Provide Security in Social Networking Sites using Honeyword based Approach

Bhosale Santosh[1] Gholap Gaurav[2] Kamble Vicky[3] Kokade Rahul[4]

[1,2,3,4]Department of Computer Engineering

[1,2,3,4]Government College of Engineering and Research, Awasari (KD), Pune, Maharashtra, India

Abstract— From the recent survey, it has proven that the passwords are not secured from the cyber attackers. Using only hash password is not enough to keep cyber attackers from password file cracking. And so, there is a need for more secure and reliable approach which is honeyword i.e. fake passwords which are used to deal with different cyber-attacks and to prevent password file disclosure. If an attacker steals the hashed password file, then it becomes very easier for an attacker to login into the account through authenticated way. We need to understand that once a password file is stolen then there is no mechanism that can detect the attacker from hacking the account. And to do so attacker may use variety of attacks to recover the hashed password file, some of them are brute force attack, rainbow table attack, dictionary attack etc. An auxiliary service which is known as honey checker is a secure server that stores only the index of the real passwords along with the index of honeywords for each of the user whenever there is a use of honeyword is detected it immediately triggers the alarm and notify the administrator. In this research paper, we will discuss one of the honeyword generation method hybrid model which is combination of chaffing with tweaking and password model and suggest some improvement from the previous methods along with improved security and easy implementation, we will also address the drawbacks of previous approach and overcome almost every drawback.

Key words: Honeywords, login, password cracking, authentication

I. Introduction

In the authentication process password is most important asset against cyber attackers. Natural tendency of user to select a password related to their information such as birthdate, pet name, their ideals, phone numbers etc. that can be easily remember. Due to the weak nature of passwords it becomes very easy for an adversary to crack the password, most of the times these passwords can be found in precomputed dictionary such as rainbow table which is used for password cracking. Using only hash function without salt value on the passwords is not safe because it can be easily recovered in plain text. An adversary may use any means necessary to get the password which often includes attacks like brute force, rainbow table, dictionary attack etc.

So we need a strong mechanism in order to strengthen the password which is easy to compute but difficult to invert this is where Honeyword comes into the picture

Honeywords are the decoy passwords they play major role against cyber-attacks. These passwords placed in the same password file with original passwords to deceive the attackers during the authentication process.

II. Literature Survey

Users often use same password for multiple highly important account because it is easy to remember and this makes passwords extremely weak either being too short containing only letters or digits or combination of both giving advantage to adversary. Such kind of passwords highly vulnerable as they can be easily found in dictionaries or in the list of names, sometimes computer user suffers from password overload .so there is need to educate to assist when choosing password for highly important accounts .recently numerous high profile thefts have been occurred .some of the examples are LinkedIn ,yahoo, eHarmony .these companies have suffered from several password thefts because they are too predictable or can be easily guessed.

III. Proposed System

A. *System architecture:*

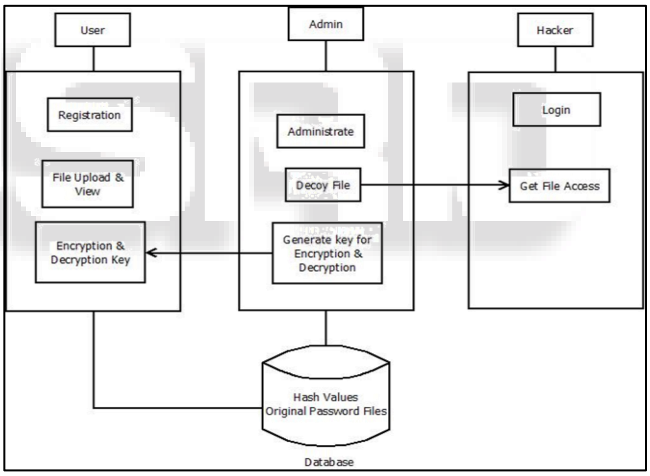

Fig. 1: System Architecture

IV. Modules

A. *Registration:*

User is going to register into the system providing normal credentials along with a key provided for uploaded file encryption and decryption. Honeywords are generated from entered user password. Password is stored along with the honeywords at random location by the system into the database.

B. *Login:*

User is going login into his account using username and password provided at the time of registration. The entered password is validated against that of stored password's hash if true then login successful else login failed and user has to enter details again. If user fails thrice then it gives access to the decoy account.

C. Hacker:

Hacker tries to get access to authenticated user account. If he enters the password it checks with the indices of hashes that stored in database. If it matches with index of hash it gives access to the authenticated user neither it gives access to decoy account

D. File upload and view:

Authenticated user of system can upload his files into the system. Using key provided for encryption and decryption.

E. Admin:

Admin can login into the system and manage the users of the system. Also, admin can upload decoy files in the fake account for intruder.

F. Log creation:

Each and every activity of user stored in the form log files. This log files used to track behavior of user as well as intruder and it manage by admin

V. FLOW OF SYSTEM

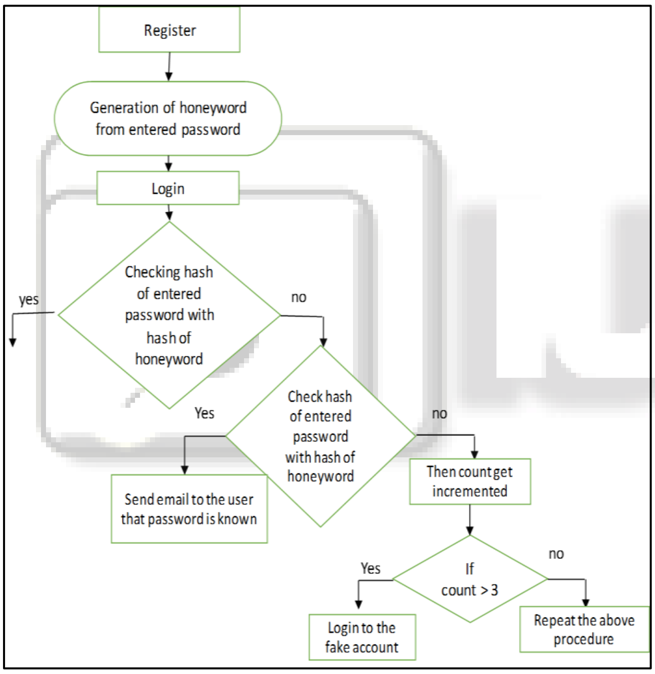
Register
Generation of honeyword from entered password
Login
Checking hash of entered password with hash of honeyword
yes
no
Yes
Check hash of entered password with hash of honeyword
no
Send email to the user that password is known
Then count get incremented
Yes
If count > 3
no
Login to the fake account
Repeat the above procedure

Fig. 2: System Flow

VI. HENEYWORD GENERATION METHODS

A. Password model:

In this method password is splitted into characters ,integers and then this characters and integers are replaced by random characters and random integers respectively .for example pearl8diamonds the password is splited into character sets as L5+D1+L8 and replaced with same composition rahul2monsters

B. Chaffing by tweaking:

In this method randomly selected digits and characters positions are replacedto generate the honeywords for ex every character of user password in predetermined position replaced by randomly choosen character of the same type .Tushar1993 replaced tushar1693,tushar7854,tushar3244,tushar1648

C. Hybrid method:

This method is combination of password model and chaffing by tweaking method .random password model will generate seeds for tweaking digits of the password to generate honeyword

Ex sagar69facebook replaced by asfwe23mnjgifty ,werfg65opfhridn

VII. TYPES OF ATTACKS

A. Brute force:

To find the real password in this attack hacker try number of passwords combinations until and unless he get's real password.

B. Guessing attack:

In this type of attack hacker trying some common passwords to login into the system.

C. Malware:

In this attack model hacker introduces a trojan file into the system of user.trojan track the system of user and send information to the intruder.intruder will get required users password information.

D. One password to many system:

Generally users habit to keep same password to many account for remember purpose.if intruder know the one of the password of users account he will try that password to other same users account.

REFERENCES

[1] Imran Erguler,” Achieving Flatness: Selecting the Honeywords from Existing User Passwords”, DOI 10.1109/TDSC.2015.2406707, IEEE Transactions on Dependable and Secure Computing.

[2] A. Vance, “If Your Password is 123456, Just Make It Hackme,” The New York Times,vol. 20, 2010.

[3] K. Brown, “The Dangers of Weak Hashes,” SANS Institute InfoSec Reading Room, Tech. Rep., 2013.

[4] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password Cracking Probabilistic ep., 2013.

[5] H. Bojinov, E. Burs ztein, X. Boyen, and D. Boneh, ―Kamouflage: Loss -resistant Password Management,‖ in Computer Security– ESORICS 2010. Springer, 2010, pp. 286–302.

[6] M. Weir, S. Aggarwa l, B. de Medeiros, and B. Glode k, ―Password Cracking Using Probabilistic Context –Free Grammars,‖ in Security and Privacy, 30th IEEE Symposium on. IEEE, 2009, pp. 391–405.

[7] F. Cohen. The use of deception techniques: Honeypots and decoys. In H. Bidgoli, editor, Handbook of Informat ion Security, volume 3, pages 646–655. Wiley and Sons, 2006

[8] L. Spitzner. Honeytokens: The other honeypot. Symantec SecurityFocus, July 2003

[9] J. Yuill, M. Zappe, D. Denning, and F. Feer.Honeyfiles: deceptive files for intrusion detection. In Information Assurance Workshop, pages 116–122, 2004

[10] A. Juels and R. L. Rivest, ―Honeywords: Making Passwordcracking Detectable,‖ in Proceedings of the 2013 ACM SIGSAC Conference on Co mputer & Co

mmunicat ions Security, ser. CCS ’13. Ne w Yo rk, NY, USA: A CM, 2013,pp. 145–160. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516671

[11] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez,― Guess again (and gain and again): Measuring Password Strength by Simulat ing Password-cracking Algorithms,‖ in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523–537.