International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 17 April 2019.

Link : http://www.ijiemr.org

Title:- Resolving the Analysis of Minimum Character Bounds of Password Length.

Volume 08, Issue 04, Pages: 198 - 202.

Paper Authors

ANKAM BRAHMA DURGABHAVANI, M.S.VENUGOPALA RAO.

Department of MCA, SKBR PG College.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Approvals We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

RESOLVING THE ANALYSIS OF MINIMUM CHARACTER BOUNDS OF PASSWORD LENGTH

[1] ANKAM BRAHMA DURGABHAVANI, [2] M.S.VENUGOPALA RAO
[1]PG Scholar Department of MCA, SKBR PG College, Amalapuram
[2]Assistant Professor, Department of MCA, SKBR PG College, Amalapuram

ABSTRACT: Information Security has become one of the most pressing issues facing businesses in today's competitive e-commerce that is driven by online transactions. User authentication serves as the first line of defense against security breaches, which predominantly uses passwords. There have been growing controversies as per the minimum length of a password required to make the password withstand guessing and hacking attacks. For example, a password can receive a rating as "strong" with only six characters on Face book but not on Gmail where it must have at least eight characters. There is, therefore, the urgent need to address these minimum password length controversies in view of its negative consequences on the security of the end-users' web accounts. In this paper, a mathematical model for determining minimum password length was developed. A combination of entropy formula and the bit strength threshold were used in developing the mathematical model. This was tested and a table of minimum password length needed for different character sets was generated. It is hoped that software developers as well as web account owners will find the table useful.

KEY WORDS: Bit Strength Threshold, Brute-Force Attacks, Entropy Model, Minimum Password Length, Randomness.

I.INTRODUCTION

A password is a character or sequence of characters used to determine that a device user requesting access to a system is really that particular user [1]. The main authentication mechanism employed in millions of computer installations and websites is passwords [2]. According to [3] and [4], password will continue to maintain its predominance as a form of authentication even in the face of new developments in authentication systems such as biometric. This seems to remain unchanged in the foreseeable future [3, 5, 6]. This is so because of its easiness, cost effectiveness, simplicity and familiarity to all users [5, 7]. In addition, it provides adequate security to the end-users' online accounts, although there are some concerns about weak passwords which can lead to weak security [7]. However, findings from separate studies conducted by [8] and [9] showed that the weakness is not within the password authentication itself, but the choice of the passwords by the end-users. Since passwords are the first line of defense in web accounts, there is the need to educate end-users on how to create good passwords.

Towards this end, many systems administrators as well as software developers provide advice to their users on how to construct a good password. This advice comes in form of password policies, feedback mechanism, among others. One of these password policies is the minimum password length. However, there have been growing controversies on the

minimum password length that can give the needed protection of end-users' online accounts. These conflicting minimum password lengths bring confusion to the end-users with far reaching negative consequences on the security of the end-users' web accounts. This calls for urgent scientific solution. To the best of our knowledge, this is the first scientific attempt at resolving the minimum password length controversy The remainder of this paper is organized into five sections namely: brief history of password development, related work, methodology, implementation and results. Finally, recommendations and conclusion were discussed.

II. BACKGROUND

Password, which was formerly called watchword in the olden days, has been used since ancient times, especially in the Roman military. In those days, a sentry, that is, a soldier stationed at a place, especially at a gate to prevent the passage of unauthorized persons, would challenge those wishing to enter an area or approaching it to supply a watchword and would only allow such a person or group of persons to pass if they knew the watchword [10]. In modern times, usernames and passwords whose implementation were pioneered by Unix system are commonly used by people during a login process that controls access to protected devices. It was initially implemented on a simple text password system whereby account passwords were stored verbatim in a file [11].

Even though the file was protected from casual reading and writing, a privileged or skillful user could gain access to the file, thereby compromising all end-users' passwords. As a result of this drawback, [12] proposed securing each password with encryption before storing them during account creation. During login at a later time, the system would encrypt the entered password, compare the result to the stored encrypted password for that user, and grant access if they matched.

Otherwise, access is denied. The encryption, in this regards added a layer of security to the stored passwords. However, if the encryption key is compromised or broken, all passwords would also be compromised. To remedy this vulnerability, [13] and [14] proposed passing the entered password through a one-way hashing function, instead of using encryption. Thus, an attacker who compromises a file of hashed passwords will not be able to obtain the plaintext passwords without performing a password guessing attack, whereby the attacker chooses and hashes a candidate password, and compares the result to each of the hashes contained in the password file.

Any hash that matches the hash in the password file is the actual password for the corresponding account From its introduction by Unix system, the study of [5] considered the four decades of research work on passwords and then classified passwords into two generations, first and second generation. The first generation considered mainly two attributes, that is, security and usability, while the second generation considered three attributes, that is, security, usability and deploys ability of the password the trade-off between them.

III. RELATED WORK

End-users of today's computer systems manage a large number of online accounts that require passwords. Each authentication system has

different rules or policies for which passwords are acceptable and which passwords are not. Some passwords must be eight characters; some must be over eight characters; some must contain multiple classes of characters; some cannot accept certain characters [15]. An analysis of minimum and maximum password lengths of twenty-three selected websites that have very high global ranking in terms of popularity was carried out by [16].

The result of the work, which is presented in table showed that there is no uniformity in the web community about the length of passwords. the minimum password length ranges from one to eight. This clearly showed that there is no consistency and common agreement on the minimum and maximum password length required for creating a password that can give basic protection. Further findings by [16] revealed that all the websites decide their minimum and maximum characters to be allowed in the password field according to their own wish. In other words, there is no scientific approach for determining minimum password length among the websites studied. In a related work, [2] conducted a study of password policies of five different websites. The result of this study which is presented in table 2, showed a minimum password length of six to eight characters

table. 1: minimum password length

Name	Minimum Password Length
Gmail	8 characters minimum length
You Tube	8 characters minimum length
Facebook	6 characters minimum length
MS Live	8 characters minimum length

Again, results from table 1 showed non-uniformity in the minimum password length. Furthermore, there is no scientific approach used in arriving at this minimum password length. Closely related to the work of but with a wider coverage was the work of that performed a study of how passwords are handled in one hundred and fifty different websites. This study was a large collection of password policies and practices of one hundred and fifty websites. This result is consistent with the finding of [19], though with a smaller sample. The findings from the two studies showed that there is no uniformity in minimum password length. In a similar work, [20] presented a detailed structural.

IV. PROPOSED SYSTEM

The goal of this work is to develop a model that will take care of both machine-generated passwords and human-generated passwords. To achieve this, we made use of the recommended bit strength threshold of 80-bit. Thus, the model for computing the minimum password length is given by equation (1):

$$Len=1/2((80*Log(2))/(Log(C))+80*1.1*Log(2)) /(Log(C))) \quad (1)$$ and

$$Len=1/2\{(Log(2)/Log(C))*(168)\} \quad (2)$$

where: Len is the minimum password length; 80 is the bit strength threshold, that is, the minimum entropy needed to withstand brute force/ guessing attacks according to, C is the character set. 1.1 is the penalty introduced to accommodate the randomness lost if it is a human-generated password. Equation (2) is the developed Model.

Algorithm of the proposed Model

The Model algorithm is presented below.

Let C be each character set

Let C1..C11 be numeric, lowercase..

num+lowcase+uppcase+special characters

Select Choice (C1…C11)

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

```
If (choice = C1) then
C=C1
CALL MODEL
endif
If (choice = C2) then
C=C2
CALL MODEL
endif
If (choice = C3) then
C=C3
CALL MODEL
endif
If (choice = C4) then
C=C4
CALL MODEL
endif
If (choice = C5) then
C=C5
CALL MODEL
endif
If (choice = C6) then
C=C6
CALL MODEL
endif
If (choice = C7) then
C=C7
CALL MODEL
endif
If (choice = C8) then
C=C8
CALL MODEL
endif
If (choice = C9) then
C=C9

CALL MODEL
endif
If (choice = C10) then
C=C10
CALL MODEL
endif
If (choice = C11) then
C=C11
CALL MODEL
endif
END
PROCEDURE MODEL
Len=1/2((Log(2)/Log(C))*(168))
OUTPUT Len
ENDPROC
```

V. RESULTS

Character Set	Minimum Password Length
Numeric only	25
Lowercase only	18
Uppercase only	18
Symbols (Special Characters) only	17
Numeric+Lowercase	16
Numeric+Uppercase	16
Numeric+Symbols	15
Lowercase+Uppercase	15
Numeric+Lowercase+ Uppercase	14
Numeric+Lowercase+ Symbols	14
Numeric+Lowercase+ Uppercase+Symbols	13

Fig. 1: Summary of Minimum Password Length for various Character Pools.

VI. CONCLUSION

This work has tried to put an end to the controversies surrounding minimum password length by using a scientific method in arriving at the minimum password length of different character sets. Developers are encouraged to make reference when developing password authentication scheme.

VII. REFERENCES

[1]. Agholor, S., Sodiya, A. S., Akinwale, A. T. Adeniran, O. J., Aborisade, D. O.: A Preferential Analysis of Existing Password Managers from End-Users' View Point. In:

International Journal of Cyber-Security and Digital Forensics, vol. 5, no. 4, pp. 187-196 (201)

[2]. Agholor, S., Sodiya, A. S.: An Assessment of Feedback Mechanism of some Selected Websites towards Improved End-Users' Password. In: Proc. Of 11th International Conference of the Nigeria Computer Society, Iloko-Ijesa, pp. 44-49, (2013).

[3]. Andreas, S.: Influencing User Password Choice Through Peer Pressure. An Unpubblished M.Sc. thesis submitted to the Department of Electrical and Computer Engineering, The University of British Columbia, pp. 1-120, (2011).

[4]. Bonneau, J., Herley, C., Van Oorschot, P. C.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: Proc. of IEEE Symposium on Securityn and Privacy, pp. 553-567, (2012).

[5]. Gayathiri, C.: Text Password Survey: Transition from First Generation to Second Generation, retrieved on 13/10/2017 from www.blogs.ubc.ca/.../ (2013).

[6]. Herley, C., Van Oorschot, P.: A Research Agenda Acknowledging the Persistence of Passwords. In: IEEE Security & Privacy Magazine, vol. 10, no. 1, pp. 28-36, (2012).

[7]. Forget, A.: A World with Many Authentication Schemes. An Unpublished Ph.D. thesis submitted to the Faculty of Graduate and Postdoctoral Affairs, School of Computer Science, Carleton University, Ottawa, Ontario, Canada, pp. 1-244, (2012).

[8]. Gaw, S., Felten, E. W.: Password Management Strategies for Online Accounts. In: Proc. of the 4th SOUPS, Pittsburgh, PA, USA, pp. 1-12, (2006).

[9]. Saheen, G. A., Jaber, A. A., Hamami, A. A.: The Effect of Weight Factors Characters on Password Selection. In: World of Computer Science and Information Journal, vol. 3, no. 6, pp. 110-113, (2013)

[1]0. Wikipedia.: Password defined, retrieved on 28/07/2017 from www.wikipedia.org/wiki/password (2017).

[1]1. Morris, R., Thompson, K.: Password Security: A case History. In: communications of the ACM, vol. 22, no.11, pp. 594-597, (1979).

[12]. Wilkes, A.: Time-Sharing Computer Systems. In: American Elsevier, pp. 1-8, (1968).