Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 279–282 DOI: 10.15439/2017R67
ACSIS, Vol. 10 ISSN 2300-5963

Password Security Mechanisms: Comparitive Study

Vasundhara R. Pagar
M.E Second Year,
Department of Information Technology,
PCCOE,
Pune, India

Rohini G. Pise
Assistant Professor,
Department of Information Technology,
PCCOE,
Pune, India

***Abstract*—Nowadays online communication is increasing rapidly, password is provided as a key for communication henceforth there is a strong need to authenticate the online communication. But currently security breach occurs by stealing the password files through various ways of cyber attacks. Different technologies are available to safeguard password. The purpose of this paper is to evaluate various techniques for protection of password like graphical password, text password enhanced by Honeyword, Jumbling and salting approach.**

Keywords—Honeywords; Jumbling; Salting; Capcha; Hashing

I. Introduction

In today's era large numbers of people are getting connected over Internet. Very less amount of Security provided over internet, to overcome this problem, a scheme called authentication is used. This authentication is a strong method for the communication over Internet. On account of protecting the user's delicate information on online services password is the vital identification key. User's identification key is used various places like Banking sector, E-Commerce websites, Online transactions etc. During authorization process all personal details like Email-id, Bank account number; Credit card information of individual user is registered by respective websites. All these user's details are stored in their database in conjunction with security. Password is a protective tool used to guard the crucial information of particular user to avoid the unauthorized access by third person. If passwords are stolen by attacker or hacker without the knowledge of genuine user then critical information of user may be used illegally. Misuse of user's personal details may suffer from huge loss. Some factors are interrelated to user authentication like pin number or password that user already knows, credit card that user posses and biometric authentication, it means human characteristics are used as password [7].Solemnly, user selects the simple password such as birth date, name of beloved thing etc so that it is easy to remember. But it leads to easy cracking of password by attacker using numerous attack like brute force attack, dictionary attack etc. Therefore it is essential to select effective password which should not be guessable. Though there are different authentication mechanisms provided to secure online services hacker is successful in fetching the information of an individual. This paper briefs about the various mechanisms for protecting passwords and comparative analysis is performed based on the effect of different cyber attacks after using the respective technique.

II. Existing Techniques and Algorithms

Hacker is very successful in theft of password file and cracking passwords from file. Weak passwords, simple passwords are also one of the reasons for password cracking. Several popular sites like LinkedIn, Yahoo, and eHarmony have been suffered from high publicity password leaks. SHA-1 algorithm without a salt is used by LinkedIn passwords and MD5 hashes without salt is used by eHarmony passwords. Among all available methods of hashing SHA-2 algorithm is cryptographically strong enough [5].

III. Honeywords For Enhancing Security

Honeywords are used as an alternate approach to store the passwords in file. Honeywords are nothing but decoy passwords or bogus password. For generation of Honeywords Chaffing-With-Tweaking algorithm is used.

A. Chaffing-With-Tweaking Algorithm

In this method, input to generator algorithm is original password and each character of original password is substituted by another character which is selected randomly. During substitution if original character is digit then new substitution is by digit only and it is applicable for letters and special characters also.[1][6].

B. System Overview

There are different stages from user registration, user login to behaviour analysis of user. In Registration phase user enters passwords and system generates the Honeywords. Hash of password is generated .Key is also provided to user for file encryption and decryption of uploaded file. In Login phase if password matches then system allows user to access the system If Password does not match, Hacker is trying to access the system then alert is given to the actual user if hacker uses one of the Honeywords. If Hacker uses the combination for password then access is given to the hacker but with the decoy or fake file. For behaviour tracking user login, the system tracks user operations and track IP Address, Mac address and data size of resources downloaded by each user per session [1]

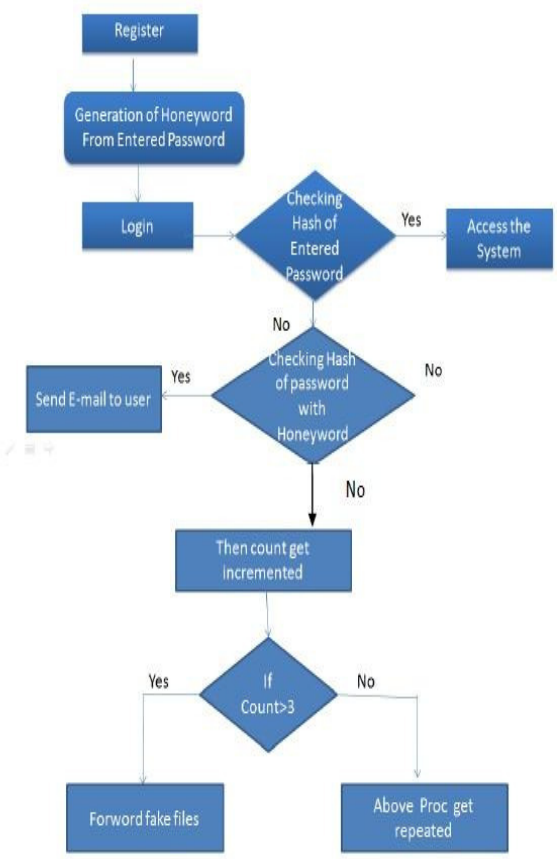


Fig. 1. System Overview

IV. JUMBLING- SALTING FOR PASSWORD ENCRYPTION

There are some predefined hashing algorithms available today like SHA, MD5 that do not offer complete security to the passwords. Simplest way to crack a hash is first guess the password and try hash for every guess. If the hashes are matched, password is easily obtained which is the basic principle of dictionary attack [8].

In this approach to protect the password, Jumbling and Salting technique is developed. This algorithm has majorly two processes namely; jumbling and salting. Jumbling process has three sub process addition, selection and reverse. In salting salt that is random data is selected which increases the length of plain text by adding salt to original string of password. After Jumbling and Salting AES algorithm is applied for encryption of passwords [2].

A. *Jumbling Process*

Process array is the array of the original password. Jumbling process has three sub processes.

a) Addition Sub-block: It generates the random value '1' by using existing mathematical function Random() and updates process array size.

b) Selection Sub-block: By using existing mathematical function Random () for particular password the character set is selected which is different from every password access. Random () function is used because character array size is large and characters from this set is selected.

c) Reverse Sub-block: Based on some predefined condition it reverses the entire process array. The predefined condition is depend on value of 1 if it is odd or even.If it is even the process array is reversed else it is kept as it is.

B. *Salting Block*

Salt is random string which is appended along with jumbled version of password. Salt is nothing but the user's sign-up timestamp value .To make the password more complex to make difficult for the attacker to crack it ,salt is added.

C. *AES*

Predefined encryption and decryption algorithm of AES is used.

V. AN IMPROVED HASHING USING SALTING AND DIFFERENTIAL MASKING

By applying salting techniques to password more security is provided. After appending salt to original password hash value of password is calculated .After hashing differential masking process is applied to generate crash list of real password [3].

a) Differential Masking: In differential masking fake passwords for every user's account is inserted. As a result when an attacker is successful in stealing password file but he is unable to guess the correct password because of many passwords[3].The real password is saved with different mask words to lure the attacker. Here, Differential masking is a result of hashing which generates different permutations of real password. The main purpose of differential masking is to hide the real password with different fake passwords[3].

b) Hashing algorithm: In Hashing process password string is converted into the binary string and i^{th} position character from both side of binary string is interchanged. After interchanging all characters string is reversed by r characters. New string is formed by combination of r no of zero's and one's and XOR is performed with password binary string. After XOR binary string is converted into the hexadecimal string.

c) Salting algorithm: Salting is process of appending the random data to original password. In this process salt is added

to both side of password.Algorithm to generate the salt is as follows

Salting (s)

i. L = length (s)

ii. N = l/8

iii. Now, create a binary string formed by nth bits from left side.

iv. Now, prepend the first four bits to the left of s and last four bits to the right of s[3].

VI. Graphical Password Authentication Scheme(Captcha)

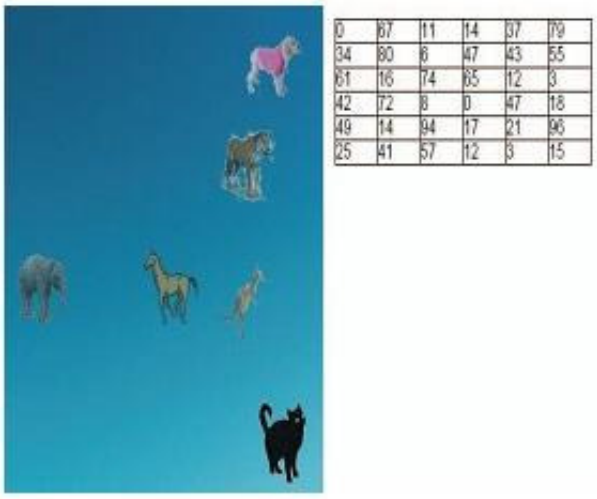
To minimise human guessing attack graphical password is used. It is acronym as CaRP. Image is used as passwords key[4]. Four different schemes are implemented in this approach.

a) Click Text: In this scheme capital letters and special characters are selected and they are randomly arranged in CaRP images which is generated by Captcha engine. To avoid the confusion between same character like 6,9 and o,0 that are kept single. Thus total 40 characters are contained in the password set.To provide password user clicks on any alphabets or numbers in CaRP image. At the time of log-in sequence of clicking the alphabet is very important because server checks same sequence at the time of authentication[4].

b) Animal Grid: User provides password which consist of animal names from the set of 6 animal figures. Each set consists of diverse figures of same animal. One animal figure is selected at random from each set for password formation. Animal figures dataset which has many smaller animal figures.Along with the animal set 6×6 number grid is also provided for password creation. Number grid contains 1-100 numbers, user clicks on number to generate the password. For example password selected is 'cat25'[4].

c) TextPoints4CR: For the formation of password single character of large sized figure is selected and points of same figure are choose by clicking on it at different location. As font size of figure increases, it gives more options for deciding click points[4].

Fig. 2. *ClickText Figure*



0	67	11	14	37	79
34	80	6	47	43	55
61	16	74	65	12	3
42	72	8	0	47	18
49	14	94	17	21	96
25	41	57	12	3	15

Fig. 3. *AnimalGrid Figure*

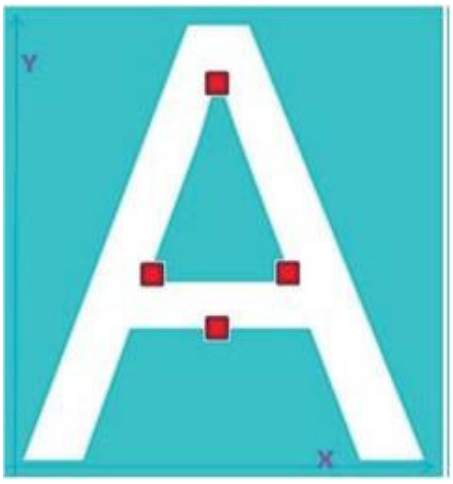


Fig. 4. *Single character Figure*

d) Shuffle Text: This scheme is same like ClickText scheme only difference is user can enter the password in any order like shuffled text etc.

IV. COMPARISON ANALYSIS

TABLE I. COMPARITIVE ANALYSIS

Mechanism/Algorithms	Pros	Cons
Honeywords For Enhancing Security	Removes Brute-force attack to some extent	-Storage cost is major overhead - Only designed to withstand off-line attacks
Jumbling-Salting for Password Encryption	Difficult to crack the encrypted password due to involvement of different randomization processes.	Due to different randomization processes The Encryption time and decryption is more than AES and DES algorithm
An Improved Hashing Using Salting and differential Masking	-Less time complexity -minimizing the DoS vulnerabilities - Brute-force attack is not possible because of High complicated Hashing	-Generation of false alarm by attacker may expose password file.
Graphical Password Authentication Scheme	Effective solutions as far as password security	Very sensitive towards Key Logger Attack

CONCLUSION

The most universally used method for authenticating users to access computer systems and online services is password. Passwords are recurrently targeted by attackers to break into systems. Therefore password security is very important to avoid the cyber crime. Choosing secure password is also very crucial in today's life. Main focus of many organizations is strengthening password security. Various authentications Schemes are available.

By protecting password strongly,vulnerability activities can be avoided which will help to individual from any kind of loss in online system.This analysis makes knowledge about several password encryption techniques which are required to provide password security in online environment as well as in organization

REFERENCES

[1] Manisha Jagannath Bhole, " Honeywords: A New Approach For Enhancing Security," International Research Journal of Engineering and Technology (IRJET) , Volume: 02 Issue: 08 | Nov-2015J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Prathamesh P. Churi, Vaishali Ghate, Kranti Ghag "Jumbling- Salting: An Improvised Approach for Password Encryption"; International Conference on Science and Technology 2015, RMUTT.

[3] Seema Kharod, Nidhi Sharma, Alok Sharma ,"An Improved Hashing Based Password Security Scheme Using Salting and Differential Masking", 978-1-4673-7231-2/15/$31.00 ©2015 IEEE.

[4] Vikas K. Kolekar, Milindkumar B. Vaidya," Click and Session Based—Captcha as Graphic Password Authentication Schemes for Smart Phone and Web" 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015

[5] A. Juels and R. L. Rivest, "Honeywords: Making Passwordcracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 145–160.[Online].Available: http://doi.acm.org/10.1145/2508859.2516671.

[6] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords", IEEE Transactions On Dependable And Secure Computing, Vol. 13, No. 2, March/April 2016

[7] Nilesh Chakraborty, Samrat Mondal,"Towards Improving Storage Cost and Security Features of Honeyword Based Approaches", 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

[8] Prathamesh P. Churi, Medha Kalekar, Bhavin Save "JSH Algorithm: A Password Encryption Technique using Jumbling-Salting-Hashing"; International Journal of Computer Applications(0975 – 8887) Volume 92 – No.2, April 2014