The Influence of Native Language on Password Composition and Security: A Socioculture Theoretical View

Pardon Maoneke, Stephen Flowerday, Naomi Isabirye

The Influence of Native Language on Password Composition and Security: A Socioculture Theoretical View

Pardon Blessings Maoneke, Stephen Flowerday and Naomi Isabirye

University of Fort Hare, Information Systems Department, East London, South Africa
blessings83@gmail.com,{sflowerday, nisabirye}@ufh.ac.za

Abstract. This study investigates the influence of native languages on password composition and security. The socioculture theory's psychological development principles were used to argue the influence of language on passwords. 107 Namibian and South African university students were asked to generate a new password for the study using a web based experiment. Levenshtein's edit distance, language experts and a password guessing algorithm were used for data analysis. Results showed that users generated passwords that were oriented towards both English and native languages. English is the first language of instruction while native languages are typically the first spoken languages of the participants. These passwords were based on names and words. A difference in character distribution confirmed the disparity in character preferences among researched groups. These findings suggest the influence of psychological development according to the socioculture theory. Password guessing shows that English oriented passwords are weaker than those oriented in native languages. The study shows that choices of password generation policy design should be informed by contextual factors if they are to be effective.

Keywords: passwords, password characteristics, socioculture theory, native language, security.

1 Introduction

The idea of using passwords for authentication purposes can be traced to ancient Roman times [1]. Today, passwords remain a dominant authentication mechanism, irrespective of research publications dating back to at least 1979 documenting various password security and usability limitations [2, 3, 4]. As research is progressing, focus is on passwords of Western computer users (mainly English speaking) and the recent insurgence of studies on Chinese passwords [3, 5, 6, 7]. Little is known about passwords generated by African computer users. This coincides with growing evidence suggesting passwords can differ according to contexts. For instance, the success of probability guessing algorithms shows a reliance on the use of related password dictionaries, something that points to the influence of a user's language. In addition, the effectiveness of targeted

attacks over trawling password guessing attacks further emphasizes the role of contextual factors in influencing password composition [8]. The language orientation used during password generation is one of the factors promoting password composition disparities across different contexts [3, 5]. Even though most African languages are Latin character-based unlike Chinese languages [5], the socioculture theory argues that learning and thinking is not only a result of biological factors but contextual factors too. Hence, according to the socioculture theory, African passwords are expected to portray unique traits that reflect contextual factors.

In terms of language, Africa portrays a unique context where English is the dominant language of instruction and first written language in literacy, while native languages are the spoken languages [9, 10]. It is against this background that this study adopts a socioculture theoretical view in its investigation of the influence of native African languages on password composition and strength. There are suggestions that the use of multiple languages including native languages, promotes different password composition orientations, which have the potential to enhance password strength [11]. From a business perspective, the African continent is experiencing growth in technology use such as social media, electronic mails, mobile phones, personal computers [12], internet banking, electronic commerce and adoption of cryptocurrencies – developments that emphasize the importance of studying authentication mechanisms within the African context. Understanding the influence of native languages on password composition and strength will help understand users' misconceptions about password generation strategies from which viable solutions can be proposed. For instance, given a multilingual environment, African system administrators have difficulties in deciding which password dictionaries to consider when implementing the recently suggested password policy best practice of using a blacklist [13].

This paper is organized as follows: the next section presents the theoretical foundation of this study. The section discusses characteristics of passwords guided by principles in the socioculture theory. This is followed by a presentation of the research methodology used in this study. A presentation of research findings and a discussion of these findings concludes the paper.

2 Theoretical Foundation

Information Systems is a multidisciplinary subject domain and where its theories cannot address certain problems, one can adapt theories from other research disciplines [14]. This study adapts the socioculture theory. Lev Semyonovich Vygotsky is credited for laying out the theoretical framework of the socioculture theory [15]. The socioculture theory argues that an individual's mental function is related to participations in contextual social interactions. The socioculture theory drew from the Marxist theory and proposed three principles that explain psychological development: the genetic law of development, mediation and genetic domains. These principles have been widely used to explain high mental activities that are argued to be socially constructed instead of being biologically constructed alone [15, 16]. Accordingly, this study assumes that

password generation and use are higher order mental activities involving voluntary attention, logical thinking and problem solving. The next section discusses principles in the socioculture theory, reflecting on their implications to password composition.

2.1 The Generic Law of Development

The generic law of development suggests that the settings of an individual as determined by culture, language, history, peer groups and institutional structures at school or workplace play a critical role in shaping the initial human mental development [16]. It is argued that "human psychological process does not pre-exist inside the head waiting to emerge at just the right maturational moment" [17, p. 14]. Neither is mental development considered an inborn capacity that would naturally unfold with time. Instead, human psychological development occurs across two levels: first at a social level as one is interacting with those in one's social environment and then at an individual level. This suggests that the social environment in which a computer user resides/grew up has an influence on the password a user is likely to generate. In particular reference to Africa, the present language landscape portrays a multilingual society where individuals speak and write at least two different languages, which are expected to affect password composition. For example, South Africa (SA), Nigeria, Namibia, Ghana and Ethiopia, just to name a few, have more than ten recognised indigenous languages [9, 10]. Other contextual factors found influencing the composition of passwords include website information and website functionality [18]. For instance, users use website information or website functionality as they adapt phrases such as "mail account", "rockyou", "news" or "amazon" in their passwords. Further to that, elements in the context of a user, such as individual names and those of geographical locations, are some of the strings that could be used when generating passwords [18]. The next section on mediation reflects on possible effects of these contextual factors on password composition.

2.2 Mediation

The socioculture theory suggests different cultural artefacts (symbolic tools), such as language, are used to mediate social interactions and regulate cognitive activities of thinking and problem solving. These cultural artefacts differ according to contextual factors depending on the social environment, as explained by the generic law of development. This study focuses on user-generated passwords with the aim of determining how social contextual factors influence password composition. Due to the paucity of a publicly available password corpus of African computer users, this section makes reference to research contexts that have publicly available password corpora. The said contexts are able to demonstrate the influence of the generic law of development as reflected by a preferential use of mediating symbolic tools. For example, an analysis of more than 100 million publicly leaked English and Chinese passwords shows that close to 50% of Chinese passwords are purely digit-based when compared to English passwords that are mainly a concatenation of English words and digits or words in the English dictionary (25.88%) [3, 5, 6, 7]. In addition, one in every ninth Chinese user inserts

a Pinyin name while one in four English users include their name when generating passwords. A closer analysis of these different password corpora shows that the respective passwords reflect the influence of native languages found across the analysed data sets [3, 5]. Affirming the use and influence of native language on password composition, Wang et al. [3] observed a difference in character distribution between English and Chinese passwords. Further to that, Chinese computer users are more likely to use keyboard patterns as passwords compared to English computer users [6]. An analysis of the Chinese social context shows that few websites support characters of Chinese languages, something that is compounded by a society that is not well versed in the English language [5, 7]. As such, the Chinese resort to keyboard patterns and the use of digits when generating passwords [5, 7].

In addition, other isolated studies conducted in different countries confirmed the influence of native language (mediating tools) on password composition and structure. For instance, [11] noted a small (2.5%) percentage of native Greek language-oriented passwords generated by Greek computer users. In another study, [5] noted passwords that were oriented towards native languages, namely, Hebrew and Spanish. Besides native language use, culture was found playing a critical role in influencing the composition of Chinese passwords. For instance, the numbers 6 and 8 are culturally believed to be lucky numbers in Chinese, hence these are regularly used [7]. Four, on the other hand, is an unlucky number and less frequently used [7]. Furthermore, the use of digits also portrays the pronunciation of certain specific phrases in Mandarin Chinese. For example, 5201314, a common password among Chinese users, translates to "I love you forever" [3, 6, 7]. All these findings point to the influence of contextual factors in shaping password composition. Consequently, mediating tools (native and non-native languages) that shape psychological development in Africa are expected to influence the composition of user-generated passwords.

2.3 Generic Domains

The socioculture theory motivates the notion that higher order mental functionality is always in motion and goes through continuous changes [19]. A generation inherits cultural artefacts from previous generations and acts on them; these modified artefacts are then passed on to the next generation. Such evolutions can be initiated by changes that occur in a society thereby enabling "changes in human consciousness and behaviour" [19, p. 119]. For instance, a longitudinal study by [20] found that, user passwords evolved over time due to changes in password security requirements. Such evolutions involved minor changes to existing passwords as users adapted old passwords in an attempt to comply with password requirements, without compromising memorability. In addition, [21] observed that users can evolve their passwords by making spelling mistakes, insertions, concatenating different character classes and replacing different character classes, for example, LEET could be written as L33T [21]. Concatenation is the dominant password creation strategy that is mainly characterised by the LSD or LDS password structure where L represents alphabetic letters, S represents symbols and D is for digits.

3 Methodology

This study is aligned to the design science research methodology as it focuses on generating new knowledge by building (designing) and evaluating artefacts [22]. For evaluation, this study uses an experiment to gather data [22]. University students based in SA and Namibia participated in the experiment for this study. The literature showed that experiments and existing leaked password corpora are the commonly used data sources of passwords [3, 6, 7, 13]. There were also isolated reports on using interviews and questionnaires or a combination of both as password gathering techniques [20]. However, one of the challenges associated with using leaked passwords is that details of password rules used in password generation often remain unknown. The influence of password meters and password policies is well documented in the literature and failure to articulate such details when reporting characteristics of leaked passwords makes contextualising research findings complex [20, 23]. Further than that, some of the existing passwords may have been generated by password managers [3, 6]. Besides, findings from leaked passwords are biased towards successfully guessed passwords with characteristics of those unguessed passwords remaining unknown behind encryption and salting algorithms.

Conversely, [7] argues against the use of experiments, interviews and questionnaires as techniques for gathering user passwords and instead used existing leaked passwords. Yang et al. [7] is of the view that participants may not always reflect real-life password experiences; samples are often small, or the target group comprises students/company employees who could compromise the generalisability of findings. However, it is important to realise that experiments can be designed in such a way that participants can simulate password generation and treat the process in the same manner they would when generating real passwords [13]. von Zezschwitz et al. [20] justify the proxy of university students as they have found that, on average, computer users generate their first password at the age of 15 and these passwords often remain unchanged or experience minimal changes as users adapt their first passwords for different accounts.

3.1 The Experimental Design and Administration

This study adapted and modified an experimental framework used by [13] and [24], a leading research group on password policies and guessing algorithms. Their experimental framework has been used widely to underpin research since 2011. This experimental framework gives user password generation conditions and keeps data for each user organised. The experiment of this study was based on a web application built specifically for the purpose of this experiment. Users (students) of the web application were asked to generate a password following specified password rules. Upon opening the password generation platform, participants were presented with a scenario encouraging the generation of a realistic password as purported by [13] and [24]. This study adapted an existing scenario from [24] that was modified as follows:

"Imagine that your main email service provider has been attacked and your account has been compromised. You need to create a new password for your email account, since your old password may be known to the attackers.

Because of the attack, your email service provider is also changing the provider's password rules. You are to generate a new password following new conditions."

Users were required to generate passwords following the comprehensive eight character (Comp8) password policy. The Comp8 password policy is a popular policy that was designed following a guideline by the National Institute of Standards and Technology (NIST) [13]. Participants were required to generate a password that is at least 8 characters long, containing at least one: upper-case letter, lowercase letter, digit and special character. Furthermore, participants were asked not to use their name or personal details in their passwords, though no control was put in place to avoid participants from using personal information. After generating passwords, participants were asked to complete an online survey. The online survey gathered data on demographics and attributes for evaluating principles in the socioculture theory.

3.2 Data Analysis

Socioculture Theory Principles. This study used mediating symbolic tools to evaluate the generic law of development. It is argued that contextual factors influence psychological development as suggested by the socioculture theory. Hence, computer users are expected to reflect contextual factors by orienting user-generated passwords towards languages and following cultural practices that are common within their contexts. Language orientation in user-generated passwords was used to establish the influence of contextual factors. According to [16], "language in all its forms is the most pervasive and powerful cultural artefact that humans possess to mediate their connection to the world, to each other, and to themselves" (p.5). Content analysis was used to identify the use of English and native languages in user-generated passwords. English is the official language in Namibia and SA. Levenshtein's edit distance was used to measure the distance between passwords and dictionary words [8, 25]. The edit distance shows the number of characters that need to be changed in order to convert a password to the closest dictionary word. Two language experts were engaged to identify passwords oriented towards native languages. The engaged experts consisted of a Namibian and a South African national. In addition, a frequency distribution of characters was used to establish the influence of contextual factors. Differences in character distribution between password corpora could be used as a basis to justify the differences between social contexts [3, 6].

Measuring Password Strength. This study considers password strength or security as a factor of the number of guessing attempts needed to guess a particular password by any given password guessing algorithm. Accordingly, considerations of password threats for this study are limited to online and offline threats where the perpetrator has an opportunity to make several password guessing attempts.

This study used Dropbox's zxcvbn; an open source password guessing algorithm. The algorithm was introduced in 2012 and has seen various modifications to enhance guessing performance [4]. Unlike Probabilistic Context-Free Grammar (PCFG) and Markov chain that use probability, zxcvbn uses heuristics to guess passwords. Hence, zxcvbn is a low cost password guessing algorithm that can work with a small password

sample and does not require a powerful computer, as is the case with resource intensive algorithms such as the PCFG and Markov chain. Furthermore, zxcvbn shows to be a better password guessing algorithm than the currently commercialised measures and algorithms for guiding users to generate secure passwords [26]. When compared to leading password guessing algorithms such as the PCFG, zxcvbn is comparable to PCFG until 10^5 [4]. Wheeler [4] gave a detailed overview of the version of zxcvbn considered in this study. It should be noted this study retained password dictionaries for zxcvbn that were used by [4] and [26] to test the effect of language on password strength.

4 Findings and Results

This section presents findings and results from data collection and analysis.

4.1 Demographics

A total of 107 participants took part in the password generation experiment for this study. Demographic data on gender and age group was gathered. A total of 44% of the participants were female with 56% male students. Notably, 88% of the participants were 18 to 25 years old, and the remaining 12% were more than 25 years of age. The age groups of university students are consistent with those found in the literature [23]. Moreover, 64% of the participants were Namibians with 28% representing South Africans. The remaining 8% represented other African countries.

4.2 Social Context Overview

Data was gathered to establish characteristics of the social context. This data was used to evaluate attributes of the generic law of development as purported in the socioculture theory. To evaluate the generic law of development, this study used data on user computer skills, first language, second language and ethnic group. In terms of computer use, the majority of participants indicated that they had had exposure to computers and had the know-how to use computers. The majority (98%) of the participants indicated that they had at least basic computer skills. Only 17% indicated that they were experts at using computers, while 47% indicated that they were above average.

In addition, data gathered on first and second language showed that the most common first language was Oshiwambo (36%) from the Vambo tribe of Namibia, followed by isiXhosa (24%) from the Xhosa tribe of South Africa. The Vambos are the dominant tribe in Namibia while the amaXhosa are a dominant tribe of a targeted province of SA. There were fourteen other language varieties from different Namibian ethnic groups representing 1% to 5% of the participants. At least twelve ethnic groups were observed among Namibian participants. In particular to the targeted South African province, five diverse ethnic groups using different native languages were observed. Native languages from participants who came from countries other than Namibia and SA represented 7%. However, when all the participants were combined, 92% of the participants indicated

that English was their second language. These findings suggest that participants in this study grew up speaking different native languages within their ethnic groups and went on to use English as a medium of instruction at learning institutions [9, 10]. This study posits that these unique social contexts played a critical role in participants' psychological development at both social and individual level. The next sections investigate how these contextual factors influence password composition.

4.3 Mediating Symbolic Tools and Password Composition

English-oriented Passwords. A review of user-generated passwords showed that English (47%) words or names were most commonly used to generate passwords. This could be explained by the fact that English is the first language of instruction and remains a dominant language of technologies used within the context of this study [9]. The edit distance for English-oriented passwords ranged from two to nine characters. The majority (26%) of passwords had an edit distance of three. Passwords with an edit distance of at least three characters are difficult to guess using a dictionary attack especially if a perpetrator does not have any prior knowledge of the password [25]. Nevertheless, a closer inspection of passwords oriented towards the English language showed that computer users are more likely to use an English word (57%) or English first name (43%) to generate a password. The majority (45%) of participants concatenated a name/word, number(s) and a symbol. Other participants (42%) combined a name/word, symbol and put numbers at the end when generating passwords. Another observation was the presence of passwords based on common English words such as P@55w0rd777, Ilove!995 and the use of a commonly used profane English word. Other common English words used when generating passwords included Smooth, Favour, Internet and Help. Arguably, these passwords reflect what [2] referred to as global passwords.

Native Language-oriented Passwords. Content analysis showed that, of all the passwords gathered, 30% were oriented towards native languages; 9% were oriented towards multilingualism; 11% were considered random passwords, while 2% were based on keyboard patterns. An analysis of native language-oriented passwords showed that 76% of these were based on the name of a person. Most of these were Oshiwambo and isiXhosa names. Twelve percent (12%) of the passwords oriented towards native language were names of towns and districts in participants' contexts. The majority (38%) of passwords had an edit distance of three characters. Native language-oriented passwords had an edit distance ranging from two to sixteen characters. Users often concatenated a name with numbers and a symbol. The content analysis showed that the majority of multilingual passwords had traces of English and native languages.

Frequency Distribution of Characters. To establish the magnitude of influence by native languages on password composition, the distribution of characters in passwords of the researched contextual environments was extracted. Results showed that Namibian participants preferred characters "anoetumisrhlbdkcpygfwxjvqz" in descending order. South Africans' passwords assumed the "aneosmlituhyrbgpdwzvkqf" character

distribution in descending order. For both samples, “a”, “n”, “o”, “e” were popular characters among South African and Namibian passwords. However, there is a difference in the overall distribution of character use. The study posits that this finding points to differences in the social contextual environments that informed preferred mediating artefacts.

Passwords generated by South Africans and Namibians were combined to establish a joint password distribution in descending order: “anoetmiushlrbygdpkcfwvzxjq”. Given that both SA and Namibia use English as their official language and as the first language of instruction in schools, it is interesting to establish how South African and Namibian passwords’ character distribution compares to that of English users. This study uses a password distribution for English users that was generated from more than 33 million leaked English passwords [3]. An analysis of these English passwords by [3] established a character sequence “aeionrlstmcdyhubkgpjvfwzxq” in descending order. It is not clear to what extent password rules used in this study and that of existing passwords from English users influenced the preference of characters. When compared to the distribution of combined South African and Namibian passwords, it can be noted that characters “a”, “o” and “n” are the most popular across the samples. However, as observed in the literature, there is a degree of difference in the order of preferred characters, which is attributed to a difference in languages used when orientating user generated passwords [3, 6]. These findings suggested that contextual factors did have an influence on password composition due to differences inspired by psychological development as suggested in the socioculture theory.

4.4 Password Generation Strategy

Participants were asked to indicate the strategy used to generate their passwords. The five most commonly used password creation strategies include adapting a name, adapting an existing password, using words in local language, using non-standard spellings and using a non-English language as shown in Figure 1.

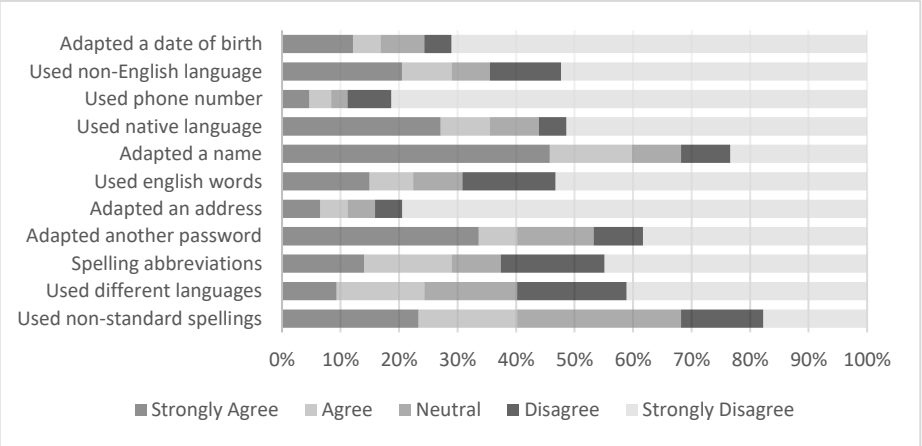

Fig. 1. Password creation strategy.

These findings were supported by findings from content analysis. Based on the research findings, it can be argued that the practice of adapting existing passwords promotes password evolution as suggested in the generic domain. In addition, it was observed that the selection of numbers in passwords was linked to a year or the age of participants. For instance, it was noted that passwords often had numbers within the range of 18 to 25 which might reflect the age of a participant at the time of generating the password. Furthermore, the majority of passwords had a number like 95 or 1995 which could be traced to the year of birth given the average age group of participants reported in section 4.1. In addition, other participants included digits such as 2017 – a number that reflected the current year at the time of password generation. These practices were also reported as common in the literature [3, 6, 7].

4.5 Password Strength

This section reports on password strength as ascertained by the zxcvbn password guessing algorithm. Figure 2 summarises password strength according to five categories, namely very weak, weak, normal, strong and very strong, as proposed in the zxcvbn password guessing algorithm.

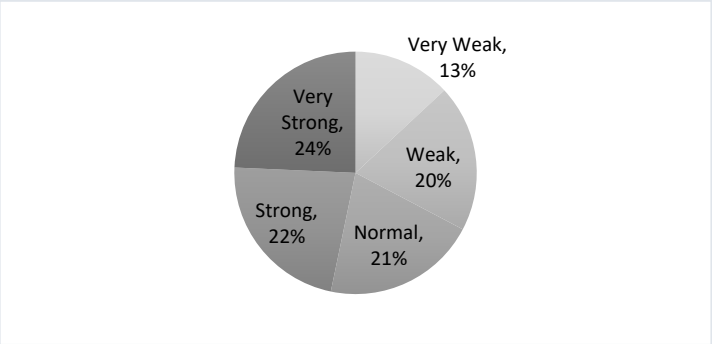

Fig. 2. Password strength according to zxcvbn.

Data analysis showed that more than 40% of the passwords were considered strong to very strong, according to password guessing results from zxcvbn. Results from zxcvbn showed that it would take at least three months to centuries to guess passwords classed as strong to very strong. This suggests an attacker would need many attempts to guess passwords within this category. Assuming a password attacker adopts an optimal approach to password guessing, passwords classified as very weak to normal are likely to be targeted first [13]. Hence, 46% of user-generated passwords in this study are considered secure according to findings from zxcvbn. However, a closer look at the passwords showed that language orientation during password generation had had an effect on password strength. Passwords oriented in native languages were stronger than English passwords. Figure 3 shows the difference in password strength according to language orientation.

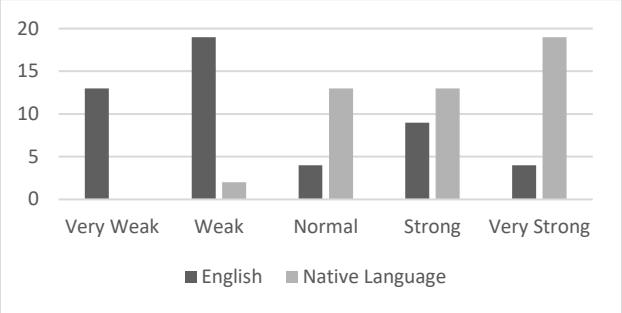

Fig. 3. The effect of language orientation on password strength.

A subsequent significance test at 0.05 confirmed that there is a significant (0.00) difference in password strength according to language orientation. Bonneau [2] observed a loss in efficiency when using a password dictionary that is not related to the language orientation of passwords under test. This could explain our finding given that the password dictionary used is oriented towards English passwords. Nonetheless, this finding confirms that language specifics do have a significant effect on increasing the password search space which positively contributes to password security [2, 11, 18]. Thus, it can be concluded that a trawling password attack may find native language-oriented passwords difficult to guess. However, findings from this study have to be considered with caution given that users generated passwords using personal information that included names and year of birth as reported in section 4.3 and 4.4. The literature shows that personal information can be exploited to greater effect in a targeted password guessing attack [8]. In addition to language orientation, a significant test shows that password length had a significant effect (0.00) on password strength. There is a growing research interest in long passwords (passphrases) with the objectives of improving security and usability [13].

5 Recommendations and Conclusion

While passwords found in this study assumed structures that were reported in the literature, namely the LDS or LSD, a closer look at the data showed that a combined character distribution of researched South African and Namibian passwords followed a unique trend compared to that of English passwords. Native languages are considered a major force behind the uniqueness in character distribution. This is an interesting finding given that English is the first written language and a language of instruction in most African countries. Nonetheless, passwords oriented towards the English language were observed in the password corpus. Some of the observed English passwords were based on common English words. Similarly, passwords with an orientation towards native languages were observed in the corpus. The use of different language orientations in password generation reflected common languages within the research context.

These findings affirmed the explanation of the psychological development as stated in the socioculture theory.

An evaluation to establish the influence of language orientation on password strength showed that passwords based on native languages are significantly stronger than English passwords. No password with a native language orientation was found to be weak or very weak. However, it has to be highlighted that the dominant use of personal information when generating passwords is a huge security concern.

Based on these findings, it is argued that a blacklist with common English oriented passwords can be a useful inclusion in password policies for the targeted multilingual user groups. Findings from this study suggest that such a blacklist has the potential of improving password security on approximately 50% of the occasions. However, a blacklist with English-oriented passwords alone may not be a complete solution when targeting multilingual user groups. For instance, multilingual users can switch between common words in different languages upon stumbling into blocked passwords that are oriented in a particular language. In support of our opinion, [27] concluded "that trivial password choices can vary between contexts, making a simple blacklist approach ineffective" (p. 5). A blacklist with common native names and words could be a useful addition for enhancing password security within the context of this study. However, while a blacklist can enhance security especially in the case of online password attacks, it is vulnerable to offline password attacks and makes password generation complex [13, 28]. It is therefore worthwhile to investigate the usability of blacklists within this study's research context prior to implementation.

In addition, password authentication designers within our study context should consider devising mechanisms that prevent the use of personal information in user generated passwords. Approximately one in three participants based their passwords on names or names of loved ones. Notably, some website platforms are already implementing password generation frameworks that prohibit the use of personal information in passwords [26]. In addition, this study confirms that using different language orientations in password generation, within a context, has a potential to increase the password search space which could improve password security. Hence, understanding principles of psychological development according to the socioculture theory could go a long way in guiding users to generate secure and usable passwords. However, there is a need for further research on using native languages in password generation.

Limitations: The study was based on a relatively small sample of 107 when compared to samples reported in the literature. Thus, increasing the sample size could improve the generalisability of findings.

References

1. Adeka, M., Shepherd, S., Abd-Alhameed, R.: Resolving the Password Security Purgatory in the Contexts of Technology, Security and Human Factors. IEEE International Conference on Computer Applications Technology, pp. 1--7, IEEE, Sousse, Tunisia (2013).
2. Bonneau, J.: The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. IEEE Symposium on Security and Privacy, vol. 2012, pp. 538-552 (2012).

3. Wang, D., Cheng, H., Gu, Q., Wang, P.: Understanding Passwords of Chinese Users: Characteristics, Security and Implications. IEEE, pp. 1--14 (2015).
4. Wheeler, D. L.: zxcvbn: Low-Budget Password Strength Estimation. In: Proceedings of the 25th USENIX Security Symposium, pp. 157—173, USENIX Association, Austin, Texas, USA (2016).
5. Bonneau, J., Xu, R.: Of Contrase˜nas, תואמסיס!, and 密密密码码码 Character Encoding Issues for wWeb Passwords, pp. 1-8, Citeseer (2012).
6. Li, Z., Han, W., Xu, W.: A Large-Scale Empirical Analysis of Chinese Web Passwords. In: proceedings of the 23rd USENIX Security Symposium, pp. 559—574, USENIX Association, San Diego, USA (2014).
7. Yang, C., Hung, J.l., Lin, Z.: An Analysis View on Password Patterns of Chinese Internet Users. Nankai Business Review International, vol. 4(1), pp. 66-77 (2013).
8. Wang, D., Zhang, Z., Wang, P., Yan, J., Huang, X.: Targeted Online Password Guessing: An Underestimated Threat. In: proceedings of the 23rd ACM Conference on Computer and Communications Security, pp. 1242—1254, ACM, Vienna, Austria. (2016).
9. Deumert, A., Lexander, K. V.: Texting Africa: Writing as Performance. Journal of Sociolinguistics, vol. 17(4), pp. 522-546 (2013).
10. Lexander, K. V.: Texting and African Language Literacy. New Media & Society, vol. 13(3), pp. 427-443 (2011).
11. Voyiatzis, A. G., Fidas, C. A., Serpanos, D. N., Avouris, N. M.: An Empirical Study on the Web Password Strength in Greece. In: Proceedings of the 15th Panhellenic Conference on Informatics, pp. 212—216, IEEE Computer Society, Kastoria, Greece (2011).
12. Stork, C., Calandro, E., Gillwald, A.: Internet Going Mobile: Internet Access and Use in 11 African countries. Info, vol. 15(5), pp. 34-51 (2013).
13. Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., Ur, B., Bauer, L., Christin, N., Cranor, L. F.: Designing Password Policies for Strength and Usability. Transactions on Information and System Security, vol. 4(13), pp. 13:1-13:34 (2016).
14. Shin, D.: A Socio-technical Framework for Internet-of-Things Design: A Human-centered Design for the Internet of Things. Telematics and Informatics, vol. 31, pp. 519-531 (2014).
15. Mercer, N., Howe, C.: Explaining the Dialogic Processes of Teaching and Learning: The Value and Potential of Sociocultural Theory. Learning, Culture and Social Interaction, vo. 1, pp. 12--21 (2012).
16. Lantolf, J. P., Thorne, S. L., Poehner, M. E.: Social Theory and Second Language Development. In B. van Patten, & J. Williams, Theories in Second Language Acquisition, pp. 207--226, New York: Routledge (2015).
17. Lantolf, J. P.: Introducing Sociocultural Theory. Sociocultural Theory and Second Language Learning, pp. 1-26, Oxford Press (2000).
18. Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., Cranor, L. F.: "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In: Symposium on Usable Privacy and Security (SOUPS), pp. 123-140, USENIX Association, Ottawa, Canada (2015).
19. Marginson, S., Dang, T. K.: Vygotsky's Sociocultural Theory in The Context of Globalization. Asia Pacific Journal of Education, vol. 37(1), pp. 116--129 (2017).
20. von Zezschwitz, E., De Luca, A., Hussmann, H.: Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. In: Proceedings of the International Federation for Information Conference on Human-Computer Interaction, pp. 460—467, IFIP, Berlin, Heidelberg (2013).
21. Jakobsson, M., Dhiman, M.: The Benefits of Understanding Passwords. Mobile Authentication, vol. 2013, pp. 5-24 (2013).

22. Baskerville, R. L., Kaul, M., Storey, V. C.: Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production. Mis Quarterly, vol. 39(3), pp. 541--564 (2015).
23. Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Cranor, L. F.: Encountering Stronger Password Requirements: User Attitudes and Behavior. In: Proceedings of a Symposium on Usable Privacy and Security (SOUPS), pp. 1-20, ACM, Redmond, USA (2010).
24. Komanduri, S.: Modeling the Adversary to Evaluate Password Strength With Limited Samples, pp. 1—270, Carnegie Mellon University, Pittsburgh USA (2016).
25. Campbell, J., Ma, W., Kleeman, D.: Impact of Restrictive Composition Policy on User Password Choices. Behaviour & Information Technology, vol. 30(3), pp. 379-388 (2011).
26. de Carnavalet, X., Mannan, M.: From Very Weak to Very Strong: Analyzing Password-Strength Meters. NDSS, vol 14, pp. 23-26 (2014).
27. Blocki, J., Komanduri, S., Procaccia, A. D., Sheffet, O.: Optimizing Password Composition Policies. In: proceedings of the 14th ACM conference on Electronic commerce, pp. 1-27, ACM, Philadelphia, USA (2013).
28. Florêncio, D., Herley, C., van Oorschot, P. C.: An Administrator's Guide to Internet Password Research. In: Proceedings of the 28th Large Installation System Administration Conference, pp. 35-52, USENIX Association, Seattle, USA (2014).