Password Strength Metre Application

https://doi.org/10.3991/ijim.v15i15.22323

Sirapat Boonkrong(✉), Arkalerk Kitthimon, Patchara Koksoungnoen, Krissada Jenprakhon
Suranaree University of Technology, Nakhon Ratchasima, Thailand
sirapat@g.sut.ac.th

Abstract—Passwords are considered the most commonly used method of authentication. Unfortunately, weak passwords as chosen by many users are known to be the main cause of many cyber attacks. With stronger passwords, it is believed that this first line of defence would be able to reduce the risk of cyber attacks, trespass and information exposure. A password strength metre application was, therefore, developed so that users can try out the passwords of their choice before actually deciding to register them. This was done with an aim of assisting users in choosing stronger and harder-to-crack passwords. The proposed application was developed with four main password strength indicators namely password entropy, probability of the password being cracked, actual effective password length and time taken to crack the password. Although the application contains these seemingly complex metrics, the data is presented in a user-friendly way so that it is intuitive to any users.

Keywords—access control, authentication, password, password strength

1 Introduction

It cannot be denied that cyber attacks occur to individuals, small and large organisations almost, if not, daily. Many have put both time and resources on security mechanisms to make their information systems better equipped to withstand today's cyber threats. Although there are other mechanisms such as encryption and data hiding [2][10], access control is usually one of the first mechanisms to be deployed in a computer-related system in order to reduce the risk of an attack. Access control consists of four processes. They are identification, authentication, authorisation and accounting. *Identification* is when a user or an entity states their identity. A common example is when a user states their username when attempting to log into a system. *Authentication* is the confirmation of the stated identity. That is, it is a process in which a user or an entity proves to a system that they are who really say they are. *Authorisation* is the restriction of access. In other words, once a user or an entity is permitted to enter a system, they will be given an access right to the resources within the system. Each user or entity usually has different access restrictions. For example, the human resource department is allowed to have access to the employees' information, but the

finance department is not. *Accounting* is basically keeping track or keeping record of what a user or an entity does when working within a system. The main goal of access control is to ensure that only authorised user or entity is permitted to enter the system.

Authentication is thought of by many as the first line of defence that any user, entity and even an adversary has to face before being able to access a system. There are three major methods of authentication [4] that have been implemented by today's practitioners. They are something-you-know, something-you-have and something-you-are methods.

The *something-you-know* method of authentication is basically when a user uses something they can remember as a credential to prove and confirm their identity. A good example of this method is, of course, the use of a password or a personal identification number (PIN). The *something-you-have* method of authentication is when a user possesses and uses an additional device to help with the process of identify confirmation. Examples of this method include an authentication token, a smart phone and a smart card. The *something-you-are* method is when a user either uses a part of their body or their behaviour to prove to a system that they are really who they say they are. This method is also known as biometric authentication. Examples include the use of fingerprint, retina, iris, walking pattern and typing pattern. There are also other authentication methods available such as the something-you-process method, somewhere-you-are method and someone-you-know method. However, they have not been deployed as much.

Out of all the available authentication method, the something-you-know, specifically password, is by far the most commonly used. This is due to its low cost and convenience. When a password is deployed, there is no need for any extra devices. Users are only asked to generate a password and memorise it for the login or authentication purpose. In the case where the password is forgotten, all the users have to do is to reset their password, which is when a new password is generated.

It appears that no matter what process it is, whether it is the first time a password is generated or the time when it is reset, it is the responsible of a user to choose their own password. This is precisely the problem many organisations have today and is one of the main causes of a cyber attack on a computing system. As stated, the something-you-know method requires a user to memorise their credential, a password in this case. A study in [1] even stated that a considerable number of users stored their passwords on their mobile devices. Many users, therefore, choose a password which is easy to remember, which in turn leads to a password that can easily be guessed or cracked by an adversary. Passwords that can easily be cracked are said to be weak passwords. Examples of weak passwords [12] include 1234, aaabbbccc, password, letmein, qwerty or any of their variations such as letmein001 or letmein002. They can also be basic words that appear in an English dictionary, including dragon, football and picture.

There are a couple of techniques [4] adopted by attackers to crack weak passwords. The first is a brute force attack, which is when an attacker attempts all possible variations and combinations of a password until the correct one is found. The second is a password dictionary attack. This is when a list of most used passwords is compiled in a database called a password dictionary. Only the passwords in the dictionary are tried and tested when an attacker attempts to carry out authentication as someone else.

Up until recently, there have been countless of incidents, both reported and unreported, related to password cracking. The followings are some of the most notable ones. As early as 1998, a Computer Emergency Response Team or CERT reported an incident where almost two-hundred thousand passwords were leaked and nearly fifty thousand of them had been cracked [5]. In 2009, one of the largest credential leakages occurred in a major password breach of a Web site [8]. The attacker made all of the thirty-two million passwords available on the Internet. This list has now become the basis of today's password dictionary used by attackers. Even official international or government organisations experienced a breach personal information, which led to the release of more than eleven thousand usernames and passwords to the public. It has also been revealed that some of the government personnel used passwords as weak as 1234 [7]. In addition, there have been major security breaches in recent years including those at large social networking sites, news agencies and auction Web sites.

Furthermore, weak passwords are an important security issue, especially when default passwords remain unchanged. Default passwords are passwords that are generated by a manufacturer of a device. They are usually as simple and easy-to-guess as 1234, password or admin. It is often the case that users do not change them because they are easy to remember, which means that they become an easy target for an attacker to carry out password cracking. If the attack is successful, the attacker can take control of the device and perform any harmful action to accomplish their attack objective.

It can now be seen that it is inevitable to find users who choose to stick with using default passwords and choose easy-to-crack passwords. It is, therefore, essential that users choose stronger passwords so that the risk of an attack, namely password cracking, can be reduced. As a result, this has become our research problem to solve. One of the approaches that have been introduced and used by many systems to help users choose a stronger password is a password strength metre.

1.1 Related work and research objective

A password strength metre is an indicator, usually in graphical form, that shows how strong a password entered by a user is and how resistant to password cracking it could be. The way a password strength metre works is that it is assigned with rules so that points based on the length and combination of letters, numbers and special characters can be calculated. The points are then translated into the strength of the password. A password strength metre normally displays different colours to indicate the password strength. Red usually implies that the password is weak and can easily be cracked. Amber illustrates a medium strength password. Green provides a sign of a strong password that has a low risk of password cracking. A typical password strength metre can be seen in Figure 1.

A study [17] has found that password strength metres can be an important factor which helps motivate users to create a stronger password. The motivation effect is even higher when users are provided with numerical scores. Although the password strength metre, like the one shown in Figure 1, is simple and easy to use, it is obvious that it lacks necessary information which can assist users in producing a better and stronger password.

Fig. 1. A typical password strength metre

It is, therefore, felt that it would be more useful if a password strength metre could provide more information to the user regarding the strength of their entered password so that appropriate adjustment can be made to improve the password strength. This is the objective of our work. In other words, we would like to design and develop a password strength metre in such a way that the metre provides information in more dimension than just stating whether the entered password is "weak" or "strong." The research did not only develop an application that measured the password strength, another important aspect namely the performance or the speed of the computation was also measured to ensure that the users would not feel any delay when using the application.

Furthermore, it is important to point out and make it clear early that the difference between password managers and the proposed application is as follows. A password manager is software that allows users to generate and store their passwords either locally or on the cloud. When they log into a system, the password manager simply fills in the password for that particular system on the users' behalf. However, what the proposed application does is that it helps users examine the strength of their chosen passwords in such a way that they know which dimensions, if any, of their passwords could be improved so that they obtain stronger passwords as a result.

2 Background knowledge

According to [13] in 2005, it was claimed that passwords would still be a popular authentication method in the future due to its simplicity. However, as already suggested earlier, the strength of the something-you-know authentication mechanism relies heavily on the strength of the passwords. It is, therefore, necessary to find a way to measure the quality and the strength of passwords. Many researchers have introduced methods that can be used to accomplish the mentioned goal. These approaches have,

of course, become an integral part of the proposed password strength metre. Accordingly, this section provides the description of the background knowledge used to design and develop the password strength metre. The section gives explanation of the related principles and theories of how the strength and quality of a password can be measured.

The calculation of the strength and quality of a password is an essential part of the design and development of a password strength metre. This is because the calculated value provides a feedback to the user indicating how strong their chosen password is. For the purpose of creating a password strength metre, four different metrics have been selected to be included in the system. They are password entropy [8][16], probability of a password being cracked [6], effective length of a password [9] and password crack time. These quantitative measurements form the core function of the proposed password strength metre, in addition to other simpler computations that comprise of the actual length of the password, the number of lower case letters (a – z), the number of upper case letters (A – Z), the amount of numerical characters (0 – 9) and the number of special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).

2.1 Password entropy

The concept of entropy was first introduced by Shannon [14] who defined information entropy as a measure of information content. It was basically the statistical distribution of a language or information, which measures the uncertainty and randomness of the presented content. To put it simply, it is the measurement of how unpredictable a password is. Password entropy has, therefore, been applied as the quality indicator by many. One common way to calculate password entropy is using Equation 1.

$$E = \ln(R^L) \tag{1}$$

where E is the password entropy and is measured in bits, R is the pool of unique characters, and L is the number of characters in the password. Higher entropy means that the password has better quality. However, Ma *et al*., [9] and Taha *et at*., [16] suggested that password entropy was only loosely defined and not suitable for indicating password quality, because it does not take into account anything else other than the two stated variables in R and L. Consequently, it was decided that the proposed password strength metre would apply the concept of distribution areas of password entropy, introduced by [16], instead. This is because [16] suggested that the distribution areas of password entropy provided a better indication of the quality of the password based on the search space. The problem with the entropy distribution calculation mentioned in [16] is that it only takes into account the combination of lower case letters, numbers and special characters. This paper, therefore, has made the calculation more complete by introducing a new variable for upper case letters. Based on the entropy distribution formula introduced in [16], the value of upper case letters is included as an additional variable, Equation 2 is derived as a result.

$$E = C_L^a * 26^a * C_L^A * 26^A * C_L^n * 10^n * C_L^s * 31^s \tag{2}$$

where E is the password entropy distribution, a is the number of lower case letters, A is the number of upper case letter, n is the number of numerical characters, s is the

number of special characters and L is the number of characters in each category (lower case letters, upper case letters, numbers or special characters.) It should be noted that 26 is the total number of the English alphabet (a – z or A – Z), 10 is the total amount of numbers (0 – 9) and 31 is the total number of special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).

Although Equation 2 or the distribution areas of password entropy is an improvement on the original password entropy calculation, it still does not cover enough criteria to indicate how strong a password is. This is why the proposed password strength metre needs to apply other indicators, too.

2.2 Probability of password being cracked

In the proposed password strength metre, password complexity is defined as the probability of a password being cracked. The probability of a password being cracked was introduced by [6] and is calculated based on several variables. They are the length of time T that a password is valid, the number of guesses G that a cracking device can guess per second, the number of possible characters N in each password position (if lower case letters, upper case letters, numbers and special characters are all allowed in a password, then the value of N is 93, for example), the password length L and the password space P which is computed by $P = L^N$. The probability that a password can be cracked is, therefore, calculated by

$$Prob(password\ being\ cracked) = (T * G)/P \tag{3}$$

The reason that the probability of a password being cracked was chosen as an indicator in the proposed password strength metre was because it was believed that the probability value would provide an easy-to-understand signal of how stronger a user's chosen password was.

2.3 Effective password length

The concept of effective password length was first introduced by [9]. The effective length is an interesting idea for indicating another dimension of the password strength. While existing password strength metres count the actual number of characters in the password to specify the size, the effective password length takes into account password complexity index. The notion of password complexity index or PCI was proposed by [9] to identify how complex a password is compared to the standard format password (letters only or numbers only).

In order to understand how the effective password length is calculated, the password complexity index needs to be explained. Firstly, a password can contain any characters from the four groups of lower case letters, upper case letters, numbers and special characters. A value is assigned to each group based on the number of characters. That is, 26 is assigned to the lower case and upper case letters groups. 10 is assigned to the number group, and 31 is assigned to the special characters group. That means if a password contains lower case letters, upper case letters, numbers and special characters, the value of each group is added to one another to obtain the PCI value of 26 + 26 + 10 + 31 = 93.

However, if a password only contains lower case letters, then the PCI will have the value of 26.

The effective password length, according to [9], can then be calculated as shown in Equation 4.

$$L = m * log_{10}C \tag{4}$$

where L is the effective password length, m is the length of the password and c is the password complexity index.

2.4 Crack time

One final indicator to be included in the proposed password strength metre is the amount of time that the password can be cracked. The reason for integrating this factor in the proposed password strength metre is that the crack time can provide a simple and quick indicator to the user. That is, higher crack time means stronger password while lower crack time indicates that the password can be cracked in a short amount of time.

The crack time of a password can simply be computed using Equation 5 as follows.

$$T = L/G \tag{5}$$

where T is the time it takes to crack a password (in seconds), L is the number all possible passwords of the given length, and G is the number passwords that a cracking device can test per second.

On the whole, the proposed password strength metre would contain four main indicators. They are password entropy distribution, probability of a password being cracked, effective password length and password crack time.

3 Design and development

The previous section shows that the indicators had now been chosen and explained. This section, therefore, gives an overview of how the password strength metre was designed and developed.

3.1 Design

The main problem with the selected indicators is that while they provide detailed calculations, they results do not seen intuitive to ordinary users. It was, therefore, necessary to design the password strength metre in such a way that it would be easy to understand and could be understood quickly

The design was begun with password entropy distribution values. From Equation 2, it can be seen that the calculated entropy distribution values will be numbers lying in a wide range, depending on the characteristics of the password. Instead of just displaying the actual entropy distribution value of each password, it was decided that a simpler gauge would be more suitable for ordinary users.

In order to create a gauge for measuring password entropy distribution, a pool of different passwords was generated so that some general idea of the actual range of the entropy distribution would be obtained. In other words, fifty thousand four-character passwords were randomly generated. These passwords were both standard passwords, i.e., numbers only or letters only, and the mixture of all types of characters. The password entropy distribution value of each of the generated password was calculated and recorded. The process was repeated for five-character, six-character up to sixteen-character passwords. It was found that the range of the password entropy distribution values was between 4 (this is when the password consisted of only four numbers) and $3.13*10^{31}$ (this is when a mixture of all types of characters was chosen in a sixteen-character password).

Once the range was obtained, it was decided that the entropy gauge would be divided into four parts based on the exponents of the base number, which was ten in this case. Therefore, the gauge would hold the values between 0 and 31. This range was simply divided into four levels of the entropy distribution values, which were terrible, good, strong and perfect. These words were chosen due to their simplicity and ability to convey the message. The principal design of the different levels of the gauge can be seen in Figure 2.

Fig. 2. A design of the password entropy distribution gauge

The second gauge to be designed was the gauge for the probability of a password being cracked using the Equation 3. A similar process to the password entropy was followed. In other words, fifty thousand passwords of each password size from four characters to sixteen characters were generated, and the probability of each of them being cracked was then computed. Again, a wide range of the probability values were obtained. This time, the range was approximately between 10–31 and 10–92. This range was then divided into the same four levels as the entropy, including terrible, good, strong and perfect. If the probability were high in value, i.e., the exponent was a negative of a smaller number, it would fall into a lower part of the gauge. In contrast, if the probability were low, i.e., the exponent was a negative of a larger number, it would fall into a higher part of the gauge, meaning that this password was on the stronger side. The principal design of the probability of being cracked gauge was similar to the one in Figure 2 and can be seen in Figure 3.

Fig. 3. A design of the probability of password being cracked gauge

Regarding the probability of a password being cracked, looking at Equation 3, one variable that needs to be assigned a value is the number of guesses a cracking device can process per second. That means prior to computing the probability, a device to be used for cracking needs to be selected so that the speed in the number of guesses

per second can be assigned to the formula. In the proposed password strength metre, five different devices were used as the baseline for the speed of password guessing. They included the Nvidia Tesla A100, Google TPU, Nvidia Titan RTX, Nvidia GeForce RTX 3080 Ti and the Antminer S19. These processors were selected due to their performance and, more importantly, their popularity among password crackers as well as their application on high intensity operations. Their speed is summarised in Table 1. It should be noted that a teraflop is translated to a device being able to process one trillion calculations per second.

Table 1. Devices and their speed

Device/Processor	Speed
Nvidia Tesla A100	321 Teraflops
Google TPU	420 Teraflops
Nvidia Titan RTX	130 Teraflops
Nvidia GeForce RTX 3080 Ti	59.5 Teraflops
Antminer S19	1.39 Teraflops

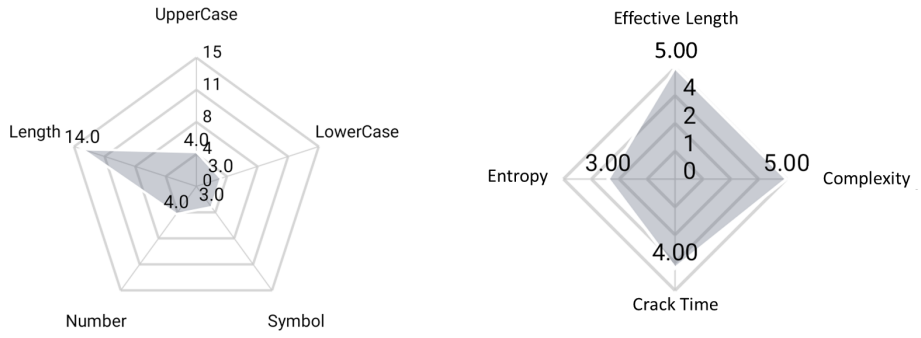
Another variable in the probability formula is the amount of time that the password is valid. It is, therefore, important to ask users to choose the length of time for which they think the password will be used. The choices that were designed to be available for selection regarding this variable were one day, seven days, one month, three months, six months and one year. It should be noted that the choice of one day could represent a one-time password and the choice of seven days could represent a temporary password to some computing system. Moreover, the choices of one month, three months and six months were selected to be parts of the design because many organisations issued a password changing policy with these periods. The choice of one year was the maximum of the design because it was not recommended to use the same password for longer than this amount of time. A closer look at the probability formula shows that the shorter the time the lower the probability of the password being cracked. That means by choosing the period in which the password was to be used would affect the strength of the password, too.

The third metre that was designed was the effective password length metre. It was mentioned in [9] that the effective length could range from a very low number. If the effective length of a password had the value of fourteen or higher, it would be deemed a strong password. This is because when the effective password length value is higher than fourteen, it means that there are at least 10^{14} possible passwords to be attempted. From this, an effective password length metre could be easily designed, following the same idea as ones explained previously. The values of the effective length were also divided into four levels – terrible, good, strong and perfect. The principal design of the metre is shown in Figure 4.

Fig. 4. A design of the effective password length metre

The fourth and final metre to be designed was the crack time metre. The crack time metre was more straight forward to design because the time taken to crack a password could range from practically no time, i.e., 0 seconds, to any arbitrary time, i.e., millions of years. The principal design of this metre was similar to the other metres and would be divided into four levels, depending on the amount of time it would take (in seconds, days or years) to crack the password.

Since the four indicators were to be separately presented in separate metres, it was felt that it would be useful to provide a summary in one simple chart so that a quick overview of the strength of the password could be examined. A radar chart illustrating the values of all four dimension was, therefore, included in the design. Furthermore, the characteristics of each password would also be shown in another radar chart so that users could grasp an overview of what their entered password consisted of. This radar chart was designed to display five characteristics of each entered password. They included the number of lower case letters, the number of upper case letters, the number of numerical digits, the number of special characters and the total number of characters or the length of the password. An example of the design of the password characteristics and pass strength radar charts can be seen in Figure 5(a) and Figure 5(b), respectively. The designs in Figure 5(a) and Figure 5(b) illustrate that when a password is entered into the application for strength test, these charts will be what the users see as the result.



(a) Password characteristics (b) Password strength indicators

Fig. 5. Design of password radar charts

3.2 Development

It was decided that the password strength metre would be developed into a mobile application. This is because in recent years the statistics indicate that more than half of all the Internet traffic can be attributed to mobile devices and smart phones. In January 2021, the actual numbers were that 57.32% of the Internet traffic was from mobile devices, while 42.68% were from desktop computers [15]. Therefore, by having a password strength metre in the mobile application format users can take the application anywhere with them. Whenever they are asked to generate a new password, the password strength metre will literally be on hand with them. The overall system can be seen in Figure 6.

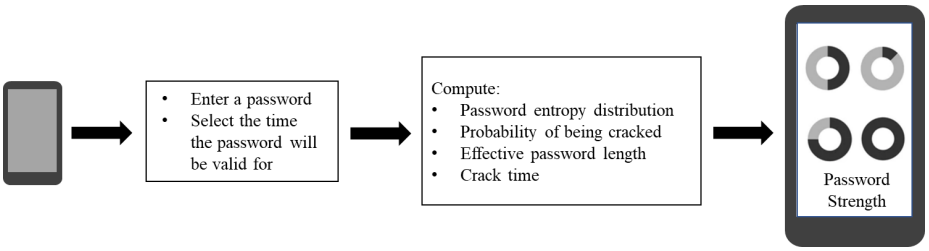


Fig. 6. System overview

Figure 6 shows the overview of the password strength metre application whereby a user willing to test the strength of their password enters a password into the application. They can also select how long their password will be valid for. The user can subsequently view the results of the password strength computation in four dimensions, which consist of password entropy distribution, probability of the password being cracked, effective password length and crack time.

The password strength metre application was developed for an Android environment. Any version of Android operating system can accommodate this application since it does not contain any sophisticated technologies. The application was tested from Android version 4.4 to Android version 10.0 without any issues.

4 Results and discussion

The password strength metre application consists of two main screens. The first screen mainly allows users to enter a password. They can also choose a cracking device from the available choices as well as the amount of time the password will be valid for. Once the information is entered, the second screen is displayed. This screen presents the results of the calculation of the password strength metrics, which consists of the four indicators in graphical form. The two main screens of the password strength metre application are shown in Figure 7.

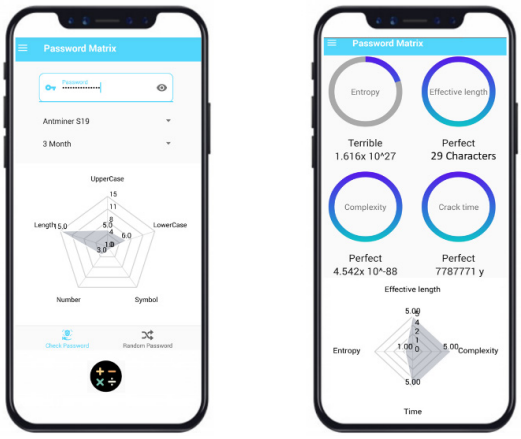


Fig. 7. Password strength metre main screens

In users' perspective, when testing the strength of their passwords, they will be presented with the screens in Figure 7. The one on the left shows what their entered password consists of in terms of number of letters, numbers and special characters. The screen on the right shows the four metrics in password entropy distribution, effective length, complexity and the time it would take to crack the entered password. In other words, what users will be able to interpret from the metrics are the unpredictability of the password, the effective length of the password, the chance of the password being cracked and how long it would take to crack the password, respectively.

In addition, the resultant password strength metre application is to be discussed in two folds. The first is the security and privacy aspect of users. The second is the performance in terms of computational speed.

Whenever an application related to any cyber security issue is developed, there is always a concern about users' security and privacy. Fortunately for this proposed password strength metre application, it must be pointed out that for security purposes, the application does not contain any database for storing the entered passwords. All the application does is that it takes an input which is a password, calculates the password strength metrics and displays the results. No passwords are stored within the application or anywhere on the Internet. This also implies that the password strength metre can work offline as a standalone application.

Another aspect that needs to be discussed here is the performance, specifically the speed of computation of all the password strength indicators. An experiment was run on fifteen random passwords of each of the password sizes between four characters and sixteen characters. The time taken to calculate the results of all four metrics were observed by looking at the application's log file and then recorded. It was found that the computation time between different sizes of passwords was not significantly different from one another, as displayed in Figure 8.

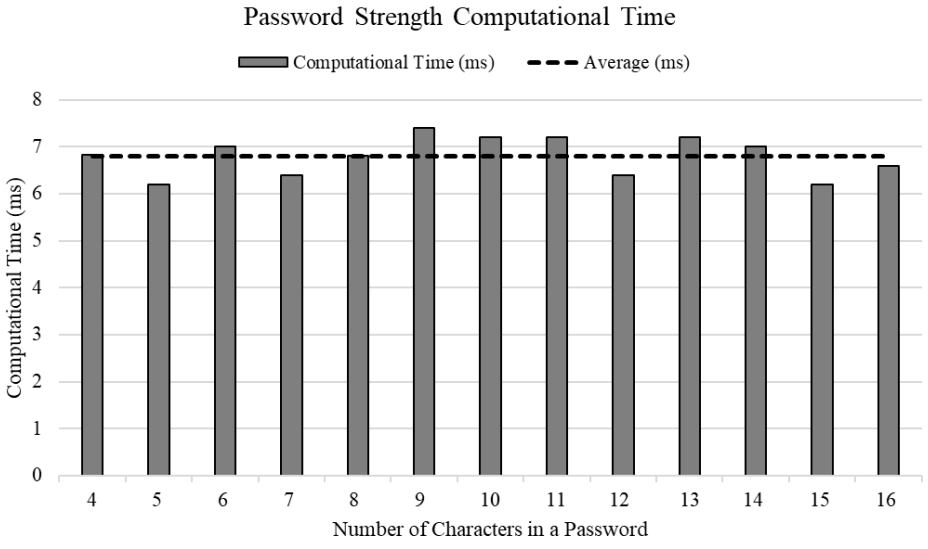


Fig. 8. Password strength computational time

From Figure 8, for four-character passwords, the computation time was approximately 6.83 milliseconds, and the time was 6.20 milliseconds for five-character passwords. It took 7.00 milliseconds and 6.4 milliseconds to compute the strength of six-character and seven-character passwords. For eight-character and nine-character passwords, the times taken to calculate the four strength indicators were 6.80 and 7.40 milliseconds. For longer passwords of the sizes ten characters, eleven characters and twelve characters, the times taken to complete the computation of the four password metrics were 7.20 millisecond, 7.20 milliseconds and 7.40 milliseconds, respectively. Finally, thirteen-character, fourteen-character, fifteen-character and sixteen-character passwords, the times taken to calculate the password strength metrics were 7.20 milliseconds, 7.0 milliseconds, 6.20 milliseconds and 6.6 milliseconds, respectively.

On the whole, the average time to complete the computation for the four password strength indicators was approximately 6.80 milliseconds. It has been found that for humans to feel satisfied with the response time on a computing device, the lag time must be less than 50 to 150 milliseconds [3][11]. This means that the obtained computation time is considered acceptable because humans would not feel any delay while using the application. We think that the fact that the password strength metre application does not require any external processing and the application is self-contained contributes to the short computational time.

5 Conclusion

The study began with an issue of the insecurity of passwords. In other words, it has been well documented that the weakness of the passwords used by a lot of users contributes to many recent cyber attacks. Consequently, it was thought that it would be useful to provide a simple tool for users to inspect whether or not their chosen passwords were adequately strong. A password strength metre application was designed and developed as a result.

The main contribution of the study is how the proposed password strength metre differs from the existing ones, which only provide the information of whether the passwords are strong enough without showing which dimensions are lacking and can be improved. The password strength metre in this research, therefore, applied four main metrics as strength indicators. They consisted of password entropy distribution, probability of the password being cracked, effective password length and password crack time. The four indicators were developed in a graphical form so that they would be intuitive to users. Moreover, a summary of the characteristics of the password and of the four metrics could also be seen in radar charts for a quick glance. In addition, a more complete formula, which now included the upper case character factor, for computing the password entropy distribution was provided.

The performance of the password strength metre was measured to ensure that there would be no delay while the computations were carried out. The average time taken to compute the four indicators was approximately 6.80 milliseconds, which was fast enough for the users not to feel any lag.

Overall, it is felt that the password strength metre can at least provide some idea to how strong or weak a password is. In other words, the four password strength metrics

provide users with information of which dimension or dimensions of their passwords still needs to be improved. This is hoped that users will be able to obtain stronger passwords after checking the strength on the proposed application. Having said that, it is believed that further study, especially on how the password strength metre affects password creation, is required.

6 References

[1] Alani, M.M. (2017). Android Users Privacy Awareness Survey. International Journal of Interactive Mobile Technologies, 11 (3), pp. 130–144. https://doi.org/10.3991/ijim.v11i3.6605

[2] Aljazaery, I., Alrikabi, H. and Aziz, M. (2020). Combination of hiding and encryption for data security. International Journal of Interactive Mobile Technologies, 14 (9), pp. 34–47. https://doi.org/10.3991/ijim.v14i09.14173

[3] Attig, C., Rauh, N., Franke, T. and Krems, J.F. (2017). System Latency Guidelines Then and Now – Is Zero Latency Really Considered Necessary?. Engineering Psychology and Cognitive Ergonomics: Cognition and Design. EPCE 2017. Lecture Notes in Computer Science, Springer, Cham. https://doi.org/10.1007/978-3-319-58475-1_1

[4] Boonkrong, S. (2021). Methods and Threats of Authentication. In: Authentication and Access Control. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6570-3_3

[5] Computer Emergency Response Team (CERT). (1998). IN98.03: Password cracking activity. In: 1998 CERT incident notes. Software Engineering Institute, Carnegie Mellon University.

[6] Fites, P.E. and Kratz, M.P. (1994). Information systems security: a practitioner's reference. Van Nostrand Reinhold Co.

[7] Imperva. (2011). Military password analysis. Available online at https://www.imperva.com/blog/military-password-analysis/. Accessed on 26th February 2021.

[8] Imperva. (2014). Consumer password worst practices. White Paper. The Imperva Application Defense Center (ADC).

[9] Ma, W., Campbell, J., Tran, D. and Kleeman, D. (2010). Password entropy and password quality. 2010 Fourth International Conference on Network and System Security, pp. 583–587. IEEE. https://doi.org/10.1109/NSS.2010.18

[10] Naman, H., Hussien, N., Al-dabag, M. and Alrikabi, H. (2021). Encryption System for Hiding Information Based on Internet of Things. International Journal of Interactive Mobile Technologies, 15 (2), pp. 172–183. https://doi.org/10.3991/ijim.v15i02.19869

[11] Nielsen, J. (1993). Usability Engineering. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[12] NordPass. (2020). Top 200 most common passwords of the year 2020. Available online at https://nordpass.com/most-common-passwords-list/. Accessed on 26th February 2021.

[13] Saita, A. (2005). Password at the breaking point. RSA 2005 Conference, San Francisco, CA, USA.

[14] Shannon, C.E. (2001). A mathematical theory of communication. ACM SIGMOBILE mobile computing and communications review, 5(1), pp. 3–55. https://doi.org/10.1145/584091.584093

[15] Statcounter. (2021). Desktop vs Mobile market share worldwide. Available online at: https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/. Accessed on 26th February 2021.

[16] Taha, M.M., Alhaj, T.A., Moktar, A.E., Salim, A.H. and Abdullah, S.M. (2013). On password strength measurements: Password entropy and password quality. 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), pp. 497–501. IEEE. https://doi.org/10.1109/ICCEEE.2013.6633989

[17] Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L. and Christin, N. (2012). How does your password measure up? The effect of strength meters on password creation. 21st USENIX Security Symposium (USENIX Security 12), pp. 65–80.

7 Authors

Sirapat Boonkrong is a full-time lecturer in the School of Information Technology and DIGITECH at Suranaree University of Technology, Thailand. He received his B.Sc. and Ph.D. in Computer Science from the Department of Computer Science at the University of Bath, UK. His main area of research is authentication and access control as well as cyber security in general. He is currently responsible for teaching both undergraduate and postgraduate students in the field of cyber security.

Arkalerk Kitthimon, Patchara Koksoungnoen and Krissada Jenprakhon are undergraduate students in the School of Information Technology at Suranaree University of Technology, Thailand. They are studying for a Bachelor's degree in Information Science, majoring in enterprise software development. They are currently in their final year and are all having an interest in cyber security.

Article submitted 2021-02-26. Resubmitted 2021-06-09. Final acceptance 2021-06-09. Final version published as submitted by the authors.