International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Password Security: Method and Techniques to Avoid Breaches

Utkarsh Singh[1]

Utkarsh Singh, Feroz Gandhi Institute of Engineering and Technology, Raebareli

---

Abstract - The password security is the very big concern for maintaining the data security whether it is online or offline. The data theft leads to some big disasters. Password can be secured in various forms out of which opti codes are used in the pictorial form which required some special attributes of picture which you see. The normal password is an 8 character string of upper case, lower case a digit and the special character. THE BRUTE FORCE attack is very common than the dictionary and key logger attack because it just requires the certain combinations of the password strings. Research shows that the 81% of data breaches of the companies is due to poor password protection. Managing employee passwords has become flounder these days. The text based password are proactive authentication of the user in various logins and sign in which just a simple string and should be concerned.

Here in this paper we have discussed how to create strong p[passwords and their algorithms beyond this some do's and don't too. Reseaches have founded that more than100 millions passwords are leaked which are founded anchored with LUDS [lower, upper case, digits and symbols

***Key Words*: BRUTE force, password managers, alphanumeric based random passwords, pronounceable based random password, mnemonics phrase based random password.**

1. INTRODUCTION

Password is a gateway if which gets encrypted then your information can collapse easily and sometimes recovery is not available. Apart from password creating, memorizing a password is also important which you can do either in form of opti codes which are the pictorial representation or alpha-numeric text string combinations. The alpha-numeric passwords are pretty easy to recognize. Some examples are:name123, name@123, password, 1a2b3c4d, date of birth, mobile numbers and so on[1].

1.1 Mistake 1

Choosing a weak password like your name, date of birth and mobile number. These are the ways by which you are welcoming the threats by yourself. These weak passwords are common terms or dictionary phrases also.

Solution**:** the easiest way is passphrase which comes from Microsoft security centre. Start with sentence or two, tricky passwords are safer. Remove spaces between words: cybersecurity misspelt the word: cibersecurity add length password by numbers: cybersecurity890use special character as a character: cyber$ecurity.

1.2 Mistake 2

Using the same password in every account, this mistake is very common mistake that the most of the people do, as this gives access to multiple accounts very easily. These password gives more threat than normal password, some major threat areas are billing payment, health systems, business and banking which may lead to you in debt or mortgage.

Solution: use the different password for different websites, with minute changes in it and if you can remember then only use a different password.

1.3 Mistake 3

Accessing public computers or sharing your passwords and exposing it. This is very popular mistake performed by the people at the door even knowing that this can take them to troublesome conditions where it is extremely difficult to that end at the data is accessed.

Solution: avoid the use of public computers or public networks to access your confidential information. If it is necessary, then change the password immediately after using it.

1.4 Mistake 4

Strictly say a big "NO" to save your password in a web browser like Google chrome and Mozilla Firefox. As the web browser access your permissions to store passwords then they store passwords in encrypted form and are publically accessed.

Solution: avoid using password managers and saving the password in web browser because these can also be accessed from browser setting after restoring it so your password will be no longer safe.

2. Password managers

Password managers are these software's which can keep a track of your passwords and passphrases which you use online and offline. These are the services which stores your password and keep reminding you to update it. These are easy and convenient because they store your password at one location. While using the password managers you have to secure your password managers too. A desktop password

manager is a software which you can use to store a password and to make it secure but somehow it can have intuitive responses while changing of your passwords. You can secure your computer on the internet by using biometrics like face recognition, retina scan and fingerprints and many more. In the real world there are endless loopholes over the internet which cannot be fixed at all. Thus, the password managers can be used but within the constrained limits. No doubt they are useful but storing password will always put you in the risk not only inside but outside internet domains. So one must be very cautious while using the password mangers.[2].

The neutralization of the password is very critical these days, because passwords patterns are same up to few repetitions. So one must avoid the repetitions of password in various account over the internet, because the alphanumeric patterns are easily recognizable as compared to the passwords which are having the alpha numeric along with special characters. And specials characters are difficult to predict.

It is very common problem of the people of that if they supposed to have a complex rules over they password security and maintenance then they avoid the information policy just to make password simpler rather than secure.

3. **Unsecure behavior changes and research gap:**

To enhance the security of the password, it is the fundamental responsibility of the system administrators, organizations and user to follow the standard criteria of password given by (NIST) which comprises of at least 8 characters including one uppercase, one lowercase and one special characters.

Although the password like Utkarsh@1 ,#diamond#, DAVId@1 are considered as the weak password because they follow the linear transition pattern which means just one uppercase, one lowercase and one special character which is the concern of the loopholes where theft are easily possible. Text based password involve trade-off between system memorability, security and authenticity

4. Alpha numeric and random password

It is the simplest random password generation technique where the charters are chosen randomly from the given set of characters which are upper case (26), lowercase (26), digits (10) and password length is of 6 characters then the cardinality of password is:

26+26+10=62…….. (1)

Now there are 62 choices for each 6 positions. Given in equation (1)

Now total password space as alphanumeric character is given as:

62*62*62*62*62*62 = 62^6 = 5.68*10*10 = 2^35.7

The cardinality is 2^35.7(approx. say p). Any password chosen from p has the cardinality of 35.7 bits. This entropy metric is used to determine the strength of the password. And thus alpha numeric password has the highest entropy among all three methods which are harder to remember.

5. Pronounceable random password.

Pronunciation random password generation technique makes the use of specific language pronunciation and generate the random string. The main objective behind this is it uses the speech recognition to resemble the password and for the user to remember it[3]. These technique use the syllables of the language to meet the speech recognition frequencies and then to generate the password[4]. The PRONUNCE3 generator define 5 vowels (a, e, i, o, u) and 22 consonants which are (b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z). It has an entropy of 30.8 bits which is less than alpha numeric passwords having better memorability.

6. Mnemonics phrase based random passwords

Some systems suggest users to create mnemonic phrase-based passwords. Kuo et al, defines mnemonic phrase-based password is one, where a user chooses a memorable phrase and uses at least one character (often first character) to represent each word in the phrase. Ideally, your password should contain a mixture of lowercase and uppercase letters, digits and special symbols. The mnemonic phrase-based passwords appear hard to guess than regular passwords. The security of mnemonic phrase password is better because they do not appear in any dictionary and usually contain a good mixture of letters, digits and special symbols. Kuo et al, build a dictionary of 400,000 mnemonic passwords using mnemonic phrase found commonly on internet. They cracked 4% of mnemonic passwords, in comparison, a standard dictionary with 1.2 million entries cracked 11% of cracked passwords. They show it is possible to create.[5]

7. Random password generation system

This can be divided into rtwo modules

7.1. Random password generation

In the random password generation method , any word is chosen randomly from a set of characters listed in the standard dictionary and also the random numbers and special characters too, in which minimum 3 combination set is required which can be used further as for proactive analysis.

7.2. Proactive analysis

Proactive analysis is a test which are performed against the attacker's approach towards the password, if these are found positive then the passwords are discarded. The proactive

test is used to perform intuition based password. If three consecutive letters are found either in lower or uppercase then password is denied. The main objective is that the sequence is not same, either of letters, digits or special characters. It confirms that password doesn't contain easily predictable pattern and if this happens then the password is dropped immediately. The whole ecosystem is design in c language

8. Password entropy and BRUTE force approach:

The brute force approach is performed by the attacker to check every possible combination. In the brute force approach the way is that there are 26 lowercase characters, 26 uppercase characters, 10 digits and special symbols so the total cardinality is of 70 characters.

26+26+10+8=70

Let us suppose the password consist of 8 character set. According to brute force approach there are 70 possibilities for each character so the total possibilities are:

70 × 70 × 70 × 70 × 70 × 70 × 70 × 70 = 70^8 = 5.76 × 10^14 + 2^49.03.

Here generated password has the entropy of 49.03 bits which is the highest of all the above methods discussed. In general the higher the entropy, the more difficult it becomes to guess and to crack the password. The table presents theoretical brute force online and offline attacks simulation against the password generated using proposed technique.

Attack scenario	Expected time to crack
Online attack 1000guesses/sec	1.85 hundred centuries
Offline attack 100 million guesses per second	66.8 days

There is one popular method called game changer password system.

The idea behind the GCPS is that a number of different games are presented on the screen, similar to viewing a screen full of movie options in Netflix, allowing users to select the game first and then to enter his or her password in the game selected. For example, a user first selects Chess, then puts a black king (BK) on position a7, a black rook (BR) on e6, white knight (WN) on c4 and white pawn (WP) on g3.. Such a combination can be transcribed as a textual password, e.g. 'BKa7BRe6WNc4WPg3'.

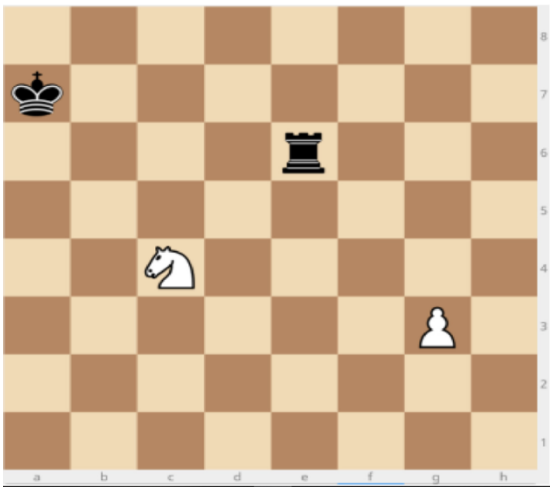

Fig 1 game changer password method

The main innovative behind this proposition is that it is based on mnemonics and graphical representations. Which are easy to remember, access and easy to control.

motivating factor for remembering passwords; the effect is shown in a rather high Next, users find the GCPS system fun to use, which is a very important recall rate (>75%). All these elements make the GCPS system a very promising one with a high potential of usability and acceptability among users.

The intruders can use brute force attacks to calculate all possible hashes for a given input set and compare the calculated one with the stored ones. To prevent brute force attacks, passwords need to be long to make the pool of possible combinations prohibitively large and hence trying all possible combinations takes too long, longer than the useful lifetime of the information protected by the password. The number of possible combinations depends on the character set – out of how many different characters one chooses components of the passwords, and the number of characters in the password themselves. Very importantly, characters need to be selected randomly from the character set.

The total number of combinations (N) in a textual password is expressed by the following formula:N=CL where C denotes the character set size and L is the number of characters in the password.

Typically, the character set consists of lower, uppercase letters (a..z, A..Z), digits(0..9) and special characters (e.g. "!@#$%^&). There are 52 English letters (2 × 26) plus ten 10 digits (0..9) plus special symbols (for simplicity, suppose we have 13 of those), totalling to 75. For one-character password, there are 75 different combinations. For up to two-character password, the password could be composed of a single character, or a combination of two characters, raising the number to $75^1 + 75^2$=5700 different combinations. Similarly, for up to eight-character password,

there are $75^1 + 75^2 + 75^3 + \ldots + 75^8 = 75^9 - 1$ = 75,084,686,279,296,874 combinations (75 quadrillion or 75,084 trillion or 7.5E + 16). Eight character passwords are minimum recommended nowadays[6]

As mentioned, an intruder can mount a brute force attack and can try to find a plaintext password that corresponds to the stored hash value. They typically do so by using general purpose graphical processing units (GPUs) optimized for cracking; the costs of such a GPU is in range of US$1000. The speeds reported at the time Game Changer Password System was published reached up to 6877 million passwords tries per second for MD5 hash function[7]; recently reported speeds reached 38,500 million passwords per second on a single GPU and over 307,000 million passwords on a GPU array[8] and are expected to double every one to two years[9] due to Moore's law[10] alone. In this paper we use speeds as they were reported at the time of publication of the original paper, i.e. speeds reported by quietal[11].

Thus, an adversary can use $1000 worth of equipment to search all the possible combinations. With 75,084,686,279,296,874 different passwords and speed of 6877,000,000 passwords per second, one needs t=75,084,686,279,296,874pwd.comb.6,877,000,000pwd.com b.second=10,918,232.7sec.=181,970,5min.=3,032.84hourst= 126,37days.

3. CONCLUSIONS

As above all the three methods we have discussed . The password strength is mentioned below in descending order:

Proactive analysis

2. Alphanumeric random password

3. Mnemonic based random password.

There GCPS is very effective method as the number of the error tricking is reduced and guessing becomes more complicated. As the game changer method is based on mnemonics and the graphical

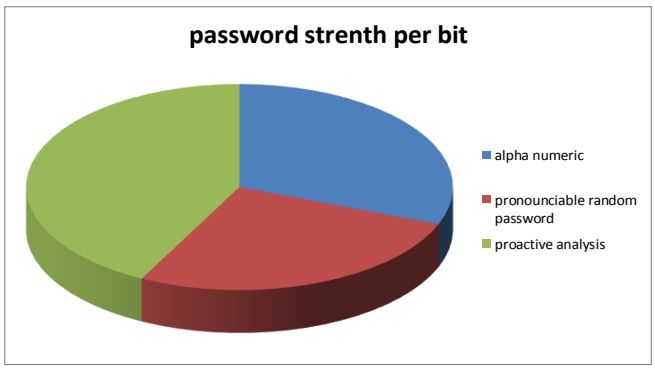

Fig 2 pie graph distribution

representations. In this method we have taken the example of chess. Some of the alternatives are Chinese checkers, pokers and playing cards used for the designing of the strategy. This is very latest method used nowadays for critical password designing.

The password protection and its security is need of the concern which can cause a threat at any level i.e. individual or public. We have discussed various methodology of how to secure a passwords like alphanumeric random password, pronounceable based random password, mnemonic phrase based random password and most the most important the brute force attack. Apart from this the password mangers are also useful to us but only up to some extent. One must avoid simple and easy password and restrict oneself towards password managers. The random password generation system and proactive approaches meet the difficulty criteria of the password to avoid intuitions by the hacker and number of attempts will be longer. Some simple mistakes along with their solutions are also discussed above. The opti codes are a bit easy way to create your password on the basis of the pictures and easy to remember. The game changer password system is very trending method used in complicated designing of the password. Easy and intresting to remember

ACKNOWLEDGEMENT

This paper and research work behind it would not have been possible without my mentor shraddha srivastava . She had guided form the very beginning to till the final drafting of the paper. Without him this would not be possible. I would also thank my friend shekhar saxena who has shared his valuable knowledge with me to make this more impactful.

REFERENCES

[1] Burr WE, Dodson DF, Polk WT. Electronic authentication guideline. NIST Special Publication 800-63 version 1.0.2, 1992.

[2] McDowell, Mindi et al. “Choosing and Protecting Passwords,” US-CERT Cyber Security Tip ST04-002, 2009. Available from: http://www.us-cert.gov/cas/tips/ST04-002.html (accessed March 1,2012).

[3] . Komanduri S, Shay R, Kelley PG, Mazurek ML, Bauer L, Christin N, et al. Of passwords and people: Measuring the effect of password composition policies. CHI’11 Proc. of annual conf. on Human factors in computing systems, 2011, p. 2595-10.

[4] Ganesan R, Davies C. A new attack on random pronounceable password generators. In Proceeding 17th NIST-NCSC National

[5] . Kuo C, Romanosky S, Cranor LF. Human selection of mnemonic phrase-based passwords. Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006 p. 67-12

[6] P.A. Grassi, J.L. Fenton, E.M. Newton, R.A. Perlner, A.R. Regenscheid, W.E. Burr, J.P. Richer, N.B. Lefkovitz, J.M. Danker, Y.-Y. Choong, K.K. Greene, M.F. Theofanos**NIST Special Publication 800-63B Digital Identity Guidelines. Authentication and Lifecycle Management**

[7] W. Qiu, Z. Gong, Y. Guo, B. Liu, X. Tang, Y. Yuan**GPU-based high performance password recovery technique for Hash functions.** J. Info. Sci. Eng., 32 (1) (2016), pp. 97-112

[8] Gosney, J.M., 2018. 8x Nvidia GTX 1080 Ti Hashcat Benchmarks. https://gist.github.com/epixoip/ace60d09981be09544fdd35005051505/. (Archived by WebCite® at http://www.webcitation.org/70yRle0jv), GitHub Gist.

[9] B. Brumen, V. Taneski**Moore's curse on textual passwords,**Information and communication technology, electronics and microelectronics (MIPRO), 2015 38th International Convention on., Opatija, Croatia, IEEE (2015), pp. 1360-1365

[10] . G.E. Moore**Cramming more components onto integrated circuits**Electronics, 38 (8) (1965), pp. 114-117

[11] W. Qiu, Z. Gong, Y. Guo, B. Liu, X. Tang, Y. Yuan**GPU-based high performance password recovery technique for Hash functions.**

BIOGRAPHIES

Myself utkarsh singh, pursuing bachelors of technology in electronics and communication engineering from feroz Gandhi institute of enginnering and technology. My fields of intrest are robotics ,machine learning and cyber security.