MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

HONEYWORD TO DETECT UNAUTHORIZED ACCESS

S.S. Kulkarni, R.V.Kulkarni, S.P.Akant,
P.D.Pophalkar, A.G.Kulkarni, Mrs. Shaikh J.N.

Department of Computer Engineering , Bhivrabai Sawant Polytechnic
Pune , India

Abstract: *The new developments in the field of information technology offered the people enjoyment, comforts and convenience, but there are many security related problems. One of them is password file. Password files have got a lot of security problem that has affected millions of users as well as many companies. Password file is generally stored in encrypted format, if a password file is hacked or theft by using the password cracking techniques and decryption technique it is easy to capture or find most of the plaintext and encrypt passwords. For troubleshoot this here we produce the honey word password, i.e. a False password using a perfectly flat honey word generation method, and try to attract illegal or unauthorized user. Hence that time we find the unauthorized user. Here we also protect the original data from unauthorized user. As mentioned above, in this system we have used Honey words also called as Sweet Password Security Strategy.*

Keywords: *Honeywords , ADS, DES, Honeychecker*

1. INTRODUCTION

Generally in many companies and software industries store their data in databases like ORACLE or Mysql or may be other. So, the entry point of a system which is required user name and password are stored in encrypted form in database. Once a password file is stolen, by using the password cracking technique it is easy to capture most of the plaintext passwords. So for avoiding it, there are two issues that should be considered to overcome these security problems: First passwords must be protected and secure by using the appropriate algorithm. And the second point is that a secure system should detect the entry of unauthorized user in the system. In the proposed system we focus on the honey words i.e. fake passwords and accounts. The administrator purposely creates user accounts and detects a password disclosure, if any one of the honey pot passwords get used it is easily to detect the admin. According to the study, for each user incorrect login attempts with some

passwords lead to Honey pot accounts, i.e. malicious behavior is recognized. In proposed system, we create the password in plain text, and stored it with the fake password set.

2. LITERATURE SURVEY

Paper Name	**Author Name**	**Proposed System**	**For this paper we referred**
1.Achieving Flatness: Selecting the Honeywords from Existing User Passwords	Imran Erguler	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 referred 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	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 referred how to create honeywords i.e. false word, using a perfectly flat honeyword generation method.
3. The Dangers of Weak Hashes	Kelly Brown	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 referred if we want to prevent our data or our password then we have to store passwords as hashes using strong encryption algorithms.

4.Explicit Authentication Response Considered Harmful	Lianying Zhao and Mohammad Mannan	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 referred password authentication of user instead of detecting or guessing attacks.

3. EXISTING SYSTEM

In this paper, 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.

Disadvantages: System doesn't provide the other security

4. PROPOSED SYSTEM

In the proposed system, we would like to refine our model by involving hybrid generation algorithms to also make the total hash inversion process harder for an adversary in getting the passwords in plaintext form from a leaked password hash file. Hence, by developing such methods both of two security objectives – increasing the total effort in recovering plaintext passwords from the hashed lists and detecting the password disclosure – can be provided at the same time.

Advantages

- System protects the original data from unauthorized user.
- System protects against the misuse of the users real data.

5. SYSTEM ARCHITECTURE

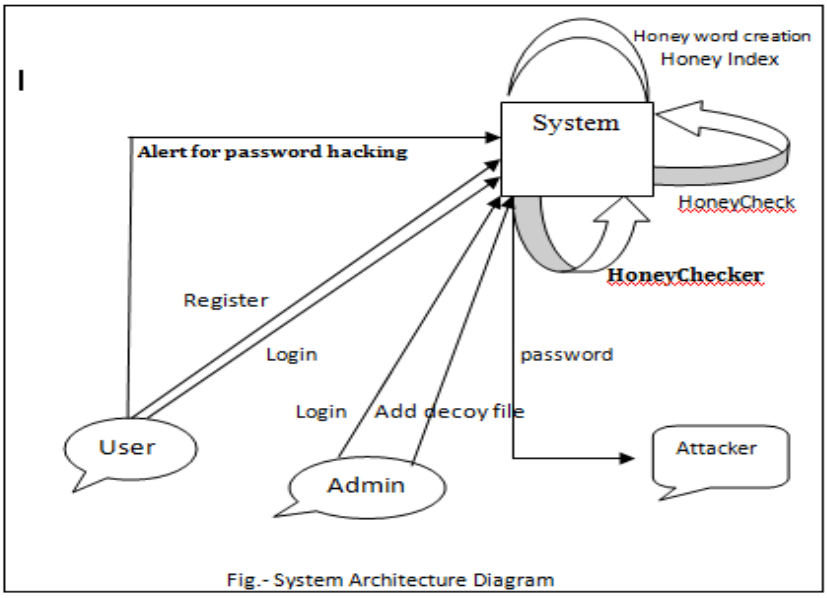

Figure 1: Proposed System Architecture-

6. CONCLUSION

We present a standard approach to securing personal and business data in the system. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegally accesses someone's documents in a system service. Decoy documents stored in the system alongside the user's real data also serve assessors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with fake information in order to dilute or divert the user's real data. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the system and in social networks model.

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*