International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | March 2019 www.irjet.net p-ISSN: 2395-0072

Honeywords: A New Approach for Enhancing Security

Lanjulkar Pritee[1], Ingle Rupali[2], Lonkar Arti[3], Ingle Vaishnavi[4]

[1,2,3,4]*Dept. of Computer Science and Enginerring, Padm.Dr.V.B.K.COE, Maharashtra, India.*

Abstract – *Every year new approach against cyber security threats are introduced. There are many issues related to data security so providing a strong security of our data. So there is one of the important security problem is with disclosure of password. To overcome this problem, we introduce a new concept of honeyword (consecutive or fake password). In this system for each user account the real password is stored with honeyword. In this system, user can perform the registration and for that purpose it's require user id and password to register in system. For every account we create a new honey index and this honey index can store with hash value. When user can login system check password, if it is match user can login. Honey checker stores the correct index for each account and the main purpose of honey checker is , if password is true or not, if it is true user can access the system. After successful login, user can perform any transaction through system. In our system, if the number of attempts more than count of three or entered password other than honeywords then the access will be issued but the files available will be decoy files.*

Key Words: Authentication, honeypot, honeywords, login, passwords, password cracking, security etc.

1. INTRODUCTION

In authentication process it becomes difficult to handle security of passwords that's why password became the most important asset to authenticate. But users choose the passwords that are easy to remember that can be predicted by the attacker using different attacks like brute force, dictionary, rainbow table attacks etc. So Honeywords plays an important role to defence against stole password files. Specifically, fake passwords placed in the password file of an authentication server.

In this paper we focus on the two issues that should be consider to be overcome this security problem:

First, Password must be protected by taking appropriate precaution and storing with their hash values computed through salting or some other complex mechanism. Hence, for an adversary it must be hard to invert hashes to acquire plain text password.

Second, A secure system should detect whether a password file disclosure incident happened or not to take appropriate action on the latter issue and deal with fake password or accounts as a simple and cost effective solution to detect compromise of passwords.

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 the passwords disclosure, if any one of the honeypot passwords gets used. According to the study, for each user incorrect login attempts with some passwords lead to honeypot accounts, i.e. malicious behavior is recognized. For instance ,there are 108 possibilities for a 8-digit password and let system links 10000 wrong password to honeypot account, so the adversary performing the brute-force attack 10000 times more likely to hit a honeypot account than the genuine account.

In this model the fake password sets are stored with the real user password set to conceal the real passwords, thereby forcing and adversary to carry out a considerable amount of online work before getting the correct information. Basically, for each user name a set of sweet words is constructed such that only one element is the correct password and the others are honeywords (decoy password). Hence, when an adversary tries to enter into the system with a honey word, an alarm is triggered to notify the administrator about a password leakage.

2. LITERATURE REVIEW

1. Avanish Pathak, "An analysis of various tools, methods and systems to generate fake accounts for social media," in Northeastern University Boston, Massachusetts December 2014.

- To study the mechanisms used by modern account creation programs and their overall effectiveness.
- This study analyzes the different ways in which these 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.
- Tests that reveal the number of accounts that can be fabricated prior to an OSN‟s countermeasures and their longevity due to the inability of the
- OSN‟s detection mechanisms are presented.
- This study highlights whether major websites are following security best practices to mitigate fake account creation, and if existing security countermeasures are effective.
- Major Websites provide critical functionality to billions of Internet users every day. However, some

users will always try to abuse these websites and exploit their resources for personal or commercial gain. The tools we examined give us a cogent understanding of how easy it is to fabricate fake accounts on these services. These fake accounts make their way onto underground market places where they can be cheaply purchased, and used to launch attacks like spam, political censorship, and black hat SEO. The wide availability of account creation tools is proof that miscreants will find a mechanism to bypass any countermeasure put forward by websites.

- Social spam campaigns can have a variety of objectives. The most obvious uses are promoting shady e-commerce sites, foreign pharmaceuticals, surveys, and scams i.e. the same kinds of content found in email spam.
- Social spam may also be used to spread malicious social applications that leverage the graph structure of OSNs propagate from friend to friend To give an idea of the scope of this problem: 8% of 25 million URLs that are posted to Twitter point to sites that are known for phishing, scams, or malware. Unfortunately it has been shown that 90% of the visitors click on these malicious links before they are blacklisted by OSNs.
- Another spam phenomenon that is unique to social networks is the manipulation of trending topics. Trending topics are highlighted by many OSNs, and receive many clicks and views. Thus, attackers often use fake accounts to try and create their own trending topics, or inject spam content into existing trending topics.

2. R. Butler and M.J. Butler "An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers" in Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014).

- Research suggests that passwords breaches are frequently the result of poor user security behavior. Internationally, poor password behavior among users is common.
- The objective of this study was to investigate the password performance of South African online consumers and to understand the factors contributing to poor password performance.
- A web-based survey was designed to determine online consumers‟ perceptions of their password-related knowledge, measure their ability to apply safe practices and assess their motivational levels to employ secure practices. Poor password practices among South African online consumers were evident from this study. Using a construct for password performance, this analysis indicated a deficiency in the knowledge, capability and motivation of users.
- Human computer interface and relevant education, training and awareness programs are required to protect password it time consuming and not 100 % correctness that password Wright and secure.

3. Gilbert Notoatmodjo and Clark Thomborson "Passwords and Perceptions" Department of Computer Science the University of Auckland Auckland, New Zealand Proc. 7th Australasian Information Security Conference (AISC 2009), Wellington, New Zealand.

- The security of many computer systems hinges on the secrecy of a single word – if an adversary obtains knowledge of a password, they will gain access to the resources controlled by this password.
- Human users are the „weakest link‟ in password control, due to our propensity to reuse passwords and to create weak ones. Policies which forbid such unsafe password practices are often violated, even if these policies are well-advertised.
- We have studied how users perceive their accounts and their passwords. Our participants mentally classified their accounts and passwords into a few groups, based on a small number of perceived similarities.
- Our participants used stronger passwords, and reused passwords less, in account groups which they considered more important. Our participants thus demonstrated awareness of the basic tenets of password safety, but they did not behave safely in all respects.
- Almost half of our participants reused at least one of the passwords in their high-importance accounts. Our findings add to the body of evidence that a typical computer user suffers from „password overload‟. Our concepts of password and account grouping point the way toward more intuitive user interfaces for password and account-management systems.
- This paper study shows how users become aware of their accounts and their passwords. They created cluster of user depending on the known similarities Participants used robust passwords, and not use repeated password.
- Every user is not aware of the security of passwords, and entering passwords are not user-friendly user's still need education and assistance when choosing passwords for important accounts.

3. PROPOSED SYSTEM

In this model, user can perform the registration and for that purpose it's require user id and password to register in system. For every account we create a new honey index and this honey index can store with hash value. When user can

login system check password, if it is match user can login. Honey checker stores the correct index for each account and the main purpose of honey checker is if password is true or not, if it is true user can access the system. After successful login user can perform any transaction through system. If attacker tries to hack the user account with different password, if attacker tries more than or 3 attempt then account was directly blocked and user can receive the alert message.

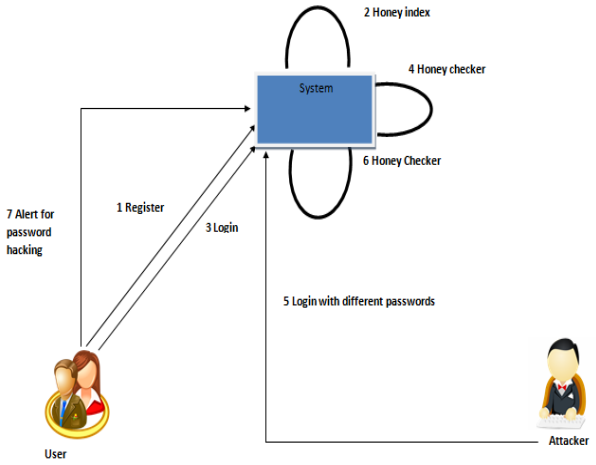

Fig: System Architecture

3.1 Honeyword:

Honeywords concept of Juels and Rivest is totally based on the generation of honeywords which is done by Gen ( ) algorithm and this is easy to crack and find the correct password. For generating these Honeywords Juels and Rivest 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**.**

3.2Honeyindex:

Instead of honeywords we use honeyindexes, for every account we created a new and unique honey index. The correct honey index is store with the hash of the correct password in a list.

3.3Login:

Here user is going to Login into the System. If password matches with the hash password then user can Login

3.4Honeyword Creation:

After login into the system, system crate honeywords using existing user Account passwords

3.5 Honeychecker:

Stores the correct index for each account and the main purpose of honey checker is if password is true or not, if it is true user can access the system.

3.6 Transaction:

After successful login user can perform any transaction through system.

3.7 Attacker:

Here attacker login to the system. Here if attacker tries to access the system and if he enters any honeyword then the notification or alert message is given to the Actual user.

4. ALGORITHM

Model algorithm for honey Random Generation

Inputs:

- words between [1-26 letter],
- Chose the random functions and its limit.
- Random value generation.
- Convert the random ascii value to its corresponding letter.

Output:

- Random cipher text of original password.

Step 1 =Honey pots creation: fake user account

1] For each account honey index set is created like

Xi= (xi; 1; xi; 2;: : : ; xi;k); one of the elements in Xi is the correct index (sugar index) as ci

2] Create two password file file f1 and file f2

- F1 Store username and honeywords set <hui,xi) Where hui is honey pot account
- F2 keeps the index number and the corresponding hash of the password(create the hash of the password), < ci;H(pi) >

Step 2=Generation of honeywords set

Gen (k; SI) -> ci; Xi

Generate Xi

1] Select xi randomly selecting k-1 numbers from SI and also randomly picking a number ci SI .

2] ui; ci pair is delivered to the honey checker and F1, F2 files are updated.

Step 3=Honey checker

Set: ci, ui

Sets correct password index ci for the user ui

Check: ui, j

Checks whether ci for ui is equal to given j. Returns the result and if equality does not hold, notifies system a honey word situation.

5. CONCLUSIONS

We have analyzed the security of the honeyword system and addressed a number of flaws that need to be handled before successful realization of the scheme. In this respect, we have pointed out that the strength of the honeyword system directly depends on the generation algorithm finally; we have presented a new approach to make the generation algorithm as close as to human nature by generating honeywords with randomly picking passwords that belong to other users in the system.

We have compared the proposed model with other methods with respect to DoS resistance, flatness, and storage cost and usability properties. The comparisons have indicated that our scheme has advantages over the chaffing with-a-password model in terms of storage, flatness and usability.

REFERENCES

[1] Avanish Pathak, "An analysis of various tools, methods and systems to generate fake accounts for social media," in Northeastern University Boston, Massachusetts December 2014.
[2] R. Butler and M.J. Butler "An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers" in Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)
[3] Ari Juels RSA Labs Cambridge, MA 02142,Ronald L. Rivest MIT CSAIL Cambridge, MA 02139 "Honeywords: Making Password- Cracking Detectable" May 2, 2013 Version 2.0
[4] K. Brown, "The Dangers of Weak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.
[5] 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. 391–405.
[6] F. Cohen, "The Use of Deception Techniques: Honeypots and Decoys," Handbook of Information Security, vol. 3, pp. 646–655, 2006.
[7] C. Herley and D. Florencio, "Protecting financial institutions from brute- force attacks," in SEC"08, 2008, pp. 681–685.
[8] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss- resistant Password Management," in Computer Security–ESORICS 2010. Springer, 2010, pp. sss286–302.
[9] Juels and R.L. Rivest, "Honeywords: Making Password tracking 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].
[10] 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.
[11] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 284 - 295, February 2015.

BIOGRAPHICS

Pritee V. Lanjulkar, Student of B.E Final year from Computer Science & Engineering Department

Rupali V.Ingle, Student of B.E Final year from Computer Science & Engineering Department

Arti P. Lonkar, Student of B.E Final year from Computer Science & Engineering Department

Vaishnavi R. Ingle, Student of B.E Final year from Computer Science & Engineering Department