Securing Internet Banking Transaction using Honeypot Algorithm

Dr. K. Karuppasamy[1] N. Priyadharshini[2] T. Ramya[3]
[1]Head of Department [2,3]UG Student
[1,2,3]Department of Computer Science & Engineering
[1,2,3]RVS College of Engineering & Technology, Coimbatore, India

Abstract— To detect attack against the hashed password databases using honeypot algorithm. For every user account the legitimate password is stored as several honey words in order to sense impersonation. If honey words are selected and processed properly then cyber attacker who steals a password cannot be sure if it is a real password or a honey word for any account. Moreover while entering through honey word login will trigger an alarm by notifying the Administrator out the password breach. We propose to minimize or overcome these problems by performing the makeover of real online banking system into a large honeypot armed with honey tokens. At the expense of increasing storage requirements, we introduce a simple and effective solution of password file disclosure events. In this study, we suggest an alternative approach that selects the honey words from existing user passwords in order to provide realistic honey words – perfectly a flat honey word generation and also to reduce storage cost of honey word scheme.

Key words: Password, Honeywords, Honeytokens, Administrator, Login

I. INTRODUCTION

Disclosure of password files is a severe security problem that has been affected millions of users. Indeed once the password file is stolen by using any of password cracking techniques it will be easy to capture many of user's plaintext password. In this system there are mainly two issues that should be concentrated to overcome this security problems: First issue is, password must be protected by taking appropriate precautions and storing their hash values which will be computed through salting or through any other highly complex mechanisms, By this it will it will be hard to inverse or convert it into plain text. Second issue is that a secure system should detect whether the password file disclosure incident happened or not then only appropriate actions will be taken.

This idea has been modified by Herley and Florencio to protect online banking accounts from password brute-force attacks. 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 accounts, so the adversary performing the brute-force attack 10000 times more likely to hit a honeypot account than the genuine account. Use of decoys for building theft-resistant was introduced by Bojinov .In this model, the fake password sets are stored with the real user password set to conceal the real passwords, thereby forcing an adversary to carry out a considerable amount of online work before getting the correct information. Recently, Juels and Rivest have presented the honey word mechanism to detect an adversary who attempts to login with cracked passwords. Basically, for each username a set of sweet words is constructed such that only one element is the correct password and the others are honeywords (decoypasswords).Hence, when an Hacker or third party tries to enter into the system with a honeyword, an alarm is triggered to notify the administrator about a password leakage.

In this study, we analyze the honeyword approach and to give some remarks about the security of the system. Furthermore, we point out that the key item for this method is the generation algorithm of the honeywords such that it is indistinguishable from the correct passwords. Moreover, this technique also reduces the storage cost compared with the honeyword method. Therefore, here the fake password sets are stored with real user password set to conceal the real password therby forcing an adversary to carry out a considerable amount of online work before getting the correct information.

II. LITERATURE SURVEY

A. Title: The Use Deception Techniques Honeypots & Decoys

Author: F.Cohen
Year: 2006
Description: Honeypot and its similar sorts of decoys represent only the most rudimentary uses of deception in protection of information systems. But because of their relative popularity and cultural interest, they have gained substantial attention in a research and commercial communities. In this paper we introduce honeypots and similar sort of decoys, and also discuss their historical use in defence of information systems, and describe some of their uses today. We will then go into a bit of the theory behind deceptions, and discuss their limitation and put them in the greater context of information protection.

B. Title: Protecting Financial Institutions from Brute-Force Attacks

Author: C.Herly and D.Florencio
Year: 2008
Description: The majority of banking and financial institutions in US authenticate users with a simple user ID-Password pair, the main encouragement for brute-force attackers is a notorious weakness of user-chosen password, observed three decades ago by Morris and Thompson. A more recent study of web password habits by Florencio and Herly showed that weak passwords are still very common. Break-ins are a problem because it can be hard to tell the fraudulent activity in a account resulting from a break-in in from the legitimate activity of an account owner. By allowing the attacker into many honeypots for every one real account we will learn detailed information on his strategy both for cash out and to tell honeypots from real accounts. Such that Denial of Service hole that lockouts create. The lockout policy opens a Denial of service vulnerability and it points out a very issue serious issue for some classes of accounts.

C. Title: The science of guessing: Analyzing an anonymised corpus of 70 million passwords

Author: J.Bonneau
Year: 2012
Description: Text passwords have dominated human-computer authentication. In 1960s the security researchers derived with multi evaluators singling passwords and found out as a weak point in the 1970s.Though many password cracking studies have supported this claim that there no consensus on the actual level of security. The security literature lacks sound methodology to answer elementary questions such as "do older users or younger users choose better passwords". The mass development of passwords on the passwords on the Internet may provide sufficient data to address these questions. Password corpora have typically been analysed by simulating adversarial password cracking leading to sophisticated cracking libraries but limited understanding of the underlying distribution of passwords.

D. Title: Explicit Authentication Response Considered Harmful

Author: L.Zhao and M.Mannan
Year: 2013
Description: Automated online password guessing is a long-standing problem for password-based authentication. Nowadys, this problem is possibly getting worse for reasons including the following. The growth of underground market for stolen credentials i.e attackers can turn stolen passwords into tangible profits, e,g, long standing facebook profiles, gmail accounts, highly reputed paypal accounts. In many cases user accounts are not as readily replaceable as in a past create a new account if the old one is compromised and the user chosen password are not getting better in terms of complexity. New services requiring passwords are emerging, causing password fatigue or sharing across sites, Also the increasing number of online participants makes the use of common passwords more possible, therefore attackers are getting more organized than before and have access to better tools and crackers; for eg the now maintain more robustness and also can use better techniques than just brute-forcing, optimized dictionary attacks.

III. PROBLEM DEFINITION

The password file is stolen at once means then by using any of password cracking techniques nit is easy to capture most of the plain texts easily. The tentative password indexes a hacker to make correct guess and cannot be easily sure about which one is an correct one.

IV. METHODOLOGY

A. Honeyword Generation Methods

1) Chaffing-By-Tweaking

In this method, the user password seeds the generator algorithm which tweaks selected character positions of the real password to produce the honey words. For instance, each character of a user password in predetermined positions is replaced by a randomly chosen character of the same type: digits are replaced by digits, letters are replaced by letters, and special characters by special characters. Number of positions to be tweaked, denoted as t should depend on system policy. For example t = 3 and tweaking last t characters may be a method for the 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.

2) Chaffing-With-A-Password-Model

In this approach, the generator algorithm takes the password from the user and relying on a probabilistic model of real passwords and it produces the honeywords. The authors give the model of as an example for this method named as the modeling syntax. In this model, the password is splitted into character sets. For example considering the password as a mice3blind is decomposed as 4-letters + 1-digit + 5-letters i.e(L4+D1+L5) and replaced with the same composition like gold5rings as a same format as a example.

3) Chaffing with "Tough Nuts"

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, For e.g. fixed length random bit strings should be set as the hash value of a honeyword. An illustrative example for a tough nut is given as '9,50PEe [KV.0?RIOtcL-:IJ"b+Wol¡*]!NWT/pb'. It is stated that the 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 attacker thereby deterring the adversary to realize her attack.

B. Architecture Diagram

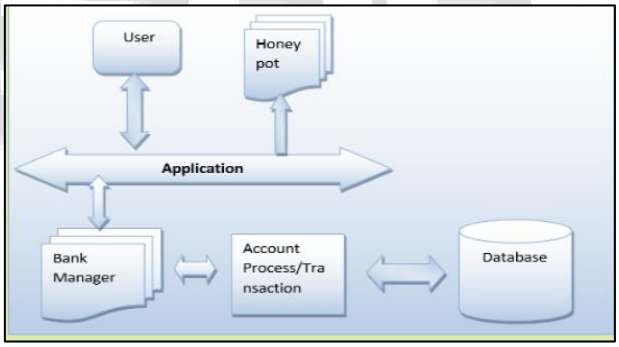

Fig. 1:

V. SYSTEM MODULES

A. User Registration & Authentication

When the user is new then they have to register by providing necessary details, after registration process user have to login through his unique username and password, if login success then it takes the user to next page or else remain in same page.

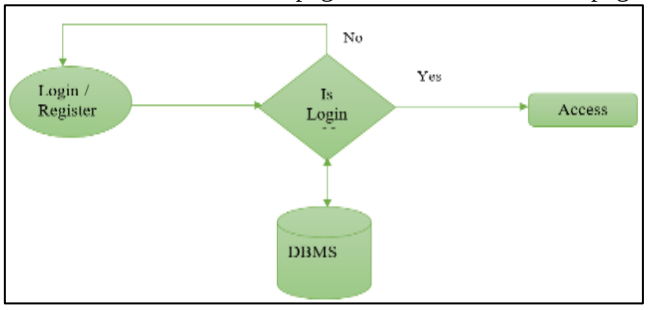

Fig. 2:

B. Hash Password

After registering their account details it will be stored in database. But for the security purpose we are using honeypots to store the password as hash password. We can see the password normally it will be stored in different tables and different format.

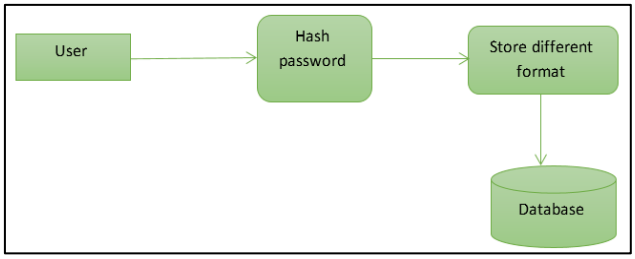

Fig. 3:

C. Money Transaction

The user have to transfer the money to any other account means then they should login the transaction process to transfer an amount. By the unique username and password the user will login and transfer the amount.so at that particular time also the password stored in database will be much secured with the help of generating honeyword mechanism.

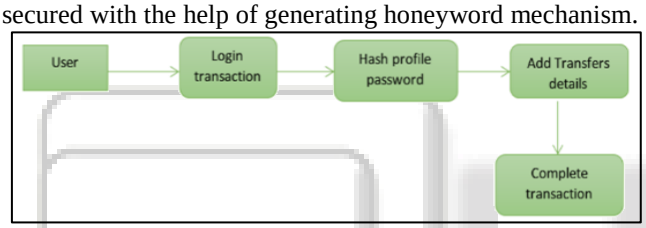

Fig. 4:

VI. RESULT

Therefore in future concept if unauthorized person trying to transfer money to other amount means we can find out and also can block transaction process, we should 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 from leaked password hash file. Hence by developing such methods both of two security objective such as increasing the total effort in recovering plaintext passwords from the hashed lists and detecting the password disclosure also provided at a same time.

VII. CONCLUSION

We have compared the proposed model with other methods with respect to DOS resistance, flatness, and storage cost and usability properties. The comparisions made in some of surveys specifies to have indication that our scheme has advantages in terms of storage, flatness and usability. Hybrid generation algorithm also make the total hash inversion process harder for a hacker in getting the password in plaintext from a leaked password hash file. Hence by developing such methods by two security objectives-increasing the total effort in recovering the plaimtext password from a hashed lists and detecting the password disclosure can be provided.

REFERENCES

[1] 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.
[2] Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times, vol. 20, 2010.
[3] K. Brown, "The Dangers ofWeak Hashes," SANS Institute InfoSec Reading Room, Tech. Rep., 2013.
[4] 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.
[5] F. Cohen, "The Use of Deception Techniques: Honeypots and Decoys," Handbook of Information Security, vol. 3, pp. 646–655, 2006.
[6] M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, "Improving Security using Deception," Center for Education and Research Information Assurance and Security, Purdue University, Tech. Rep. CERIAS Tech Report 2013.
[7] 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. 286–302.
[9] Juels and R. L. Rivest, "Honeywords: Making Passwordcracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security.
[10] M. Burnett, "The Pathetic Reality of Adobe Password Hints".

