Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 06, June -2018

# SECURED PASSWORD USING HONEYWORD ENCRYPTION

Prashant D. Shinde [1], Dr. Suhas H. Patil [2]

[1] *Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, INDIA*
[2]*Faculty of Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, INDIA*

**Abstract -** *The honeyword gadget can be used to detect an adversary who efforts to login with cracked passwords. New password is the grouping of existing passwords called as honey words. Fake password is practically nothing but the honey words. Basically, for each username a set of sweet words is produced such that only one particular component is the proper password and the others are honey word passwords. Hence, when an adversary tries to enter into the system with a honey word, an alarm is activated to notify the administrator about a password leak. Honey words to detect attacks contrary to hash password database. For each user explanation the real password stored is kind of honey words. If attacker attacks on password i.e. honeys words it cannot be sure it is real password or honey word. In this study, we need to examine in detail with utmost care the honey word technique and existing some comment to focus be utilized weak points. Also focus on pragmatic password, reduce storage value of password, and alternate way to choice the new password from existing passwords.*

***Keywords*** *- Honeyword, passwords, password cracking, Authentication, Login.*

## I. INTRODUCTION

In this paper, there are two issues that must be measured to overwhelm safety problems: First passwords must be protected by desirable appropriate defences and storage with their confused values calculated through salting or some other compound mechanisms. Hence, designed for an adversary it must be difficult to use hashes to obtain plaintext passwords. The additional view is that a protected organization should perceive whether a keyword file discovery occurred or not to take proper actions. In this study, we focus on the latter issue and deal with fake passwords or accounts as a simple and expense effective solution to detect leakage of passwords. When a user sends a login request, the login server will determine the order between the users, and the order of the submitted password among her sweetwords. The login server sends a message of the form to a secure server which is called "honey checker", for the user and her sweet word. The honey checker will determine whether or not the submitted word is a password or a honey word. If a honey word is submitted, then it will raise an alarm or take an action that is previously selected. The honey checker cannot identify near the user's password or honey words. It maintains a single database that contains made up of only the order of the real password among the user's sweet words.

## II. LITERTURE SURVEY

| Sr.No | Paper Name | Description | Year | Advantages | Disadvantages |
|---|---|---|---|---|---|
| 1 | Password Cracking Using Probabilistic Context-Free Grammars. | Selecting the greatest real word-mangling rules to use once execution a dictionary-based password cracking attack can be a difficult task. | 2010 | To provide a more effective way to crack passwords as compared to traditional methods by testing | Most effective when tailoring one's attack against different sources by training on passwords of a relevant structure. |
| 2 | Examination of a new defence mechanism: Honey words. | The incentive passwords i.e. honey words to detect attacks in contradiction of hash password database. For | 2011 | honey words may not be real passwords | It is much easier to crack a password hash with the advancements in the graphical processing unit |

 

| | | | | | |
|---|---|---|---|---|---|
| | | each user account the legitimate password is stored in form of honey words. | | | |
| 3 | Guess again : Measuring password strength by simulating password-cracking algorithms | Provides numerous distinguished results about the relative strength of different composition policies. . | 2012 | Effectiveness of a dictionary check depends heavily on the choice of dictionary | Easily guessed passwords. |
| 4 | A large-scale study of web password habits. | Report the consequences of a large scale password usage and password re-usage habits. The education involved half a million users over a three month period. | 2010 | Client component on users' machines recorded a variety of password strength | Large number and poor quality of user passwords |
| 5 | Improving Security Using Deception | The convergence between corporal and numerical world continues at a rapid pace, much of the information is becoming available online. | 2011 | Identify some of the areas that are need further investigation | To drive the security community away from deception-based mechanisms. |

## III. EXISTING SYSTEM

It separates the honey word method and gives some recognition about the security of the system. It points out that the key item for this approach is the generation algorithm of the honeywords such that they are indistinguishable from the correct passwords. So, this paper proposes a new technique that shaped the Honey words using the existing user passwords combination in hash format.

**DISADVANTAGES OF EXISTING SYSTEM**

- Less secure.
- Secure system don't detect whether a password file cracked incident happened.
- It can't detect the attacks against hashed password databases.

## IV. PROPOSED SYSTEM

This paper, focus on the security issue and deal with fake passwords or accounts as a simple and value effective solution to detect agreement of passwords. Honeypot is one of the approaches to recognize occurrence of a password database breach. In this approach, the administrator purposely produces deceit consumer accounts to lure adversaries and detects a password disclosure, if any one of the honeypot password gets used. The paper proposes a novel honeywords generation technique which reduces the storage overhead and also it addresses majority of the drawbacks of existing honeyword

 

generation techniques. Planned typical is based on routine of honey words to detect password-cracking. It propose to use catalogues that map to valid passwords in the system. The involvement of the approach is two ways. First, this method requires less storage compared to the original review. In our approach, passwords of other users are used as the fake passwords, so guess of which password is fake and which one is correct becomes more complicated for an adversary.

**ADVANTAGES OF PROPOSED SYSTEM**

1. It creates honey words from existing user password.
2. It detects attacks against hashed password databases.
3. It reduces the storage cost while creating honey words as compared to existing honey words Creation methods.

## V. SYSTEM ARCHITECTURE

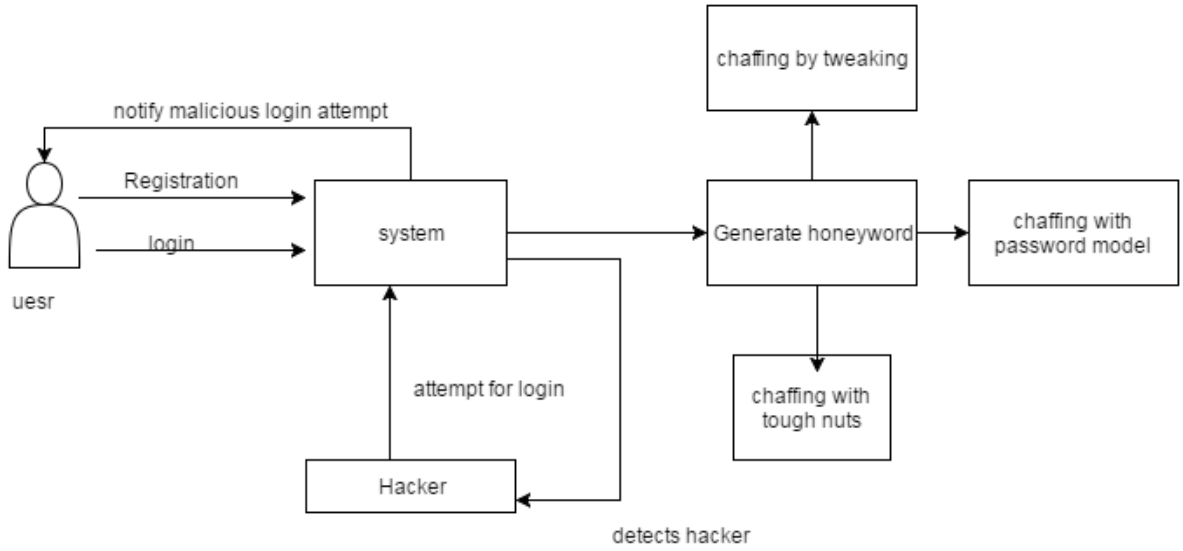


Fig.1: System Architecture

User will register to the system, at the time of registration user will enter the 3 Honey words. Also system will generate no. of Honey words with the help of user password by three methods:

- Chaffing with Tough nut
- Chaffing with Tweaking
- Chaffing with Password Model

If user entered right username but if password is wrong also password is not a honey word then system will block that particular user and request to admin for activate the account. Admin will protect the passwords by using Honey Encryption method. The honey encryption method used by using passwords and keys. We have generated the many to many relationships and compare to each key with seed space. Then XOR operation performed. It will track the user's record i.e. number of wrong passwords and number of honey words for particular user login.

## VI. METHODOLOGY

1. Chaffing with Tough nut:
   In this method, the system intentionally injects some special honeywords, named as tough nuts, such that inverting hash values of those words is computationally infeasible, e.g. fixed length random bit strings should be set as hash value of a honeyword. Moreover, it is noted that number and positions of tough nuts are selected randomly. By means of this, it is expected that the adversary cannot seize whole sweetword set and some sweetwords will be blank for her, thereby deterring the adversary to realize her attack. It is discussed that in such a situation the adversary may pause before attempting login with cracked passwords.

2. Chaffing with Tweaking:
   In this method, user password seeds the generator algorithm which tweaks selected character positions of the real password to produce the honeywords. For instance, each character of user password in predetermined

 

positions is replaced by a randomly chosen character of the same type: digits are replaced by digits, letters by letters, and special characters by special characters. Number of positions to be tweak, denoted as t should depend on system policy etc. As an example t = 3 and tweaking last t characters may be a method for generator algorithm Gen (k, t). Another approach named in the study as "chaffing-by-tweaking-digits" is executed by tweaking the last t positions that contain digits. For example, by using last technique for the password 42hungry and t = 2, the honeywords 12hungry and 58hungry may be generated.

3. Chaffing with Password Model
   It is combining the strength of different honeyword generation methods, e.g. chaffing-with-a-password-model and chaffing-by-tweaking-digits. By using this technique, random password model will yield seeds for tweaking-digits to generate honeywords. For example let the correct password be apple1903. Then the honeywords angel2562 and happy9137 should be produced as seeds to chaffing-by-tweaking-digits. For t = 3 and k = 4 for each seed.

## VII. CONCLUSION

We have studied carefully the security of the honey word technique and introduce a solution that can be used for successful realization of the scheme. In this respect, we have pointed out that the strong level of the honey word technique directly depends on the generation algorithm. We have presented a new approach to make the generation algorithm close to human nature by generating honey words with randomly selecting passwords that belong to other users in the system. We present a standard approach for securing personal and organizational information in the system. We suggest checking of information access patterns by profiling user to determine if and when a malicious user illegally access someone's documents in a system support. The documents stored in the system alongside the user's real information also serve assessors to detect illegitimate entry. Once illegal information access or exposure is supposed, and verified, with checked queries for occurrence, we inundate the malicious user with fake information in order to insipid or distract the user' s real data. Such kind of preventive attacks that depend on deception knowledge could provide unique amounts of security in the system and in social networks

## VII. REFERENCES

1. M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in Proc. 30$^{th}$IEEE Symp. Security Privacy, 2009, pp. 391–405.

2. Z. A. Genc, S. Kardas, and M. S. Kiraz, "Examination of a new defense mechanism: Honeywords," IACR Cryptology ePrint Archive, Report 2013/696, 2013.

3. 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 simulating password-cracking algorithms," in Proc. IEEE Symp. Security Privacy, 2012, pp. 523–537.

4. D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 657–666.

5. M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, "Improving security using deception," Center for Education and Research Information Assurance and Security, Purdue Univ., West Lafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013-13, 2013.

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. K. Brown, "The dangers of weak hashes," SANS Institute InfoSec Reading Room, Maryland US, pp. 1–22, Nov. 2013,

 