A SURVEY OF HONEYWORDS TECHNIQUES FOR USER AUTHENTICATION ENHANCEMENT

Rupali T. Gholap [1], Dr.Niranjan L. Bhale[2]

[1] *ME Student, Department of Computer Engineering, MCOERC, Maharashtra, India*
[2] *HOD, Department of Information Technology, MCOERC, Maharashtra, India*

ABSTRACT

Honeywords (decoy passwords) to detect attacks against DOS attack. For each user account, the legitimate password is stored with several honeywords . If honeywords are selected properly, a cyber- attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honeyword for any account. An attacker , entering with a honeyword to login will raise an alarm and notifying the administrator about a password file breach.words. selects the honeywords from existing user passwords in the system in order to provide realistic honeywords used at honeyword generation method and also to reduce storage cost of the honeyword scheme. a simple and effective solution to the detection of password file disclosure. In this study, the honeyword system is used.

Keyword : - *Hybrid technique ,Initialization, User authentication, User Registration, honeypot, honeywords, Inversion process of Hash .*

1. INTRODUCTION

Many users having a big security problem like password file disclosure.When an attacker tries to enter into the system with a fake password,that time an alarm is triggered and to notify the administrator and send a message to main user or tell user someone can access your account.The administrator creates fake accounts and detects a password disclosure, if any one of the honeypot account get used it will detect by admin.There are two issues that should be considered to overcome these security problems:

- First,By taking appropriate precautions protect a password and storing with their hash values.
- The second point is that when not to take appropriate actions that time password file is disclosure means secure system should detect.

Fake password means honeywords to detect password disclosuer.Main focus is on the use of fake passwords and accounts.Hybrid Technique using Honeypot and Honeyindex to examine the security of the begin authentication system by reducing storage of honeyword scheme.

1.1 Terminology

There are many terminology explain below:

1) Honeyword: Honeywords means decoy passwords or fake passwords. The idea is the insertion of fake passwords called as honeywords associated with each users account. When an attacker gets the password _le, he recovers many passwords for each account and he cannot be sure about which word is genuine. Hence, the cracked password _les can be detected by the system administrator if a login attempt is done with a honeyword by the adversary.For generating these Honeywords , use some methods these are Chaffing-by-tweaking, Chaffing-with-a-password-model, Chaffing with-Tough Nuts and Hybrid Method. These methods are useful and decrease the chances of guessing correct password.

2) Sweetwords:: Honeywords and true passwords are placed into a list of Sweetwords.

3) Honeychecker:: In this honeychecker is nothing but an auxiliary service which store correct indexes for each user account.

4) Honeypot: A Honeypot is a security capability whose value is being probed, attacked or comprised. A honeypot is a secure source.A Honeypot could just as simply be one of your old PCs, a script or even a digital entity like some fabricated patient records. Whose value is being probed, attacked or comprised. Hybrid Technique using Honeypot and Honeyindex to examine the security of the begin authentication system by reducing storage of honeyword scheme.

5) Honeyindex : Instead of honeywords we use honeyindexes, for every account we created a new and unique honeyindex. The correct honeyindex is store with the hash of the correct password in a list. In another list we have integer list with the username, the integer list is a honeyindexes of other accounts as well as their own account honeyindex this list is called as a honeyindex set.

2.LITERATURE SURVEY

The most important concept is information security requirement in this which is secured using some authentication method. Various authentication method are existing such as Patterns, Passwords, PIN's etc.. Now-a-days most generally used technic for authentication is passwords. Security of password is an important part in security. A password is a secret word, which a user must input during a login, this word is match only after that it is possible to get access. Generally disclosure of password les is a several security problem that has a ected millions of users and many companies and software industries store their data in database, Like facebook, Yahoo, RockYou, Gmail and Adobe. Generally user name and passwords are stored in a database. Since stolen passwords make the users target of many possible attacks. These recent events have proved that the weak password storage methods are currently used by many people on websites. For example, the LinkedIn passwords were using the SHA-1 algorithm without a salt and similarly the passwords in the eHarmony system were also stored using unsalted MD5 hashes.Once a password le is leakage, attacker by using the password cracking technique it is easy to capture most of the plaintext passwords.
In this respect, there are two issues that should be considered to avoid these security problems:

First, passwords must be protected by taking proper caution and storing with their hash values computed through some other correct complex mechanisms. Hence, for an advance it must be hard to include hashes value in plaintext passwords.
The second point is that a secure system should detect whether a password le leakage incident happened or not to take appropriate actions.

Honeypot is one of the methods to identify occurrence of a password database breach. In this approach, the administrator purposely creates deceit user accounts to lure adversaries and detects a password disclosure, if any one of the honeypot passwords get used. In the proposed system focus on the honeyindex and deal with fake passwords or accounts as a simple and cost effective solution to detect compromise of passwords. Many researchers have already worked for password security approach. Earlier, to protect online banking accounts from brute-force attacks, Herley and Florencio proposed a new approach to detect the malicious behaviour on every incorrect or unauthorized login. For every single user false login attempts with few passwords will generate honeypot accounts (fake accounts) so that malign behaviour is caught. Recently, Juels and Rivest have presented the honeyword mechanism to detect an adversary who attempts to login with cracked passwords. Imran Ergulers Achieving Flatness by Selecting the Honeywords from Existing User Passwords,this suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords a perfectly at honeyword generation method and also to reduce storage cost of the honeyword scheme. The propose system in concept is that for each username they build a set of honeyindexes in which one is real index and the others are false. When detecting the honeyword than alarm is triggered which noties the administrator about the password le breach.

Summary
In existing system honey indexing and honey pots are not used so storage cost is more. So proposed system implement the Hybrid Technique using Honey pot and Honey index to analyzed the security of the begin authentication system by reducing storage of honey word.

3. SYSTEM FLOW

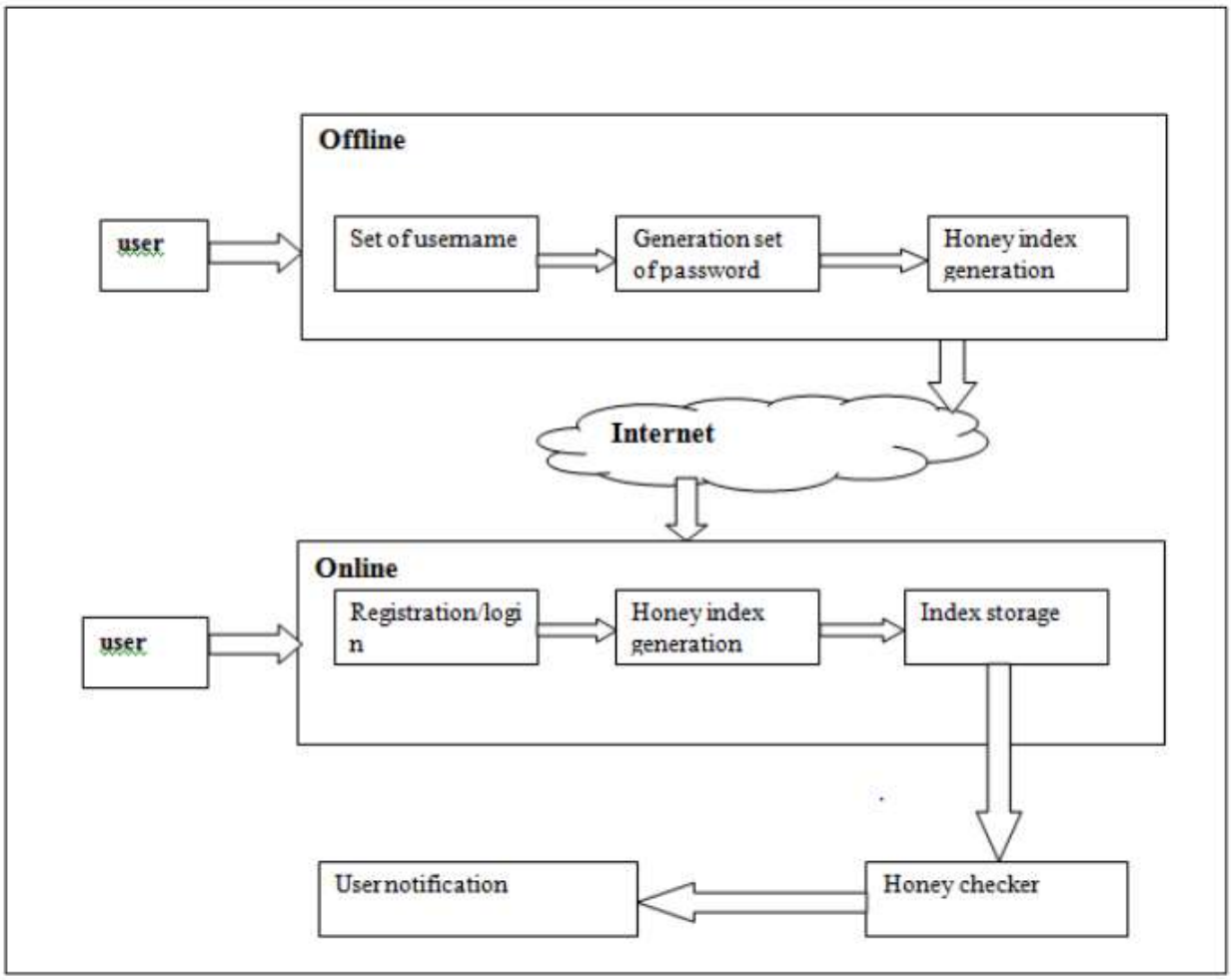

Fig1: System flow

i) For the first users of the system, there should be a previously prepared password-pool from where passwords are assigned as honeywords for these users. So, honeypot passwords indeed make up this initial password-pool.

ii) By means of the honeypots, the proposed model reduces the success probability of the brute-force attack how honeypot accounts and their respective passwords should be generated. The usernames may be _ctional and can be produced by automated software programs and scripts, e.g. spam trap, spammer address and online fake account generators.

On the other hand, to generate passwords for these accounts we adapt a similar approach of : The method uses a fixed dictionary3 that includes di_erent length of words, to pick up random dictionary words. Firstly, the length of the password l is randomly determined such that it conforms to the password policy of the system.

Honeypot Checking: If a match is not found, then it means that g is neither the correct password, nor one of the honeywords, i.e. login fails. If H(g) is found in list, then the main server checks whether the account is a honeypot. If it is a honeypot, then the attacker is get redirected to the fake application . If however, H(g) is in the list and it is not a honeypot, the corresponding indices is delivered to honeychecker with username and to verify that it is the correct index.

use two password files as F1 and F2 in the main server: F1 stores username and honeyindex set. And other hand, F2 keeps the index number and the corresponding hash of the password. Show in following tables.

Table -1 Password file f1

Username	Honeyindex Set
agent-lisa	$(93, 16626, \ldots, 94931)$
alexius	$(15476, 51443, \ldots, 88429)$
baba13	$(3, 62107, \ldots, 91233)$
$\vdots$	$\vdots$
zack_tayland	$(1009, 23471, \ldots, 47623)$
zoom42	$(63, 51234, \ldots, 72382)$

Table -2 Password file f2

S_I	S_H
3	$H(p_3)$
7	$H(p_7)$
85	$H(p_{85})$
$\vdots$	$\vdots$
100000	$H(p_{100000})$
100004	$H(p_{100004})$

4. CONCLUSIONS

After survey system ake difficult to attacker to get password from honeywords,which is based on honeyindexing. System architecture is finalized by using Hybrid Technique. Fake passwords means honeywords to detecting an attacks against DOS attack. In future scope after detecting the password.disclosure then at the same time user accounts update.

5. REFERENCES

[1]. 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. 145160.
[2] D. Mirante and C. Justin, Understanding Password Database Compromises, Dept. of Computer Science and Engineering Polytechnic Inst. Of NYU, Tech. Rep. TR-CSE-2013-02, 2013.
[3] M.Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, Password Cracking Using Probabilistic Context-Free Grammars, in Security and Privacy, 30th IEEE Symposium on. IEEE, 2009, pp. 391405
[4] F. Cohen, The Use of Deception Techniques: Honeypots and Decoys, Handbook of Information Security, vol. 3, pp. 646655, 2006.
[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. 145160.

[6] C. Herley and D. Florencio, Protecting financial institutions from bruteforce attacks, in SEC08, 2008, pp. 681685.
[7] A. Pathak, An Analysis of Various Tools, Methods and Systems to Generate Fake Accounts for Social Media, Ph.D. dissertation, Northeastern
University Boston, 2014.
[8] D. Nagamalai, B. C. Dhinakaran, and J. K. Lee, An In-depth Analysis of Spam and Spammers, arXiv preprint arXiv:1012.1665, 2010.
[9] C. Biever, Project Honeypot to Trap Spammers, New scientist, no. 2485,