passwords or changing them often (Gaw and Felten, 2006; Florencio and Herley, 2007). Human memory limitations explain users' tendencies to waive existing policies and hence devise their own password creation criteria.

Interestingly, however, one fifth of the reported personal criteria for creating text passwords coincide with the existing password guidelines. The highest ranked personal text password criteria correspond to the most popular prescribed guidelines. For example, these include the use of numbers, uppercase and lowercase letters, long passwords, special characters, avoiding reference to personal life/information, and words of personal meaning unknown to others. Moreover, the remaining personal criteria, e.g., real words and random letters, could also be extracted from, or achieved by, the existing guidelines. Therefore, although our participants perceive their criteria as their own, it is likely that the personal criteria is influenced by the externally prescribed text password guidelines.

Finally, our findings imply that users are more inclined to adopt text password criteria that provide security over those for memorability. Nevertheless, "remember" was among the most frequent words in the personal criteria. This suggests that text passwords are still popularly used for their usability, however, users account for the security of this method via the criteria they apply when generating their passwords, although they strive to minimize the memory load.

5.1. Limitations and future work

A few limitations apply to this study. The participant sample was imbalanced. It was slightly biased towards students from Mexico. Moreover, the sample from B&H was not homogeneous, it included Bosnian, as well as international students. Hence, this research focused on location-based comparison. Although, it would be interesting to explore the effect of Mexican and B&H culture on the use of authentication methods in future studies with balanced data.

This study's participants were university students, as young adults were found to be the most frequent users of computer devices and online services (Xiao *et al.,* 2014). Moreover, the majority were studying computing-related courses, hence, it is likely they were more informed and skilled in authentication approaches. For generalization purposes, future work could expand the participant pool to other demographic groups.

Online survey questionnaires were commonly used as data collection instruments in related work (Furnell and Evangelatos, 2007; Mackie and Yıldırım, 2018), and were thus adopted in this study. However, observing and evaluating actual use of authentication schemes in a lab (Zimmermann and Gerber, 2020) or field experiment, particularly in longitudinal studies, could provide further insights on this topic.

In RQ3, we asked participants about text password use for accessing computer devices. PINs were not mentioned. However, commonly, passwords for unlocking laptop and desktop are alphanumeric, while on smartphones they are numeric and shorter, which could influence the perceived security and/or usability of a method. Thus, a clearer, more explicit differentiation between text/alphanumeric and PIN/numeric password-based methods should be made in future research.

The wording of the survey questions Q6 and Q7 (see Appendix) should have been more explicit in the instructions. For Q6, only a few participants justified every guideline they did not abide by. Q7 did not specify to report only personal criteria for text password creation that is different than the prescribed guidelines, due to which most of the criteria coincided with the guidelines. However, the advantage was this provided unexpected information about user habits in relation to RQ4.

Finally, we studied user perception about a limited number of the currently most frequently available or investigated authentication schemes. Future research could expand the variety of schemes addressed and have a balanced representation of methods for each category.

5.2. Conclusion

This paper explored the perceived usability and security, and the use of five authentication methods. The primary **contribution** of our study is that it *gives an insight into perceptions and preferences of users from geographic locations that have not been addressed in prior literature*. It further contributes by showing that youth in B&H and Mexico are aware of and adopt various authentication methods, including the security guidelines for password-based methods. Moreover, that users in B&H and Mexico appear to favor text passwords and fingerprint-based biometric methods, similar to what was seen in prior research applied in other geographic contexts (Zimmermann and Gerber, 2020).

197 responses were collected from university students in B&H and Mexico via an online survey-questionnaire in 2019. Our findings imply that fingerprint authentication is perceived as the most usable and secure method. However, text passwords are the most frequently used method among young adults across continents, and the perceived usability and security of this method is still highly regarded. The results also suggest that password policies imposed on users are not necessarily the most effective. Personal criteria for text password creation are preferred, however, they mainly match the existing password guidelines. Therefore, text password guidelines should serve simply as guidelines, to raise security awareness, and to assist users to develop their own more memorable criteria, that will hence be more likely abided by.

On the other hand, it is evident that young, tech savvy users of various computer devices are becoming more inclined toward biometric methods, due to their perceived high security, as well as accessibility for different user types, including those with disabilities. The rising popularity of biometric schemes is supported by the embedded sensors and tools (e.g., for voice-, gesture-, face-recognition) in mobile computing devices. This study was performed in Spring 2019, while privacy concerns and reluctance to share biometric data might have persisted, including among young users. The privacy concerns about providing, storing and using biometric data, and the potential negative effects on biometric methods' adoption, was also seen in prior studies (Mirza *et al.,* 2018). Nevertheless, it would be interesting to explore whether Covid-19, the resulting proliferation of online activities and greater willingness to use cameras and microphones, influenced changes in user perception and prevalence of adoption of biometric authentication schemes.

In conclusion, our study can be used to inform future research on authentication methods. Moreover, our findings suggest common trends in perceptions and preferences of users around the world. Therefore, they can serve as *practical implications* for the direction of authentication scheme development. Cybersecurity organizations, including government institutions, need to consider the barriers to adoption, raising user awareness about the objective security of the different authentication schemes, however, also direct more attention to improving the methods that users persist in and are more inclined to use.

References

Abbott, J., Calarco, D. and Camp, L.J., 2018, March. Factors influencing password reuse: A case study. In *Telecommunications Policy Research Conference on Communications, Information and Internet Policy (TPRC 46). DOI: http://dx. doi. org/10.2139/ssrn* (Vol. 3142270).

Abuhamad, M., Abusnaina, A., Nyang, D. and Mohaisen, D., 2020. Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet of Things Journal*, *8*(1), pp.65-84.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C., 2016. Continuous and transparent multimodal authentication: reviewing the state of the art. *Cluster Computing*, *19*(1), pp.455-474.

Al-Harby, F., Qahwaji, R. and Kamala, M., 2009, September. The effects of gender differences in the acceptance of biometrics authentication systems within online transaction. In *2009 International Conference on CyberWorlds* (pp. 203-210). IEEE.

Alkaldi, N. and Renaud, K., 2019, January. Encouraging password manager adoption by meeting adopter self-determination needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Andriotis, P., Oikonomou, G., Mylonas, A. and Tryfonas, T., 2016. A study on usability and security features of the android pattern lock screen. *Information & Computer Security*.

Bhagavatula, Ch., Iacovino, K., Kywe, S.M., Cranor, L.F. and Ur, B., 2014. Poster: Usability analysis of biometric authentication systems on mobile phones. In *Proceedings of the 10th Symposium on Usable Privacy and Security* (pp. 1-2).

Bhana, B. and Flowerday, S., 2020. Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security*, *96*, p.101925.

Biddle, R., Chiasson, S. and Van Oorschot, P.C., 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), pp.1-41.

Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F., 2012, May. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553-567). IEEE.

El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C., 2010, October. A study of users' acceptance and satisfaction of biometric systems. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 170-178). IEEE.

Ferrag, M.A., Maglaras, L., Derhab, A. and Janicke, H., 2020. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommunication systems, 73(2), pp.317-348.

Florencio, D. and Herley, C., 2007, May. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666).

Furnell, S. and Evangelatos, K., 2007. Public awareness and perceptions of biometrics. *Computer Fraud & Security*, *2007*(1), pp.8-13.

Gaw, S. and Felten, E.W., 2006, July. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44-55).

Grawemeyer, B. and Johnson, H., 2011. Using and managing multiple passwords: A week to a view. *Interacting with computers*, *23*(3), pp.256-267.

Guo, Y., Zhang, Z. and Guo, Y., 2019. Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, pp.423-435.

Hofstede Insights (2021). “Country comparison”, available at: https://www.hofstede-insights.com/country-comparison/bosnia-and-herzegovina,mexico/ (accessed 17 June 2021)

ISO 9241-11:2018(en), “Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts”, available at: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en (accessed 17 June 2021).

Katsini, C., Belk, M., Fidas, C., Avouris, N. and Samaras, G., 2016, November. Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics* (pp. 1-6).

Lee, H., Kang, D., Ryu, J., Won, D., Kim, H. and Lee, Y., 2020. A three-factor anonymous user authentication scheme for Internet of Things environments. *Journal of Information Security and Applications*, *52*, p.102494.

Li, C., Jing, J. and Liu, Y., 2021, March. Mobile user authentication-Turn it to unlock. In 2021 6th International Conference on Mathematics and Artificial Intelligence (pp. 101-107).

Mackie, I. and Yıldırım, M., 2018, July. A novel hybrid password authentication scheme based on text and image. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 182-197). Springer, Cham.

Mathis, F., Fawaz, H.I. and Khamis, M., 2020, April. Knowledge-driven Biometric Authentication in Virtual Reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-10).

Mirza, Z., Alsalem, E., Mohsin, F. and Elmedany, W.M., 2018. Users' Acceptance of Using Biometric Authentication System for Bahrain Mobile Banking. *KnE Engineering*, pp.102-121.

Nelson, D.L., Cermak, L. and Craik, F., 1979. Remembering pictures and words: Appearance, significance and name. *Levels of processing in human memory*, pp.45-76.

Raptis, G.E., Katsini, C., Cen, A.J.L., Arachchilage, N.A.G. and Nacke, L.E., 2021, May. Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K., 2019. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)* (pp. 357-370).

Riley, C., Buckner, K., Johnson, G. and Benyon, D., 2009. Culture & biometrics: regional differences in the perception of biometric authentication technologies. *AI & society*, *24*(3), pp.295-306.

Ryu, R., Yeom, S., Kim, S.H. and Herbert, D., 2021. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. *IEEE Access*.

Sasse, M.A., 2005. Usability and trust in information systems. Edward Elgar.

Shafique, U., Sher, A., Ullah, R., Khan, H., Zeb, A., Ullah, R., Waqar, S., Shafi, U., Bashir, F. and Shah, M.A., 2017. Modern authentication techniques in smart phones: Security and usability perspective. *IJACSA International Journal of Advanced Computer Science and Applications*, *8*(1), pp.331-340.

Sinigaglia, F., Carbone, R., Costa, G. and Zannone, N., 2020. A survey on multi-factor authentication for online banking in the wild. *Computers & Security*, *95*, p.101745.

Velásquez, I., Caro, A. and Rodríguez, A., 2018. Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, pp.30-37.

Wang, D., Zhang, X., Zhang, Z. and Wang, P., 2020. Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & Security*, *88*, p.101619.

Woods, N. and Siponen, M., 2019. Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*, pp.61-71.

Xiao, N., Sharman, R., Rao, H.R. and Upadhyaya, S., 2014. Factors influencing online health information search: An empirical analysis of a national cancer-related survey. *Decision Support Systems*, 57, pp.417-427.

Zhang-Kennedy, L., Chiasson, S. and van Oorschot, P., 2016, June. Revisiting password rules: facilitating human management of passwords. In 2016 APWG symposium on electronic crime research (eCrime) (pp. 1-10). IEEE.

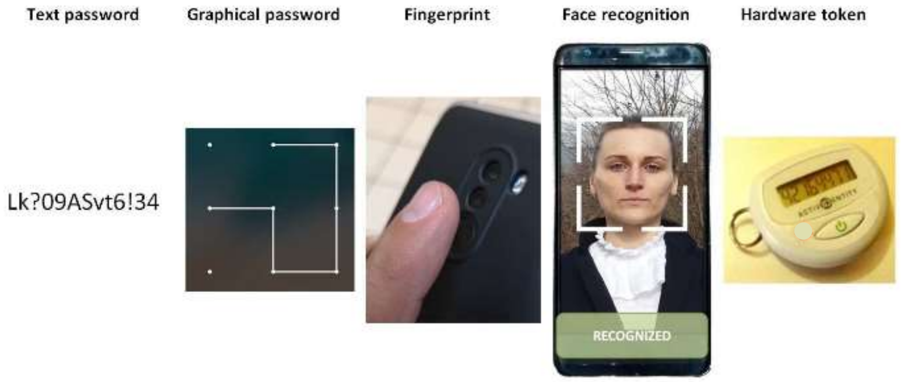
Zimmermann, V. and Gerber, N., 2017, July. "If It Wasn't Secure, They Would Not Use It in the Movies"–Security Perceptions and User Acceptance of Authentication Technologies. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 265-283). Springer, Cham.

Zimmermann, V. and Gerber, N., 2020. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, pp.26-44.

Appendix: Survey questionnaire

Q1/Q2. For each of the following authentication methods, please rate to what extent you disagree/agree with the statement:
I think this authentication method is very USABLE.

(Note: Q2 had the same wording and response options, however for the statement: *I think this authentication method is very SECURE.)*



Q3. Select which authentication methods you use for unlocking each of the following computer devices.

	Text password	Graphical password	Fingerprint	Face recognition	Hardware token	N/A
Smartphone						
Tablet						
Laptop						
Desktop						
Smart watch						

Q4. If you have stated above that you only use text passwords as an authentication method on all your devices, please explain why that is.

Q5. The following are guidelines for creating passwords. Please select all the guidelines that you use in creating your passwords:

- □ (g1) Avoid using words that reference your personal life in any way.
- □ (g2) Even when not mandatory, you create your passwords as a combination of upper and lower case letter, numbers, special characters, etc.
- □ (g3) Even when not mandatory, you create your passwords with a minimum length of 8 characters.
- □ (g4) Use different passwords for all your online accounts and computer devices.
- □ (g5) Change your passwords every 1-3 months.
- □ (g6) Avoid reusing the passwords you previously used.
- □ (g7) Use password generator applications to create randomized passwords for you.
- □ (g8) Use password manager software for password storing.
- □ (g9) Avoid writing your passwords down on post-it notes (or other places visible to a passersby)
- □ (g10) I do not use any of the listed guidelines, unless required.

Q6. For all the guidelines you have not selected, please explain why you choose not to follow those guidelines in creating passwords.

Q7. If you were asked to specify guidelines for creating memorable and secure text passwords, what would your criteria be? Make your own list.