A model for usable and secure passphrases by multilingual user groups

Pardon Blessings Maoneke
Dept. of Information Systems
University of Fort Hare, South Africa
blessings83@gmail.com

Stephen Flowerday
Dept. of Information Systems
University of Fort Hare, South Africa
sflowerday@ufh.ac.za

Naomi Isabirye
Dept. of Information Systems
University of Fort Hare, South Africa
nisabirye@ufh.ac.za

Abstract

Dominant research on passphrase usability and security is focused on passphrases generated using English as the language in use. This is so despite the fact that a password's structure and its character distribution can vary from one language to another. In light of this, we recommend an alternative approach for generating passphrases that meet usability and security requirements. This paper motivates increasing the size of the search space for passphrases by encouraging the generation and use of passphrases based on multiple languages. The paper proposes to extend the practice of code switching by multilingual user groups to the generation of passphrases. It is argued that such an approach can help reduce the chances of users generating passphrases that are limited to a few popular words in a language. In addition, our approach to passphrase generation is expected to help mitigate passphrase security limitations as a result of the underlying grammatical structures in a particular language. Accordingly, this paper makes use of a literature review to motivate its argument for generating and using passphrases based on multilingual phrases instead of monolingual phrases. The paper goes on to propose a model for passphrase usability and security that is suitable for multilingual user groups. It should be noted that this paper is part of an ongoing design science study. The paper explains the abduction process followed during the designing of a proposed model. Such a model can be used by systems administrators to inform the design of passphrases policies in multilingual environments.

Keywords: usability, security, passphrases, authentication

1.0 Introduction

There is a growing interest in research aimed at improving the usability and security of text-based authentication mechanisms with passwords being a particular focus (Wang, Cheng, Gu,& Wang, 2015; Choong, Theofanos, & Liu, 2014; Kelley, Komanduri, Mazurek, Shay, Bauer, Christin, Cranor & L´opez, 2012; Shay, Komanduri, Durity, Huh, Mazurek, Segreti, Ur, Bauer, Christin & Cranor, 2016). This is motivated by the popularity of passwords as a form of authentication despite their inherent shortcomings. Multiple word phrases (passphrases) are considered one of the alternative solutions for enhancing the security and usability of passwords (Andersson & Saedén, 2013; Keith, Shao, & Steinbart, 2009). Security and usability are seen as the building blocks of a complete text-based authentication mechanism (Andersson & Saedén, 2013; Rao, Jha, & Kini, 2013). Despite the fact that security and usability togetherare critical for a complete passphrase, some authors focus on investigating security factors alone

(Rao et al., 2013; Bonneau & Shutova, 2012; Veras, Collins, & Thorpe, 2014) while others focus on investigating passphrase usability (Keith, Shao, & Steinbart, 2007) in isolation of security factors. Nevertheless, there are other researchers who have investigated both security and usability (Kelley et al., 2012; Shay et al., 2016). However, it is quite intriguing to note that rarely do the findings on passphrase security and usability from these specialised studies complement each other. Instead, they present mixed views that portray inconclusive findings on the security and usability contributions of passphrases. For instance, Kelley et al. (2012) and Shay et al. (2016) motivated the idea that passphrases are secure and usable when compared to short passwords. Conversely, Rao et al. (2013), Bonneau and Shutova (2012) and Veras et al. (2014) question the security contributions of passphrases. They argue that users often create passphrases following linguistic patterns that can be exploited and compromise a passphrase's strength.

In short, studies that investigated passphrase security focusing on structural dependencies at character level found passphrases to be secure (Kelley et al., 2012; Shay et al., 2014; Shay et al., 2016), while studies that researched passphrases security based on linguistic properties such as grammatical structures, popular words in natural language and keyboard patterns found passphrases prone to guessing (Rao et al., 2013; Bonneau & Shutova, 2012; Veras et al., 2014). This is due to the fact that attackers can simply reduce the passphrase search space by exploiting inherent semantic patterns that users follow when generating passphrases. Further to that, the current crop of studies on passphrases is limited to a culture where English is the dominant language. This is so despite research findings by Wanget al. (2015) that suggest the structure of user-generated passphrases are influenced "by native languages (and culture background)". Arguably, this finding puts more emphasis on the importance of culture, with a particular focus on language when investigating passphrase usability and security. Given that user-generated passphrases confined to a particular language are likely to be weak and easy to guess (Rao et al., 2013; Bonneau & Shutova, 2012; Veras et al., 2014), this paper explores the use of multiple languages (multilingual phrases) when creating a user-generated passphrase. This is done with the idea of increasing the size of the passphrase's search space (Rao et al., 2013) without compromising the security or usability of passphrases. As such, the paper uses a literature review and proposes a model for passphrase security and usability that is suitable for multilingual user groups. The paper reflects on the research progress of culture, passphrases usability and security to propose a tentative model. In particular, the paper reports on findings from an abductive use of kernel theory or justification knowledge in the literature. These activities align to the design and development phase as explained by Peffers, Tuunanen, Rothenberger, and Chatterjee (2008).We are of the view that the current state of research findings on passphrase security and usability, coupled with conflicting findings, presents a research opportunity to explore alternative approaches for addressing the security and usability dilemma. The current state of findings also promotes further research on usability and security with the hope of producing consistent findings that can guide system administrators into designing policies for user-generated passphrases.

The paper is organised as follows: The next section discusses the paper's theoretical foundation by reviewing cultural models and their impact on language. We are of the view that looking into culture, language in particular, gives an opportunity to explore a different angle for increasing the size of passphrase search space. In light of culture findings, the paper goes on to discuss considerations of security and usability of passphrases from which a model is proposed.

1.1 Theoretical foundation

1.1.1 Culture

Hofstede's model on culture. A model proposed by Hofstede (2013) defines culture as a "collective programming of the mind that distinguishes the members of one group or category of people from others" (p.3). This suggests that culture can be differentiated at national level and is deeply rooted in such a way that it is resistant to outside influence. Culture is an umbrella term for various cultural attributes that include race, ethnicity, religion, class, gender, values, traditions, language, lifestyles and nationality (Beeler & Saint-Leger, 2014). This study focuses on language given its influence on text-based authentications (Li, Han, & Xu, 2014; Wang et al. 2015; Kang, 2015). Bonneau and Shutova (2012)

support our view by recommending continued consolidated research on security and linguistics. In addition, language (mother tongue) is also considered one of the main factors influencing information systems security awareness (Kruger, Flowerday, Drevin, & Steyn, 2011). Nevertheless, if culture is to be viewed according to Hofstede (2013) where language is considered rigid, passphrases generated under this cultural view are expected to be composed of character and substring distribution that conforms to a particular culture. Research findings by Wang et al. (2015) and Li et al. (2014) corroborate Hofstede's propositions by establishing that user-generated passwords from a single language group exhibits consistency in terms of character distribution. However, there is a significant difference in character distribution of passwords generated using different language groups (Wang et al., 2015). Further, Bonneau and Shutova (2012) found that the choice of user-generated passphrases is a factor of popular phrases in a particular language. Based on these findings, this paper concedes that linguistic patterns in a language can reduce the search space of user-generated passphrases, a weakness that can be exploited to compromise the security of passphrases (Wang et al., 2015). These arguments lead us to the following proposition:

Proposition P1: Generating passphrases based on monolingual phrases can reduce the search space of passphrases.

The multiple cultures perspective. In addition to Hofstede's view on culture that led to proposition P1, culture can also be viewed from a different perspective. For instance, the multiple cultures perspective motivates the notion that culture is not rigid. The multiple cultures perspective argues that individuals can identify with values of several overlapping "cultures", any of which may become salient within a given context (Beeler & Saint-Leger, 2014). This implies that an individual living in a multiple language environment has a chance of learning and understanding some of the languages they are exposed to within a context. Education and migration are some of the factors that result in the overlapping of multiple languages. When viewed from a bigger scale, the principles of the multiple cultures perspective would result in a globe with islands of isolated and unique multiple lingual individuals. Arguably, the practise of code switching is ample evidence that reflects the multiple cultures perspective within a given environment. Code switching involves alterations to phrases based on the use of spelling abbreviations; juxtaposition of words from different languages; phonological approximations; non-standard spellings; paralinguistic restitutions (ideographic); style shifting; neologisms, and semantic shift and pseudo-borrowings (Deumert & Masinyana, 2008; Carrier & Benitez, 2010; Morel, Bucher, Doehler, & Siebenhaar, 2012). Different studies provided empirical evidence of the practice of code switching in short message texting that result in unique phrases without compromising usability (Deumert & Masinyana, 2008; Carrier & Benitez, 2010; Morel et al., 2012). It is argued that extending certain usable practices of code switching to user-generated passphrases holds the potential of helping users generate secure passphrases through enlarging the search space. For example, it is assumed that individuals who are comfortable in Chinese and English languages can be influenced by the use of relevant password policies in such a way that they generate passphrases that are based on words or substrings from these two languages. Hence, the arguments for the use of multilingual passphrases in this paper are grounded on the multiple cultures perspective. It is therefore proposed that:

Proposition P2: The use of multilingual phrases in a user-generated passphrase can increase the passphrase search space.

1.1.2 Passphrase security

This study is focused on offline security attacks. Cases of frequent database attacks that expose millions of hashed passwords from popular sites like CSDN, Tianya, Duduniu, 7k7k, 178.com, RockYou and Yahoo (Li et al., 2014) have increased the need for further studies aimed at mitigating the impact of offline attacks. Passwords are not stored as plain text in a service provider's database but in a hashed file. Every password in the hashed password file will have its own hash pattern generated by a hashing function. Upon gaining access to the hashed password file, security perpetrators often generate guessed passwords together with their respective hash patterns. Hash patterns of guessed passwords are compared to those in the hashed password file to see if there is a match. A match of hash patterns suggests that a corresponding password has been successfully cracked. Service providers can use slow hash schemes to reduce the likelihood of

password guessing. It is also common that service providers can use poor hash schemes leaving users' passwords prone to offline attacks (Shay et al., 2016). Nevertheless, generating strong passphrases can help reduce the chances of password cracking (Melicher, Kurilova, Segreti, Kalvani, Shay, Ur, Bauer, Christin, Cranor & Mazurek, 2016; Shay et al., 2016).

The literature suggests two most common measures for estimating passphrase security (Rao et al., 2013; Shay et al., 2016; Wanget al., 2015). These measures can be classed into those based on passphrase distribution or information entropy and passphrase prediction. Entropy is a measure of a passphrase's randomness based on the passphrase's sequence of characters. A passphrase with random characters is considered to have high entropy and is deemed secure (Keith et al., 2009). It is believed that computing entropy can give one an estimated figure of the least number of attempts needed to crack a passphrase (Shay et al., 2016). A move by the United States of America's National Institute of Standards and Technology (NIST) to use Shannon entropy in designing a guideline that should be followed when establishing policies for strong passwords suggests the importance of entropy (Wang et al., 2015; Houshmand & Aggarwal, 2012). On the other hand, passphrase prediction measures the number of guesses needed by a passphrase cracking algorithm to guess a particular passphrase. Shay et al. (2016) refer to this approach as the "guessability". It is important to realise the success of guessing a passphrase depends on the effectiveness of the chosen passphrase cracking algorithm. Hence, guessability varies with algorithms used. This paper assumes the guessability method for estimating passphrases' strength and resistance to offline guessing attacks. There is a general consensus in the literature that guessability is a better measure of passphrase strength when compared to Shannon entropy (Rao et al., 2013; Shay et al., 2016; Wanget al., 2015). Shay et al. (2016) give further evidence that shows entropy may not always be an accurate predictor of passphrase strength. Within the context of this study, guessability is considered a function of the size of passphrases' search space and the distribution of passphrase values (Rao et al., 2013). Search space is defined as the set of all possible unique values or words that could be used when generating passphrases (Rao et al., 2013). The previous section demonstrated this paper's approach towards increasing the search space for passphrases based on the use of multilingualism.

1.1.2.1 Factors for passphrase strength

Passphrases generated within a search space should possess certain attributes that can enhance its strength and resistance to passphrase guessing. A research study by Shay et al. (2016) that based its evaluation of passphrase strength on character distribution suggests structural patterns (substrings and character distribution) as determinants of passphrase strength. Based on their research findings, Shay et al. (2016) recommend that organisations should abandon short passwords and use passphrases for authentication purposes. They further found that, while passphrases are secure, it is important to put in place measures for curbing users from generating predictable passphrases (Shay et al., 2016). They recommend the use of a blacklist substring and strict pattern requirements (Shay et al., 2016). However, these measures have usability costs during passphrase creation and recalling. Blacklisting common substrings makes generating passphrases harder (Shay et al., 2016). It should be noted that their use of strict pattern requirements to control character distribution on user-generated passphrases saw an enhancement of passphrase security even though this resulted in making passphrases difficult to create and recall. Rao et al. (2013) argue that the security limitations of passphrases can be traced to the use of a few selected grammatical rules in a language that users follow when generating passphrases. Their argument points to the fact that a passphrase made of random words may not resist guessing attacks as long as such a passphrase is generated following common grammatical rules. This implies that a corpus has to portray a uniform distribution in the use of different grammatical rules by users during passphrase generation. Rao et al. (2013) also recommend the use of random words when generating passphrases. In addition, a study by Bonneau and Shutova (2012) noted that passphrases have the potential to enhance the security of passwords against guessing attacks. However, it was observed that passphrases are prone to guessing attacks if words for coming up with passphrases are not randomly chosen. These remarks were made following revelations that the majority of user-generated passphrases are composed of words that are skewed towards popular words in a natural language (Bonneau & Shutova, 2012).

Considering our proposed approach of using multilingualism in generating passphrases, we argue that findings from studies by Shay et al. (2016), Rao et al. (2013) and Bonneau and Shutova (2012) can be explained by the fact that respective passphrases are generated using a single language. As stated earlier, character distribution of words from different languages are not always the same. Accordingly, the next section outlays constructs for ascertaining passphrase security that are deemed suitable for our proposition. Using code switching in generating passphrases allows users to take advantage of languages that often have different character distribution. Hence, juxtaposing substrings, passphrase length and dictionary checks are considered important constructs for ascertaining passphrases security.

Juxtaposing substrings. Juxtaposing substrings from different languages as reflected in code switching has the potential to increase the search space and make the resultant passphrase random and difficult to guess. Passwords from different languages have different character distributions (Wanget al., 2015). As noted by Wanget al. (2015), if one tests the security strength of a native Chinese password together with English based passwords, the Chinese password is likely to be considered stronger and difficult to guess, yet it might be weaker when tested together with other Chinese passwords. As a result, this paper suggests juxtaposing substrings from at least two different languages in order to enhance passphrases security. It is also important to realise that passphrase policies recommended by Shay et al. (2016) and Melicher et al. (2016) on security grounds have at least two words separated by blank spaces. As such, juxtaposed substrings in a passphrase for this study shall be separated by blank spaces. These requirements on passphrases have the ability to overcome security loopholes that result from using common substrings in a language. In addition, the adoption of substrings from different languages is expected to reduce the effect of grammatical structures that result from using a single language to generate passphrases. It is therefore proposed that:

Proposition P3: Passphrases generated by juxtaposing substrings from different languages are more secure.

Passphrase length. Studies have shown that moving from short passwords to long passwords, herein referred to as passphrases, has the potential to enhance the overall security of passwords (Shay et al., 2016; Kelley et al., 2012; Komanduri, Shay, Kelley, Mazurek, Bauer, Christin, Cranor & Egelman, 2011). For example, all the password policies recommended by Shay et al. (2016) and Melicher et al. (2016) on security grounds are strictly for generating passphrases. The recommended password policies encourage the generation of passphrases that range from twelve to more than sixteen characters long. However, Shay et al. (2016) also note that users often generate very weak and easy to guess passphrases should these passphrases be generated without additional security enhancement controls. Thus, observations by Bonneau and Shutova (2012) and Shay et al. (2016) on reviewed passphrases revealed that the passphrase length alone was not adequate to compensate the shortcomings of generating passphrases based on a few popular words in a language. In addition, Rao et al. (2013) used parts of speech tagging to demonstrate that passphrase strength is not a direct function of length. Underlying password structures together with length play a pivotal role towards a passphrase's strength (Shay et al., 2016; Rao et al., 2013). This paper concedes juxtaposing of substrings from different languages as the determining factor of the underlying structures of passphrases for this study. As such, length is considered a function of juxtaposed substrings that make up this study's passphrase structures. It is therefore proposed that:

Proposition P4: Passphrase length moderates the relationship between the underlying passphrase structure and passphrase security.

Dictionary check. Dictionary check is a common practice for restricting users from using words in the dictionary as passwords (Komanduri et al., 2011). However, this paper proposes to use dictionary checks for making sure that user-generated passphrases are not based on a single language. Thus, dictionary check is used to promote the occurrence of juxtaposed substrings in a passphrase. Consequently, the use of a dictionary check is expected to enhance passphrase security by restricting users into generating passphrases based on substrings from multiple languages. It therefore enforces the study's view of increasing passphrase search space by encouraging the use of multilingual phrases. This control is put in place considering the fact that without any strict controls, users are bound to generate passphrases based on popular and easy- to- guess phrases in a language (Bonneau & Shutova, 2012; Komanduri et al., 2011; Shay et al., 2016). Nevertheless, users may generate passphrases based on non-standard spelling or

following phonological approximations – something that is common in code-switching among multilingual user groups (Deumert & Masinyana, 2008; Carrier & Benitez, 2010). Such substrings will not be detected by dictionary checks. However, findings from other research studies suggest that such practices have the potential of promoting the generation of secure passphrases (Shay et al., 2016; Melicher et al., 2016). For instance, the use of different character classes when generating passphrases is a proven technique for enhancing passphrase security (Shay et al., 2016). Hence, it is worthwhile to explore this practice in a multilingual user group to establish security implications. Following research findings by Komanduri et al. (2011), it is proposed that:

Proposition P5: The use of dictionary checks will improve the security of passphrases.

Based on the propositions above, a passphrase security model for a multilingual environment is shown in Figure 1.

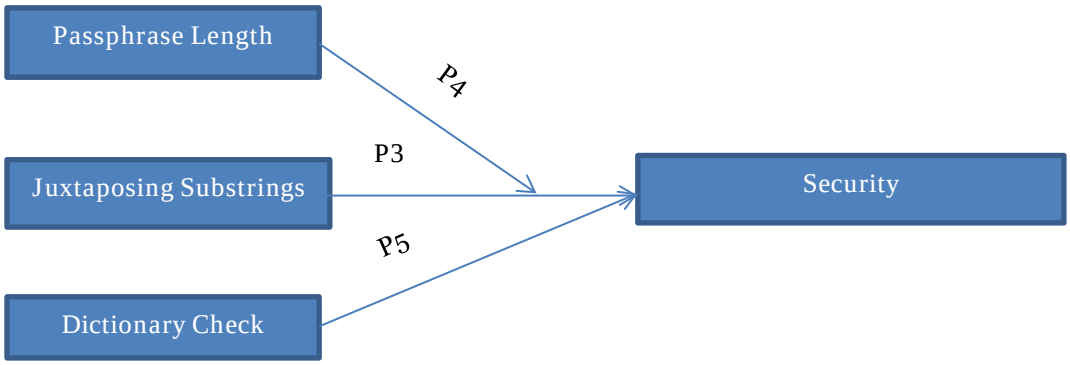

Figure 1: A passphrase security model in a multilingual environment

1.1.3 Password usability

A bias towards password security has seen the introduction of system-generated and rule-based passwords (Choong et al., 2014; Keith et al., 2009). However, users find rule-based and system-generated passwords difficult to memorise and often compensate the shortcoming of memorising complex passwords by writing them down, storing them in insecure places and in some cases, users repeatedly use the same password across multiple domains because they are difficult to create and recall (Choong et al., 2014;Keith et al., 2009). In addition, these burdensome password policies often result in users spending 1.5 to 2.25 business days each year generating new passwords (Choong et al., 2014). Choong et al. (2014) went on to rank factors considered by users when generating a password. They found memorability highly prioritised, followed by compliance with password requirements (because it is required), synchronisation of passwords for other accounts, typographic and lastly, password strength. Zhang, Akkaladevi, Luo, and Ziegelmayer (2009) state that the relationship between "text password security and memory theory has long been recognised". Psychological studies show that the working memory has a limited capacity (Cowan, 2000). It should be noted that the working memory is where learning that involves temporally maintaining, manipulating, and integrating verbal and pictorial information takes place (Schweppe & Rummer, 2014). This calls for lexical and logical semantics (Cowan, 2000; Gruszka & Orzechowski, 2016) between newly created passwords and the already known subjects in the memory. This study proposes the use of simple code switching practices to enhance passphrase usability and security. Section 1.1.1 argued for the paper's use of code switching in a multilingual society.

1.1.3.1. Factors of passphrase usability

The definition and factors of usability in the ISO 9241-11 guideline were adopted and used to guide passphrase usability in this paper. The ISO 9241-11 is a tried and tested guideline both in the industry and academia, hence it is expected to provide balanced and complete measures for evaluating passphrase usability (Bevan, Carter, & Harker, 2015). It is important to realise that research is slowly acknowledging the role of culture on the usability of information technology products and services (Winschiers-

Theophilus & Bidwell, 2013). The ISO 9241-11 of 1998 guideline defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and user satisfaction in a specified context of use". During the time of releasing this definition, usability was only limited to products. Recent reviews on the ISO 9241-11 guideline for usability saw the incorporation of services and systems, thereby making the guideline suitable for this study. As required by the definition of usability, this study concedes that all users of password authentication mechanisms with multilingual skills are its system users. Further, this paper agrees with research findings by Choong et al. (2014) that irrespective of the importance of passphrase security to the systems administrator, generating a memorable passphrase is the primary goal of system users.

It is therefore considered that users should be able to generate memorable passphrases with effectiveness, efficiency and user satisfaction if they are to attain passphrases usability. Effectiveness, efficiency and user satisfaction are therefore considered as factors of passphrase usability in this study. There are different metrics in the literature that can be put against effectiveness, efficiency and user satisfaction such as those in Keith et al. (2007), Shay et al. (2016) and Melicher et al. (2016). Melicher et al. (2016) researched usability and security of text passwords on mobile devices and identified the following usability factors: time taken to create a password; copy and paste; number of deletions during password generation; password storage on other media; the number of password creation attempts; re-entry: attempts needed to correctly type in a password, and reason of password failure. A research study on different password policies by Shay et al. (2016) evaluated usability factors. Some of the evaluated factors of usability were similar to those used by Melicher et al. (2016). Their usability factors included study drop out; password storage; password creation attempts; password creation failure; recalling the password, and time spent entering passwords during first successful attempt (Shay et al., 2016). Choong et al. (2014) researched users' password management behaviours that could be aligned to passphrase usability and noted that users find passwords requirements burdensome; users spend a lot of time generating passwords; users prioritise password memorability; users often store passwords on secondary devices, and users face log in problems (Choong et al., 2014). In addition, Keith et al. (2007) investigated passphrases usability and user satisfaction. Typographical errors and memorability were used to evaluate usability. One's intent to switch to the use of passphrases as a form of authentication was used to measure user satisfaction (Keith et al., 2007). These factors were combined and some were consolidated to arrive at metrics for ascertaining effectiveness, efficiency and user satisfaction. It should be noted some of these usability factors have received thorough validation as they have been tested on different password policies and different devices over a considerable amount of time (Shay et al., 2016; Melicher et al., 2016).Table 1 summarises the usability factors for this study in accordance to the revised ISO 9241-11 guideline.

According to ISO 9241-11, effectiveness relates to the accuracy, completeness and appropriateness with which users are achieving their goals. As a result, the ability to generate a passphrase accurately and memorise it can contribute to passphrase usability. It is the systems administrator's duty to create passphrase policies that can promote both usability and security. Some complex passphrase policies aimed at enhancing security can make passphrase generation difficult, thereby making them unusable (Choong et al., 2014; Shay et al., 2016). For example, in some studies the use of dictionary checks was found to be frustrating for users during passphrase generation (Komanduri et al., 2011). However, increasing the size of the search space from which to source optional substrings for passphrases generation is expected to compensate for possible limitations associated with dictionary checks. In addition, accurately memorising and recalling a passphrase is expected to enhance the usability of the passphrase policy. Psychological studies show that poorly designed passphrase policies make it difficult for users to exploit their easily accessible short-term memory when generating passphrases (Keith et al., 2007). Users end up generating passphrases that do not relate to their immediate memory, thereby complicating passphrase generation and their subsequent memorisation. However, this study's approach of encouraging users to generate passphrases based on their daily skills of practicing code switching as demonstrated in short text messages is expected to make passphrase generation and memorability easy. Further, users will also be expected to meet passphrase requirements when completing the task of generating passphrases.

Table 1: Factors of passphrase usability considered for this study

Factors	Attribute	Measure	Source
Effectiveness	Accuracy	Recalling passphrases	Choong et al., (2014); Keith et al. (2007); Shay et al. (2016)
	Completion	Meeting passphrases requirements	Shay et al. (2016)
	Appropriateness	Password creation failure: Failure to meet requirements and password mismatch	Melicher et al. (2016); Shay et al. (2016)
		Password reminder usage	Shay et al. (2016)
		Password storage: writing down passphrases, copy and paste, and automatic text entry	Choong et al., (2014); Melicher et al. (2016); Shay et al. (2016)
Efficiency		Time taken to type in a passphrase	Melicher et al. (2016); Shay et al. (2016)
		Passphrase creation attempts	Melicher et al. (2016); Shay et al. (2016)
		Passphrase recalling attempts	Melicher et al. (2016); Shay et al. (2016)
		Time taken to generate a passphrase	Choong et al., (2014); Melicher et al. (2016)
User satisfaction		Users quitting passphrase generation	Shay et al. (2016)
		Attitude towards passphrase policy	Choong et al., (2014); Keith et al. (2007)

The revised ISO 9241-11 guideline for usability recommends that the efficiency metric should account for expected risks should users fail to meet their goals. As such, it is expected that a passphrase policy's failure to assist users to perform (accurately and completely) appropriately might result in the user failing to generate passphrases accurately according to the policy requirements. Users who find passphrases difficult to memorise are expected to store their passphrase on secondary media. In addition to memorability challenges, users are also expected to request for password reset. Conversely, more time spent on typing long passwords compared to the time needed to type in a short password is expected to reduce the efficiency of passphrases. User frustration from a complex passphrase policy might negatively impact user satisfaction, leading to study drop out. Nevertheless, a keen interest to continue using passphrases as a form of authentication in the real word might suggest user satisfaction.

1.2 The proposed model

The usability and security propositions in this paper led to a model shown in Figure 2. The past decades have seen a number of policy propositions for increasing the size of the search space from which unique passwords could be drawn. Different approaches to increasing the size of the search space have been suggested. For example, "enforcing the inclusion of numbers and special characters, requiring both upper and lower case letters, and increasing minimum password lengths" (White, Monrose, Shaw, & Moreton, 2014), while others recommend less use of predictable grammatical structures in passphrases (Rao et al., 2013). Despite all these efforts, the usability and security of passwords and passphrases remain questionable (Andersson & Saedén, 2013; Bonneau & Shutova, 2012; Rao et al., 2013; Kelley et al., 2012).

As such, this paper motivates the use of passphrase policies that encourage passphrases made of multilingual substrings. The use of multilingual substrings is expected to increase the size of the search space from which passphrases can be drawn and overcome most usability and security concerns. Such policies are applicable in sub-Saharan Africa, for instance, where the majority of countries do not use their native languages as their official language – a move that created a multilingual environment (Lexander, 2011). In addition, Kang's (2015) admission that globalisation is fast promoting a multilingual environment and his subsequent research findings suggest that the success in usability and security of a text-based authentication mechanism may lie in policies that are driven by contextualised factors such as culture and language in this case. Figure 2 shows constructs of usability and security in the proposed model. Such a model can be used for designing passphrase policies for multilingual societies.

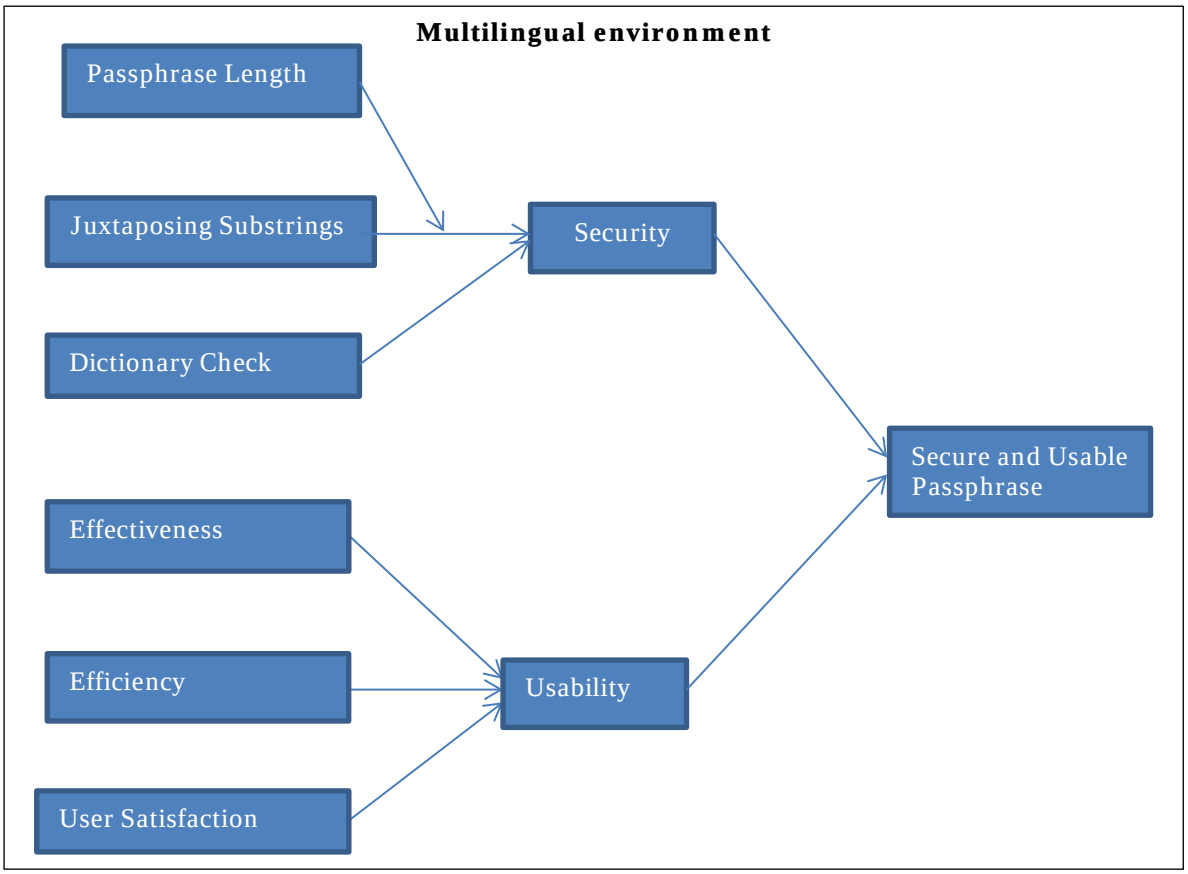

Figure 2: A proposed model for usable and secure passphrases in a multilingual environment

1.3 Conclusion

The paper motivated the need to increase the size of passphrase search space by using more than one language during the generation of passphrases. The multiple cultures perspective suggests users can learn and understand different languages which can be used simultaneously as revealed by the practice of code switching. This is suggested with a motive to maximise on passphrases usability and security. Even though less recognised in the literature on passwords, other studies found culture with language in particular to be a major factor in depicting usability and security issues (Kang, 2015; Winschiers-Theophilus & Bidwell, 2013). As such, this paper presented its argument on how multilingual passphrases can address challenges that are herein considered a factor of generating passphrases using a single language. The paper proposed dictionary checks, the use of juxtaposed substrings and passphrase length as major factors contributing to passphrases security in a multilingual environment. The ISO 9241-11

guideline on usability was used to provide guidance in identifying factors of usability. This guideline has been tried and tested; hence it can provide a complete set of factors for ascertaining usability for passphrases. These factors include effectiveness, efficiency and user satisfaction. Extending a common practice of code-switching in a multilingual environment to authentication is expected to enhance the usability of passphrases. In conclusion, it is argued that juxtaposing during passphrases generation can be done with effectiveness and efficiency, thereby resulting in user satisfaction.

Future research: This model is going to be tested for security and usability. The aim is to establish utility compared to the available approaches for generating usable and secure passphrases. The model and its factors shall be quantitatively tested with data gathered through an experiment in line with other related research studies (Kelley et al., 2012; Komanduri et al., 2011; Melicher et al., 2016). It is believed that, if tested, such a model can help inform the designing of passphrases policies for multilingual environments.

References

Andersson, D., & Saedén, D. (2013). Authentication with Passwords and Passphrases-Implications On Usability And Security. *Unpublished Work, Lund University School Of Economics And Management, Department Of Informatics, Sweden*.

Beeler, B., & Saint-Leger, G. (2014).Understanding Technology Adoption from the "Multiple Cultures Perspective": The Case of a Successful Post-Implementation Recovery. *Management international / International Management / Gestiòn Internacional*, *18*(2), 169-180.

Bevan, N., Carter, J., & Harker, S. (2015). ISO 9241-11 revised: What have we learnt about usability since 1998 ? In *Proceedings of Human Computer Interaction*.

Bonneau, J., & Shutova, E. (2012).Linguistic properties of multi-word passphrases. *In International Conference on Financial Cryptography and Data Security* (pp. 1-12).Springer Berlin Heidelberg.

Carrier, L. M., & Benitez, S. Y. (2010). The Effect Of Bilingualism On Communication Efficiency In Text Messages (SMS). *Multilingua-Journal of Cross-Cultural and Interlanguage Communication*, *29*(2), 167-183. DOI: 10.1515/mult.2010.007

Choong, Y. Y., Theofanos, M., & Liu, H. K. (2014).United States Federal Employees' Password Management Behaviors– a Department of Commerce Case Study. *National Institute of Standards and Technology Interagency Report (NISTIR), 7991*: USA.

Cowan, N. (2000). The Magical Number 4 In Short-Term Memory: A Reconsideration Of Mental Storage Capacity. *Behavioral and Brain Sciences*, *24*(1), 87–185.

Deumert, A., & Masinyana, S. O. (2008). Mobile Language Choices—The Use Of English And Isixhosa In Text Messages (SMS) Evidence From A Bilingual South African Sample. *English World-Wide*, *29*(2), 117-147.DOI: 10.1075/eww.29.2.02deu

Gruszka, A., & Orzechowski, J. (2016). Meta-Analysis of the Research Impact of Baddeley's Multicomponent Working Memory Model And Cowan's Embedded-Processes Model Of Working Memory: A Bibliometric Mapping Approach. *Polish Psychological Bulletin*, *47*(1), 1-11.

Hofstede, G. (2013). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, *2*(1), 1-26.

Houshmand, S., & Aggarwal, S. (2012).Building Better Passwords Using Probabilistic Techniques. *Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, Florida, USA International* (pp. 143–151). Los Angeles: Springer LNCS.

Kang, P. (2015). The effects of different alphabets on free text keystroke authentication: A case study on the Korean–English users. The Journal of Systems and Software 102 (2015) 1–11.

Keith, M., Shao, B., & Steinbart, P. J. (2007). The Usability Of Passphrases For Authentication: An Empirical Field Study. *International Journal Human-Computer Studies*, *65*(1), 17–28. doi:10.1016/j.ijhcs.2006.08.005

Keith, M., Shao, B., & Steinbart, S. P. (2009). A Behavioral Analysis of Passphrase Design and Effectiveness. *Journal of the Association for Information Systems*, *10*(2), 63-89.

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., & Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms.*In2012 IEEE Symposium on Security and Privacy* (pp. 523-537).IEEE.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Egelman, S. (2011). Of passwords and people: measuring the effect of password-composition policies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 11-7 May, Vancouver, BC, Canada.

Kruger, H., Flowerday, S., Drevin, L., & Steyn, T. (2011).An assessment of the role of cultural factors in information security awareness.*ISSA2011*. Presented at the Information Security South Africa Conference, Hyatt Regency Hotel, Rosebank, Johannesburg, South Africa: IEEEXplore. doi:10.1109/ISSA.2011.6027505 - ISBN: 978-1-4577-1481-8

Lexander, K. V. (2011). Texting and African language literacy. *New media & society*, *13*(3), 427-443. DOI: 10.1177/1461444810393905

Li, Z., Han, W., & Xu, W. (2014).A Large-Scale Empirical Analysis of Chinese Web Passwords. *Proceedings of the 23rd USENIX Security Symposium, 20–22 August, San Diego, USA.*

Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., & Mazurek, M. L. (2016).Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 7-12* May, San Jose, USA.

Morel, E., Bucher, C., Pekarek-Doehler, S., & Siebenhaar, B. (2012). SMS Communication As Plurilingual Communication: Hybrid language use as a challenge for classical code-switching categories. *Lingvisticae Investigationes*, *35*(2), 260-288.DOI: io.i075/li.35.2.oSmor

Peffers, K., Tuunanen, T., Rothenberger, M., A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77.

Rao, A., Jha, B., & Kini, G. (2013).Effect of Grammar on Security of Long Passwords. *Proceedings of the CODASPY Conference, 18–20 February, San Antonio, Texas, USA.*

Schweppe, J., & Rummer, R. (2014). Attention, Working Memory, And Long-Term Memory In Multimedia Learning: An Integrated Perspective Based On Process Models Of Working Memory. *Educational Psychology Review*, *26*(2), 285-306.

Shay, R., Komanduri, S., Durity, A. L., Huh, P. S., Mazurek, M. L., Segreti, S. M., & Cranor, L. F. (2016).Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security (TISSEC)*, *18*(4), 13.

Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, L. M., Segreti, S. M., Ur, B., Bauer, U., Christin, N., & Cranor, F. L. (2014).Can Long Passwords Be Secure and Usable? *Proceedings of the CHI 2014, 26 April – 01 May, Toronto, Canada.*

Veras, R., Collins, C., & Thorpe, J. (2014). On the semantic patterns of passwords and their security impact. *Proceedings of the* NDSS, 23, 23-26 February, San Diego, USA.

Wang, D., Cheng, H., Gu, Q., & Wang, P. (2015). *Understanding Passwords of Chinese Users: Characteristics, Security and Implications.* Available online: https://www.researchgate.net/profile/Ding_Wang12/publication/269101022_Understanding_Passwords_of_Chinese_Users_Characteristics_Security_and_Implications/links/5544e2700cf23ff7168696a8.pdf

White, A. M., Shaw, K., Monrose, F., & Moreton, E. (2014).Isn't that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens. *In Proceedings of the 2014 workshop on New Security Paradigms Workshop* (pp. 25-38). ACM.

Winschiers-Theophilus, H., & Bidwell, N. J. (2013).Toward an Afro-Centric indigenous HCI paradigm.*International Journal of Human-Computer Interaction*, *29*(4), 243-255.

Zhang, J., Akkaladevi, S., Luo, X., & Ziegelmayer, J. (2009). Improving Multiple-Password Recall: An Empirical Study. *European Journal of Information Systems*, *18*(2), 165–176.