|| Volume 6 || Issue 5 || May 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

# HONEYWORD FOR SECURITY: A REVIEW

**Miss. Vrushali Thite , Prof. Dr.Mininath Nighot**
*D. Y. Patil College of Engineering Ambi, Talegaon, Pune*

---

**Abstract: - In recent years, all of the activities of countries worldwide have been carried out digitally, and all information or data has been shared over the network, increasing the speed and efficiency of data. Nevertheless, this transformation of data over the digital network poses a security risk, namely the loss of user data by third-party unauthorized persons or attackers. To preserve security, every user is given a unique identifier or password, but the attacker still robs the password using several techniques to avoid this risk, we use "honey words". For detecting password database breaches, we propose a system called the "Advanced Honey words System". The plan is to create several honey words, or false passwords, and store them alongside the real password. Because legitimate users are not required to recognize the honey words corresponding to their passwords, any login attempt with honey words is flagged as a password database compromise. Their concept includes honey word production, typo-safety measures to prevent false alarms, alarm policy upon detection, and checking the system's robustness against various attacks. If hackers trying to access user accounts and enter 3 times wrong password, the hacker will get decoy file, also for each incorrect password, a notification will go to the admin and user. This will provide security. For each wrong password, the user and admin get a notification.**

***Keywords***— *Password, Honeywords, Password hash breach, Detection technique, Authentication, Security.*

---

## INTRODUCTION

### Overview

Many businesses and software sectors store their data in databases such as ORACLE or Mysql, or other databases. Thus, in the database, the entry point of a system that needs the username and password is encrypted. Once a password file has been stolen, it is easy to capture most plaintext passwords using the password cracking technology. There are two issues that must be addressed in order to avoid this: The first passwords must be secured with the appropriate algorithm and protected. The second point is that the entry of unauthorized users into the system should be recognized by a secure system.

In the system we are concentrating on fake passwords and accounts. If any of the honey pot passwords is used, you can easily detect the admin. If the administrator creates user accounts and finds a password disclosure. According to the study, incorrect login trials with a certain password are recognized for every user and result in Honey Pot accounts. We have created and saved the password with the fake password set on the proposed system. We analyses the approach of honeywords and make a few comments about system security. In the case of unauthorized users trying to enter the system, the alarm is triggered and administrator will receive notification since unauthorized users receive decoy documents.

### Motivation

Generally real passwords are very easy to detect and thus hack the system. So here the main motivation is to avoid this kind of hacking by the creation of honeywords. The human mind is incapable of accurately storing a large amount of data. In fact we can sometimes not even remember one password easily. This is why a honey word based security system is needed to save crucial files from going into wrong hands that can manipulate important data for a wrong use and harm someone personally or harm the whole industry or company. Using this process the main user just needs to remember one original password that he sets for the account. The rest of it is taken care of by the working of the honey word security set up.

### Goal and Objectives

Goal

Develop a system that protects security of the database file. Detect attacks against hashed password databases.

Objectives:

- To design a system that to identify occurrence of a password database breach.
- To focus on fake passwords or accounts as a simple and cost effective solution to detect compromise of passwords.
- To design a system that focuses the cracked password files can be detected by the system administrator if a login attempt is done with a honey word by the adversary.
- To propose a completely different approach to securing the cloud using decoy information.

- To use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

## II RELATED WORK

In this paper [1], they check the honeyword system and present some remarks to highlight possible weak points. Also, they suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honeyword generation method – and also to reduce storage cost of the honeyword scheme.

In this paper [2], they create the honeyword, i.e. a false word, using a perfectly flat honeyword generation method. Hence that time they catch the unauthorized user and also the attacker not getting the original data. Now a day, rapid expansion of the accessing data from the network or from the other system the security becomes biggest issue. Storage of information also becomes the insecure because of attacker. And encryption of the data is also having some deficiencies. So the security of data is the latest issue. As the solution of above problem is the honey word generation is the best option for providing security to the data. In existing systems they only concentrated on the security of the password file but the different issues come. For solving this here we create the honeyword, i.e. a false word, using a perfectly flat honeyword generation method. Hence that time we catch the unauthorized user and also the attacker not getting the original data.

In this system [3] the tools create fake accounts and how they manage to circumvent existing security measures. It also helps to get an insight into what websites do in order to handle fake accounts, both during the account sign-up process, as well as and after the fake accounts have been created.

Using deception techniques [4] (as in honeypots), they propose the user-verifiable authentication scheme (Uvauth) that tolerates, instead of detecting or counteracting, guessing attacks. Uvauth provides access to all authentication attempts; the correct password enables access to a legitimate session with valid user data, and all incorrect passwords lead to fake sessions.

Over the last year [5], there have been many high-profile login leaks, including LinkedIn, Yahoo, and eHarmony. Although you never want vulnerabilities that give hackers access to your password hashes, you also want to make sure that if the hashes are broken, hackers can't easily generate passwords from them. Large businesses are using poor hashing mechanisms that make it easy to break user passwords, as these leaks have shown. In this article, I'll go through the fundamentals of password hashing, look at password cracking software and hardware, and talk about how to use hashes safely.

In this paper [6], proposed comparing password distributions with a uniform distribution which would provide equivalent security against different forms of guessing attack, author estimate that passwords provide fewer than 10 bits of security against an online, trawling attack, and only about 20 bits of security against an optimal offline dictionary attack.

Author [7] create partial guessing metrics that include a new type of guesswork that is parameterized by the attacker's desired success rate. Our new metric is simple to calculate and directly applicable to security engineering. We estimate that passwords provide less than 10 bits of protection against an online trawling attack and just about 20 bits of security against an optimal offline dictionary attack by comparing password distributions to a uniform distribution that would provide equal security against various types of guessing attacks. Surprisingly little variation in guessing difficulty exists; every recognisable group of users created a password distribution that was similarly poor. Security motivations like registering a credit card have no more influence than demographic factors like age and nationality. Also constructive attempts to encourage users to use better passwords by providing graphical input are ineffective.

Authors create [8] partial guessing metrics that include a new type of guesswork that is parameterized by the attacker's desired success rate. Our new metric is simple to calculate and directly applicable to security engineering. We estimate that passwords provide less than 10 bits of protection against an online trawling attack and just about 20 bits of security against an optimal offline dictionary attack by comparing password distributions to a uniform distribution that would provide equal security against various types of guessing attacks. Surprisingly little variation in guessing difficulty exists; every recognizable group of users created a password distribution that was similarly poor. Security motivations like registering a credit card have no more influence than demographic factors like age and nationality. Also constructive attempts to encourage users to use better passwords by providing graphical input are ineffective.

In this paper [9] we studied one of the Honeyword generation method i.e. chaffing-with-tweaking provide some possible improvements which are easy to implement and introduce an enhanced model as a solution to an open problem also overcomes almost all the drawbacks of previously proposed honeyword generation approaches.

Author develop [10] an efficient distributed method for calculating how effectively several heuristic password-guessing algorithms guess passwords. Leveraging this method, we investigate (a) the resistance of passwords created under different conditions to guessing; (b) the performance of guessing algorithms under different training sets; (c) the relationship between passwords explicitly created under a given composition policy and other passwords that happen to meet the same

requirements; and (d) the relationship between guessability, as measured with password-cracking algorithms, and entropy estimates. Our findings advance understanding of both password-composition policies and metrics for quantifying password security.

| Paper Name | Author Name | Publication Paper | Description | Observation |
|---|---|---|---|---|
| 1.Achieving Flatness: Selecting the Honeywords from Existing User Passwords | Imran Erguler | 2015 | In this paper, they check the honeyword system and present some remarks to highlight possible weak points. Also, they suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honeyword generation method – and also to reduce storage cost of the honeyword scheme. | In this paper, we have observed the solution to the detection of password file disclosure events, and also referred how to reduce storage cost of the honeyword scheme. |
| 2.Security Analysis of Honey words Generation Scheme to Evade Unauthorized Access | Ms. Manisha B. Kale and Prof. D. V. Jadhav | 2016 | In this paper, they create the honeyword, i.e. a false word, using a perfectly flat honeyword generation method. Hence that time they catch the unauthorized user and also the attacker not getting the original data. | In this paper, we have observed how to create honeywords i.e. false word, using a perfectly flat honeyword generation method. |
| 3.An analysis of various tools, methods and systems to generate fake accounts for social media | Avanish Pathak | 2014 | In this system the tools create fake accounts and how they manage to circumvent existing security measures. It also helps to get an insight into what websites do in order to handle fake accounts, both during the account sign-up process, as well as and after the fake accounts have been created. | In this system we have observed how to manage security of user accounts and how to handle fake accounts during sign-up process and after the accounts have been created. |
| 4.Explicit Authentication Response Considered Harmful | Lianying Zhao and Mohammad Mannan | 2013 | Using deception techniques (as in honeypots), they propose the user-verifiable authentication scheme (Uvauth) that tolerates, instead of detecting or counteracting, guessing attacks. Uvauth provides access to all authentication attempts; the correct password enables access to a legitimate session with valid user data, and all incorrect passwords lead to fake sessions. | In this paper we have observed password authentication of user instead of detecting or guessing attacks. |
| 5. The Dangers of Weak Hashes | Kelly Brown | 2013 | In this paper, discussed the basics of password hashing, look at password cracking software and hardware, and discussed best practices for using hashes securely. | In this system we have observed if we want to prevent our data or our password then we have to store passwords as hashes using strong encryption algorithms. |

| | | | | |
|---|---|---|---|---|
| 6) The science of guessing: analyzing an anonymized corpus of 70 million passwords | Joseph Bonneau | 2013 | In this paper proposed comparing password distributions with a uniform distribution which would provide equivalent security against different forms of guessing attack, author estimate that passwords provide fewer than 10 bits of security against an online, trawling attack, and only about 20 bits of security against an optimal offline dictionary attack. | From this we observed Preventing password cracking, Preventing cross-account compromise. |
| 7) Password Cracking Using Probabilistic Context Free Grammars | Matt Weir, Sudhir Aggarwal, Breno de Medeiros, Bill Glodek | 2012 | In this paper proposed method that generates password structures in highest probability order. | In this system we observed create a rule set to generate password guesses for use in cracking unknown passwords. |
| 8)Guess again (and again and again):<br><br>Measuring password strength by simulating password-cracking algorithms | Patrick Gage Kelley, Saranga Komanduri, ichelle L. Mazurek, ichard Shay, Timothy Vidas Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez | 2012 | In this paper author develop an efficient distributed method for calculating how effectively several heuristic password-guessing algorithms guess passwords. | We observed policies for guessability |
| 9) Honeywords: A New Approach For Enhancing Security | Manisha<br><br>Jagannath<br><br>Bhole | 2013 | In this paper we studied one of the Honeyword generation method i.e. chaffing-with-tweaking provide some possible improvements which are easy to implement and introduce an enhanced model as a solution to an open problem also overcomes almost all the drawbacks of previously proposed honeyword generation approaches | We observed Chaffing-With-Tweaking algorithm |
| 10) Examination of a New<br><br>Defense Mechanism: Honeywords, | Dr.Prashant Kumbharkar, Snehal Aher, Ashish Dhamal, Vinay Maslekar,Akshay<br><br>Takale | 2012 | In this paper studied a False watchword utilizing a consummately level nectar word era strategy. | In this paper we observed this model by involving hybrid generation algorithms |

## III.OPEN ISSUES

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the techniques for Honeyword systems.

In existing approach, they check the honey word system and present some remarks to highlight possible weak points. Also, they suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honey word generation method – and also to reduce storage cost of the honey word scheme.

## IV CONCLUSION

In this system we analyzed the possibility of using Honeyword as an ideal mechanism to protect passwords if the problems it addresses could be resolved. We have indicated the strength of the honeyword system will be determined by the honeyword creation mechanism we have adapted. Another point we want to emphasize is that the system has to guarantee the low probability of DoS since it may present a serious threat. The proposed model has been compared to other models in terms of resistance, flatness and usability in terms of safety and usability compared to other models.

## 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] Ms. Manisha B. Kale, Prof. D. V. Jadhav, " Security Analysis of Honey words Generation Scheme to Evade Unauthorized Access" , Department of Computer Engineering, Zeal College of Engineering and Research, Pune, India1, Tech. Rep. Issue 7, July 2016.

[3] A. Pathak, "An Analysis of Various Tools, Methods and Systems to Generate Fake Accounts for Social Media," Ph.D. dissertation, Northeastern University Boston, 2014.

[4] L. Zhao and M. Mannan, "Explicit Authentication Response Considered Harmful," in Proceedings of the 2013 Workshop on New Security Paradigms Workshop–NSPW '13. New York, NY, USA: ACM, 2013, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/2535813.2535822

[5] K. Brown, "The Dangers of Weak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.

[6] A. Juels and R. L. Rivest, "Honeywords: Making Password cracking 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

[7] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 538–552.

[8] D. Malone and K. Maher, "Investigating the Distribution of Password Choices," in Proceedings of the 21st International Conference on World Wide Web, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 301–310. Q111111111[Online]. Available: http://doi.acm.org/10.1145/2187836.2187878

[9] Z. A. Genc, S. Kardas, and K. M. Sabir, "Examination of a New Defense Mechanism: Honeywords," Cryptology ePrint Archive, Report 2013/696, 2013

[10] 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 Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523–537.