Edge Hill University

Addressing the problem of insecure keyboard-derived patterns in user-generated passwords and PIN codes with a focus on smartphone users

Student Name: Veronika Chupova

The statement: 'This document is a part of the Dissertation Report for a Master's Computer Science Degree at Edge Hill University. The publication aims to present the research results to the participants and can't be utilised for any other use.'

Abstract

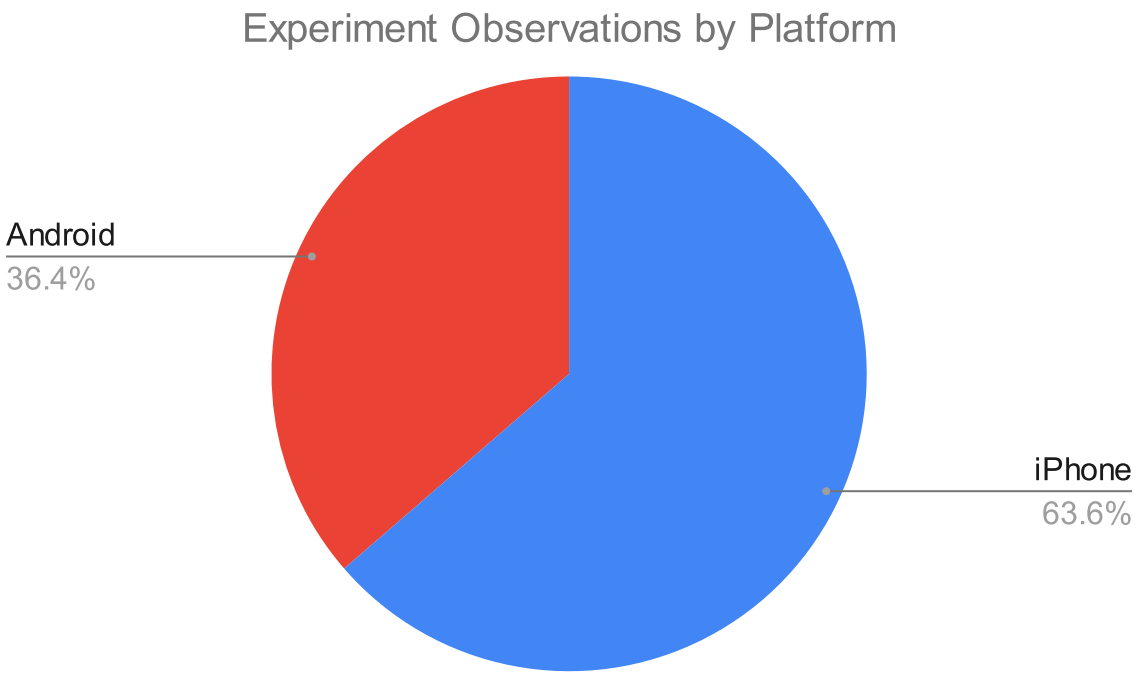
As online services become integral to daily life, the importance of robust data protection mechanisms, particularly password security, is undeniably critical. Despite early predictions of the refusal of passwords, they remain a primary line of defence against unauthorised access. However, the inherent simplicity of passwords often leads to vulnerabilities, as users frequently employ weak or repetitive combinations that are susceptible to cyberattacks. This study addresses the challenge of keyboard-derived patterns in passwords and PIN codes, particularly among smartphone users, through the innovative application of a keyboard shuffling algorithm. The research aims to enhance password strength by eliminating predictable sequences inherent in standard keyboard layouts. A mixed-methods approach was employed, combining qualitative and quantitative data collection, including a literature review of existing methodologies, algorithm development, and experimental validation. The findings reveal that the shuffled keyboard significantly mitigates the use of common patterns, resulting in stronger passwords and PIN codes as assessed by established password strength meters, including NIST entropy, Bitwarden and zxcvbn test. This research contributes to the field of cybersecurity by offering insights into user behaviour regarding password creation and by demonstrating the potential of shuffled input methods to improve security against prevalent vulnerabilities related to traditional keyboard layouts.

Results Evaluation

Data Statistical Analysis

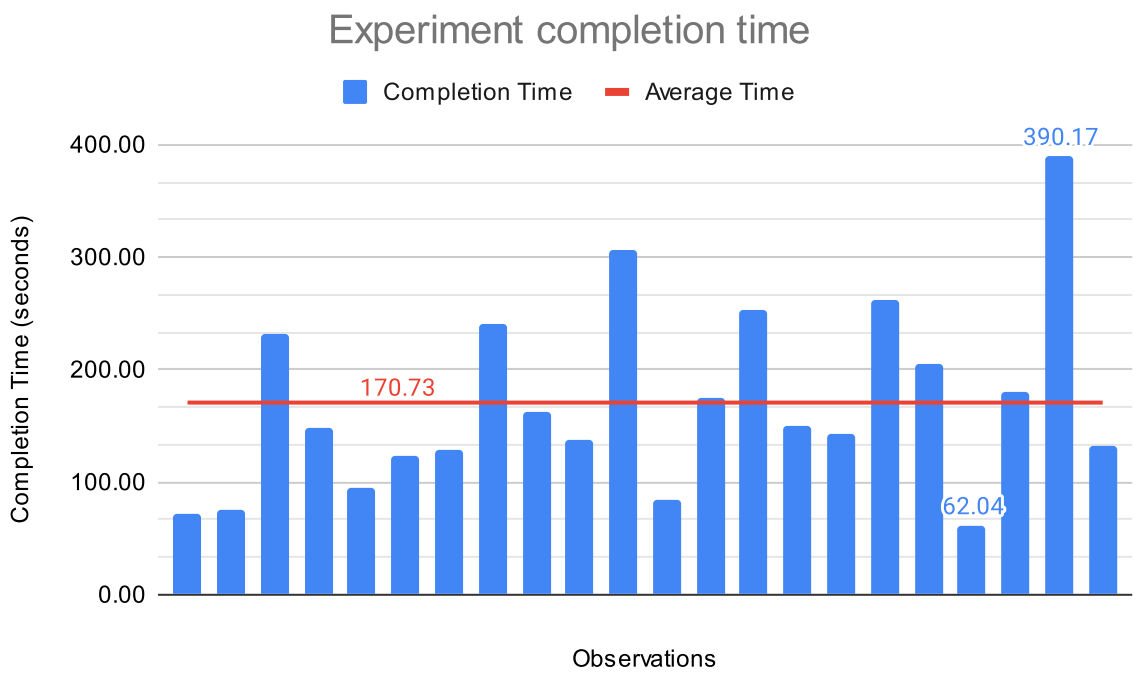
Within the experiment phase of the study, primary data was collected from a total of 22 participants. An initial analysis was conducted to verify that each entry contained a complete dataset as outlined in the Data Collection section of this report. As expected, the web application was accessed from only two mobile platforms: Android and iOS, as shown in Figure 1. Although the UserAgent method did not provide specific model information for Android devices, iOS devices were clearly identified as iPhone smartphones.

Figure 1. Source platform analysis



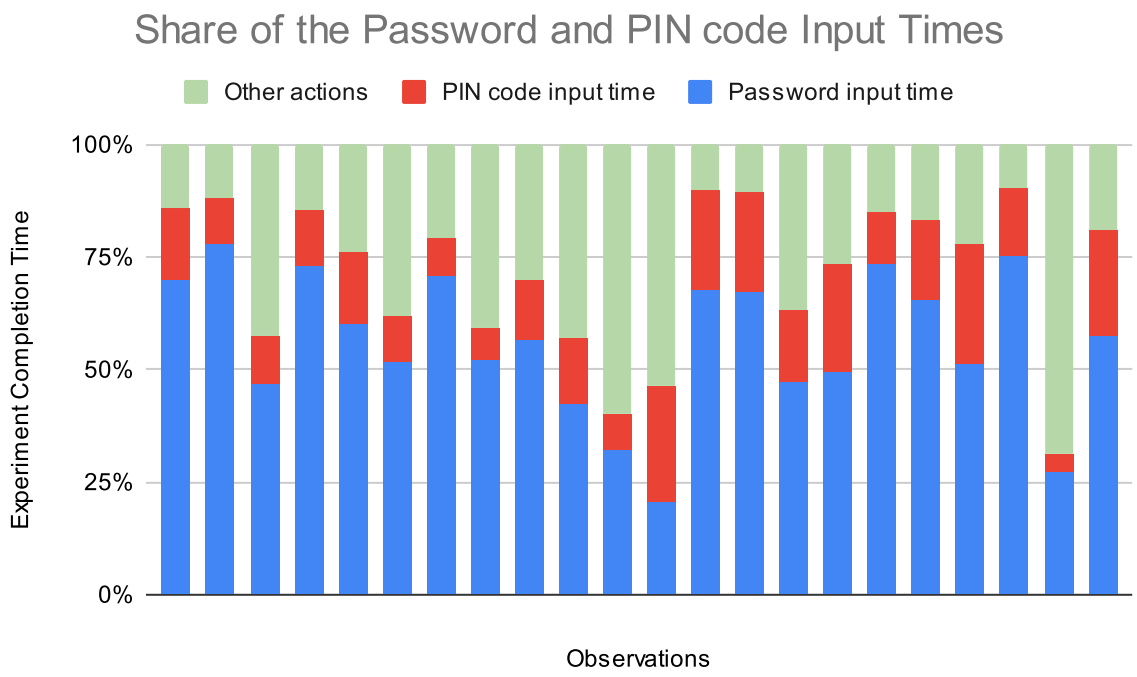
The timestamps of participants' navigation actions within the experiment platform were analysed to determine the time each user spent on every page of the web application. As shown in Figure 2, the time participants took to complete the experiment varied widely, with an average of 170.73 seconds (s) and a standard deviation of 82.81 s. The longest time a participant spent on the web application was 390.17 s or approximately 6.5 minutes, while the shortest time was 62.04 s, roughly 1 minute.

Figure 2. Experiment completion time analysis



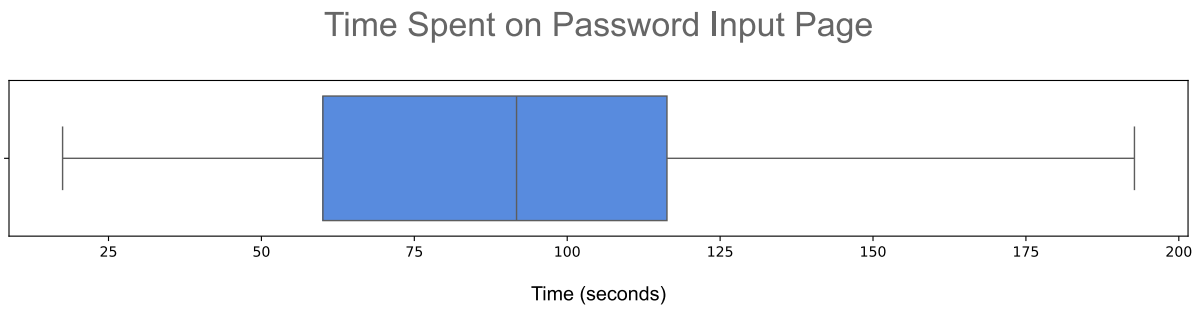
A more detailed analysis of page statistics reveals that most participants spent around half or more of their total experiment time on the password input page, significantly longer than the time spent on the PIN code input page. This likely indicates that interacting with the concise numpad was much easier for participants compared to using the full-scale shuffled keyboard. The data is illustrated in Figure 3.

Figure 3. Experiment actions time analysis



Earlier, Liu et al (2013) evaluated the time it took for individuals to enter passwords on a smartphone touchscreen using the classic QWERTY keyboard, with times ranging from 7 to 117 seconds and half of the observations (interquartile range) falling between 14 and 23 seconds. However, the data from the current experiment shows a significant shift in the interquartile range compared to the authors' findings, with the first quartile (Q1) at 60.056 seconds and the third quartile (Q3) at 116.311 seconds, as illustrated in Figure 4. Notably, the upper bound of the interquartile range in this study is very close to the maximum time participants needed to input a password using the standard QWERTY keyboard in the prior research. This suggests that participants encountered confusion and difficulty when interacting with the unfamiliar shuffled keyboard.

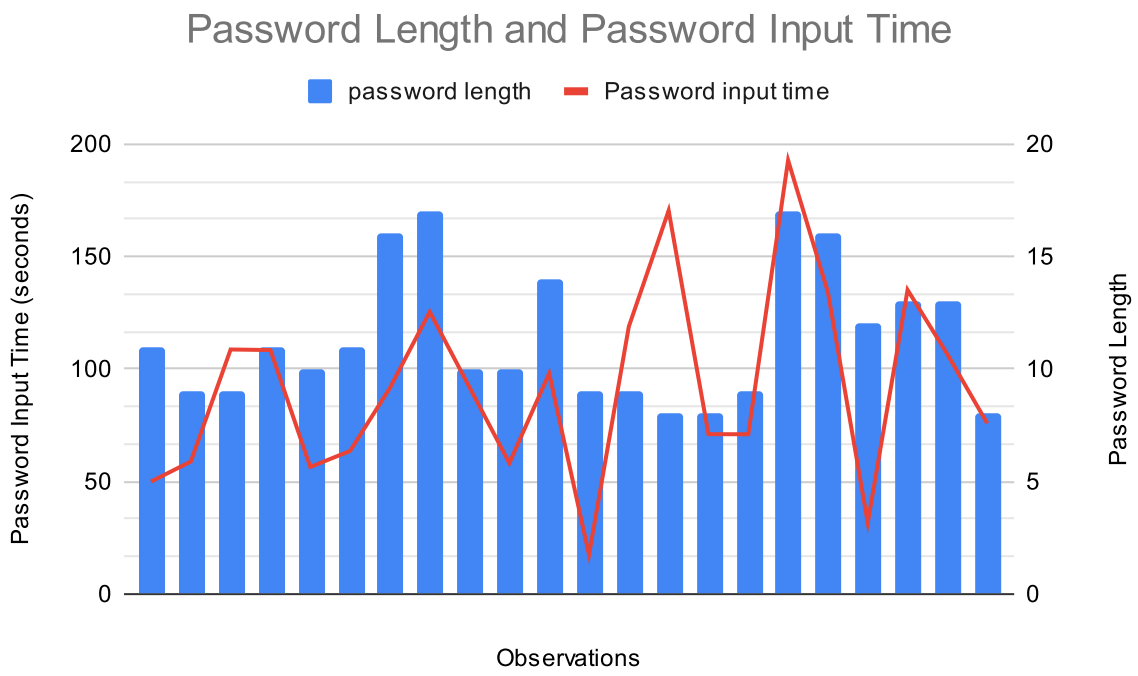
Figure 4. Password input time dispersion



On the other hand, the analysis of the relationship between password length and input time, shown in Figure 5, suggests that the longer time taken to enter passwords

in this experiment may not be solely due to the extra time spent searching for characters on the shuffled keyboard. In fact, the correlation between these two variables is 0.44, which is considered the lower bound of a moderate correlation. However, the primary data collected in the experiment does not provide enough detail to explore this issue further.

Figure 5. Password input time and password length relation



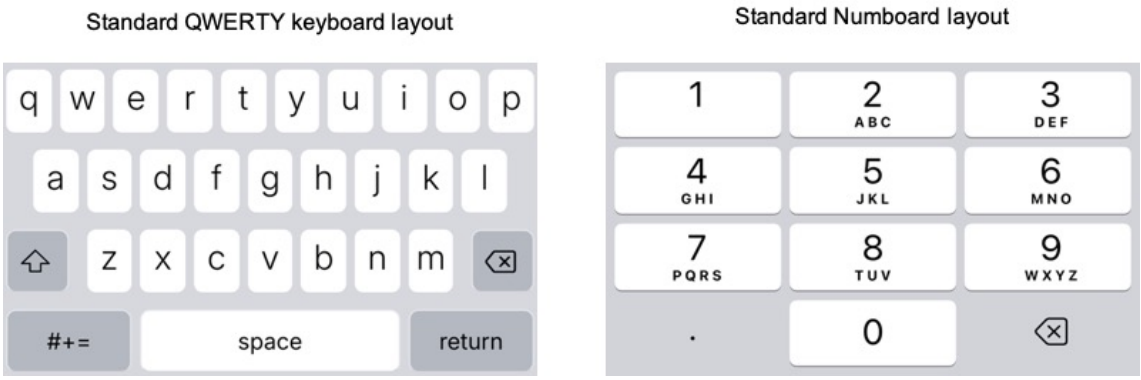
Finally, an analysis of the composition of the collected passwords and their compliance with the study's password policy was conducted. Since the password requirements were strictly enforced—meaning participants could not proceed without providing a valid password—all strings met the criteria of being at least 8 characters long and containing at least 1 digit, 1 uppercase letter, and 1 lowercase letter. However, 19 of the passwords (86%) exceeded the minimum length requirement, with 4 of them including optional special symbols. This suggests that most participants likely aimed to create meaningful, secure passwords rather than simply entering random strings to proceed.

Passwords Sequential Pattern Analysis

This section focuses on the final objective of the research and assesses its accomplishment. To this end, the passwords and PIN codes collected during the experiment were analysed for character sequences (patterns) derived from the

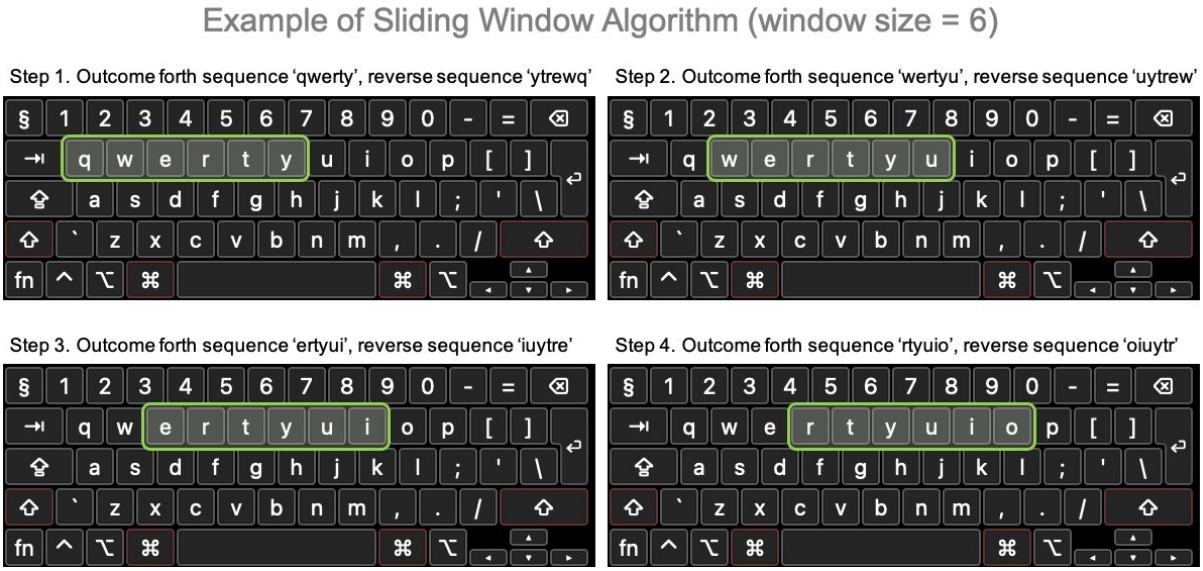
standard QWERTY keyboard layout and the classic grid numpad, as shown in Figure 6.

Figure 6. Standard layouts of QWERTY keyboard and numpad



A specialised function was developed to analyse passwords for frequent patterns derived from the standard keyboard layout. This method was built on the algorithm used to validate the quality of keyboard shuffling, discussed in the earlier section of this report "Shuffling Algorithm." The core concept of this algorithm is a sliding window that consequently moves through the rows of the standard keyboard layout, as shown in Figure 7, searching for sequences, forward and reversed, included in passwords. In this task, the window size varied gradually from the length of an entire keyboard row down to three characters.

Figure 7. Sliding window algorithm visualisation



The analysis identified two instances where standard keyboard patterns were present in passwords entered using the shuffled keyboard:

- The forward pattern "ert"
- The reversed pattern "987"

However, a closer examination of these two patterned passwords revealed that the "ert" sequence was part of a dictionary word, and "987" was part of the number 1987, likely referencing a year. Therefore, it can be concluded that no intentional QWERTY keyboard patterns were incorporated into the passwords created with the experimental shuffled keyboard.

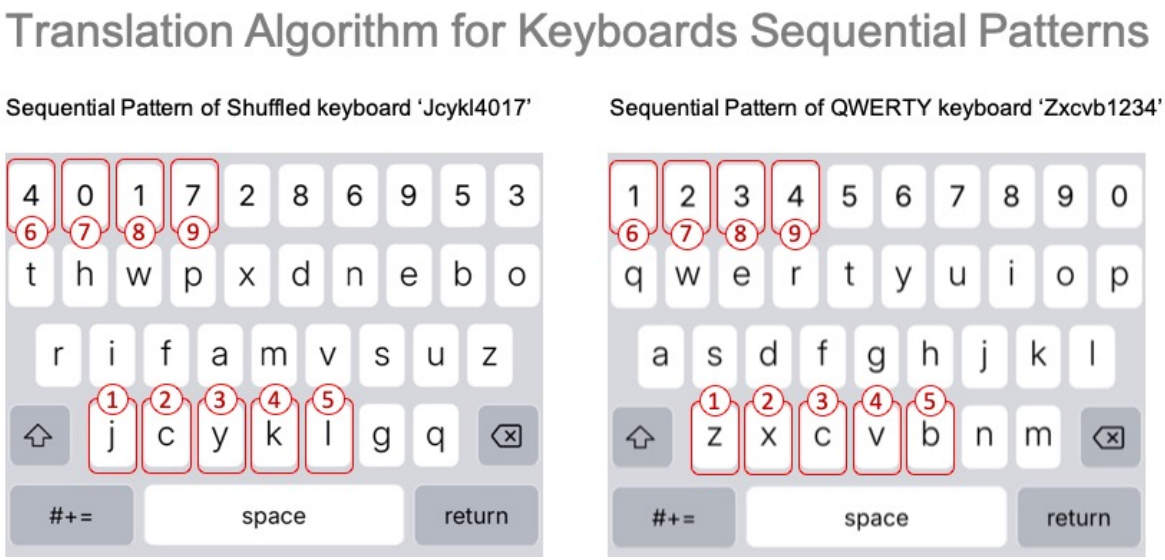
An additional analysis was conducted on the collected data to identify any positional patterns specific to the shuffled keyboard variant used for entering each password. A function was developed for this assessment, utilising the same sliding window algorithm. The only difference was that the keyboard lines analysed were taken from the shuffled keyboard variant, which was unique to each participant in the experiment. This analysis uncovered four instances where shuffled keyboard patterns were incorporated into passwords:

- Forward pattern “Oetjrlp”
- Forward pattern “048716”
- Forward pattern “Nkvpoy”
- Reverse pattern “168”

None of these patterns appears to carry any meaningful connotation and was likely included in the corresponding passwords as a result of habitual behaviour to input sequentially positioned characters, as discussed earlier in this report. Additionally, the sequences ‘048716’ and ‘Nkvpoy’ were part of the same password, clearly indicating the participant's intention to use this approach.

For each password containing sequential strings derived from the shuffled keyboard, a corresponding set of characters from the standard QWERTY keyboard was generated by maintaining the same positional order of the characters. The visual representation of this translation method is shown in Figure 8.

Figure 8. Translation algorithm for keyboard positional sequential patterns



To evaluate the security of passwords containing sequential patterns from the shuffled keyboard, three widely used Password Strength Meters (PSM) were utilised: NIST entropy, Bitwarden, and the zxcvbn test. The latter, proposed by Wheeler and Lowe (2016) and later adopted by Dropbox, is regarded as the most reliable, according to Thanh and Tanaka (2024). The translated strings, where the sequential patterns from the shuffled keyboard were mapped onto QWERTY keyboard sequences, were also assessed using these PSMs to identify any differences in their robustness. Table 1 presents the strength evaluation results for each password containing a sequential pattern. Though, each employed PSM applies own measurement system, the overall principle doesn't change—the more points gained, the stronger the string. Additionally, the zxcvbn test provides roughly estimated time

Table 1. Sequenctial strings' strength comparison

		NIST Entropy	Bitwarden	zxcvbn test
Password #1 with pattern 'Oetjrlp'	Original string	31.5	good	3/4 (centuries)
	QWERTY representation	25.5	very weak	1/4 (6 days)
Password #2 with patterns '048716' and 'Nkvpoy'	Original string	36	strong	4/4 (centuries)
	QWERTY representation	30	very weak	1/4 (4 days)
Password #3 with pattern with '168'	Original string	31.5	good	3/4 (centuries)
	QWERTY representation	31.5	weak	2/4 (8 years)

Evidently, the poor practice of incorporating positional keyboard sequences leads to the creation of strong, secure passwords when using the shuffled keyboard proposed

in this study. However, the same sequences on a standard QWERTY keyboard result in weak passwords that are vulnerable to both brute force and dictionary attacks.

The remaining 19 passwords that don't contain positional keyboard patterns were also assessed with the aforementioned meters and results are placed in Table 2. While about 70% of them are considered sufficiently robust (good and higher in Bitwarden, 3 and 4 in the zxcvbn test), 30% were marked as not secure. It is worth mentioning that the majority of these passwords include dictionary words and, thus, may appear in existing password dictionaries which explains the reached marks. However, the genuine reason for each mark is left unexplored in this study because it falls out of the research goal.

Table 2. Passwords strength

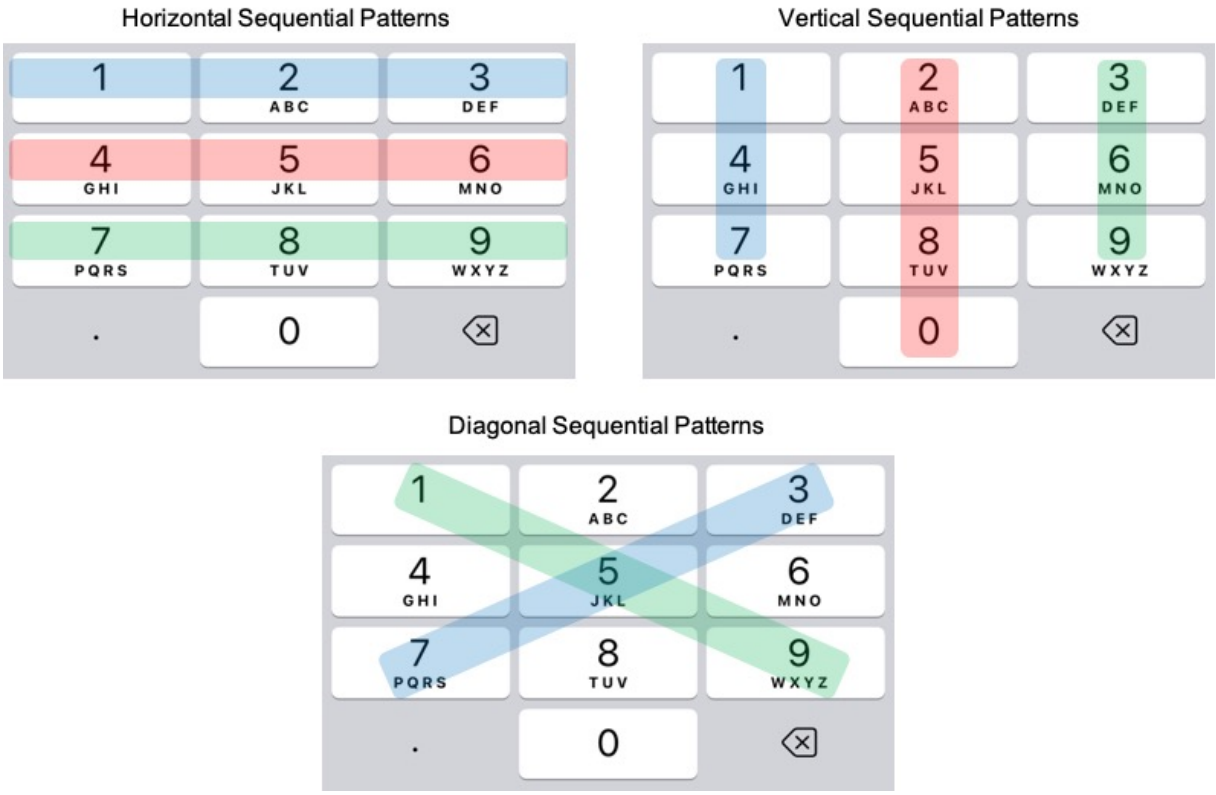
	NIST Entropy	Bitwarden	zxcvbn test
Password #1	28.5	good	3/4 (centuries)
Password #2	25.5	good	3/4 (centuries)
Password #3	28.5	strong	4/4 (centuries)
Password #4	27	weak	2/4 (7 years)
Password #5	28.5	weak	2/4 (5 years)
Password #6	36	strong	4/4 (centuries)
Password #7	43.5	strong	4/4 (centuries)
Password #8	33	good	3/4 (centuries)
Password #9	27	very weak	1/4 (1 month)
Password #10	33	strong	4/4 (centuries)
Password #11	25.5	good	3/4 (centuries)
Password #12	24	weak	2/4 (centuries)
Password #13	24	weak	2/4 (centuries)
Password #14	25.5	good	3/4 (centuries)
Password #15	43.5	strong	4/4 (centuries)
Password #16	36	strong	4/4 (centuries)

Password #17	31.5	strong	4/4 (centuries)
Password #18	37.5	strong	4/4 (centuries)
Password #19	24	weak	2/4 (centuries)

PIN codes Sequential Pattern Analysis

The common sequential patterns on the numpad follow the same principles as those on the keyboard, previously discussed in this work. The key differences lie in the shorter sequence lengths, due to the more compact layout of the standard numpad's rows, and the widespread usage of additional patterns created by vertical and diagonal sequences, as shown in Figure 9.

Figure 9. Numboard positional sequentional patterns visualisation



A specific function was developed to identify numpad patterns in the collected 4-digit PIN codes. Unlike the function used for password analysis, which included extracting keyboard sequences, this function focused solely on accelerating the search for patterns, as the number of possible sequences, both forward and reversed, is relatively small.

Surprisingly, not a single sequence derived from the standard numpad was found in the collected PIN codes entered using the shuffled numpad during the experiment. This suggests that the natural numerical order and familiar sequences from the standard numpad did not influence participants' choices when selecting their PIN codes.

To investigate whether the provided 4-digit codes were influenced by positional patterns, as illustrated in Figure 9, each entry was analysed using a similar function. This time, the search focused on positional pattern sequences, both forward and reversed, derived from the unique shuffled numpad variant presented to each participant.
The analysis revealed only one instance where a vertical pattern, represented by the string '410', was incorporated into a PIN code. However, the private research by Datagenetics.com (2012), showed that this sequence is not included in the top 20 most frequently used PIN codes, which account for 26.83% of the 3.4 million samples analysed by the author.
These findings suggest that using the shuffled numpad for PIN code entry effectively prevents the inclusion of easy-to-guess, frequent patterns from the standard numpad layout, thereby strengthening PIN codes against dictionary attacks.

Conclusion

This study offers an in-depth exploration of how keyboard layout affects the strength of user-generated passwords and PIN codes, using shuffling techniques to enhance their security.

At the beginning, the importance of password strength for comprehensive data protection was emphasised, and the vulnerabilities of traditional security methods were identified. The study aimed to use shuffled keyboard layouts to eliminate weak password and PIN combinations, ultimately improving the strength of user-generated strings.

To accomplish this, a novel algorithm for keyboard shuffling was developed. The method incorporates the well-known Sattolo algorithm, along with a specifically designed entropy assessment algorithm, to shuffle the character sequences of the standard keyboard and numpad, generating sufficiently randomised layouts.

The experiment results showed that using this shuffled keyboard for password entry effectively eliminated the frequent sequences typically associated with the standard QWERTY layout. Additionally, the shuffled keyboard produced strong passwords, even when sequential patterns were deliberately included. Similarly, analysis of the PIN codes entered on the shuffled numpad revealed no standard numpad patterns or naturally ordered sequences, further strengthening the security of the generated PINs.

Throughout the study, a critical evaluation of existing methods, tools, and solutions drived key decisions and directed the design, development, and assessment of the experiment.

The study was conducted with strict adherence to academic integrity, making efficient use of the available time and resources. The work fully complied with ethical standards and legal requirements, ensuring data security and privacy while avoiding discrimination or bias in both the algorithm development and data collection processes. Social implications were also taken into account, with a focus on promoting accessibility for all users.

Research Limitations

While the research aim is considered achieved, several limitations must be acknowledged. First, the dataset collected during the limited experiment time includes data from 22 participants, which may limit the generalisability of the findings to a wider population. Second, the sampling technique primarily relied on snowball recruitment, where existing participants invited others from their social networks. Since early participants were drawn from individuals close to the author, this approach may introduce selection bias by potentially excluding individuals from more distant social classes and backgrounds.

Due to the strict time constraints of the experiment, the long-term memorability of the collected passwords and PIN codes, reflecting the practical applicability of these secret strings, may have been overlooked. Another limitation is the English-centric design of the study. Using only one language may narrow the insights, as different languages and writing systems can significantly impact password creation patterns and user behaviour.

Additionally, resource limitations restricted the integration of a more advanced web tracking system, which would have enabled the collection, storage, and analysis of detailed user activity data across the web application, potentially offering deeper insights into behaviour and data patterns.

Finally, ethical considerations prevented the direct use of numerous leaked password and PIN code databases, so the experiment relied on summarised findings from previous research. As a result, some keyboard-derived patterns that affect password strength may have been missed, making the study's findings less precise.

Future Directions

While this study offers valuable insights into the effectiveness of the shuffled keyboard in generating user-created passwords and PIN codes, several areas require further research. Future studies should include a larger and more diverse sample size to improve the generalisability of the findings across different populations. Additionally, incorporating language variation into the study design could help assess the universality of the shuffled keyboard approach and identify potential challenges related to different languages, particularly those using logographic (e.g., Japanese) or abjad (e.g., Arabic) writing systems.

Extending the study's duration would also allow for an exploration of the long-term memorability of passwords and PIN codes entered using the shuffled keyboard within a broader experimental framework. Finally, integrating a detailed action tracking system could provide deeper insights into user-keyboard interactions and ultimately improve the overall user experience.

References

Datagenetics.com (2012). PIN number analysis. [online] Available at: http://www.datagenetics.com/blog/september32012/.

Liu, D., Cuervo, E., Pistol, V., Scudellari, R. and Cox, L.P. (2013). ScreenPass. doi:https://doi.org/10.1145/2462456.2465425.

Lowe Wheeler, D. and Lowe, D. (2016). Open access to the Proceedings of the 25th USENIX Security Symposium is sponsored by USENIX zxcvbn: Low-Budget Password Strength Estimation zxcvbn: Low-Budget Password Strength Estimation. [online] Available at: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_wheeler.pdf.

Thanh, L. and Tanaka, H. (2024). A statistical Markov-based password strength meter. Internet of Things, 25, pp.101057–101057. doi:https://doi.org/10.1016/j.iot.2023.101057.