IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Security Analysis of Honey words Generation Scheme to Evade Unauthorized Access

Ms. Manisha B. Kale[1], Prof. D. V. Jadhav[2]

Department of Computer Engineering, Zeal College of Engineering and Research, Pune, India[1, 2]

Abstract: 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.

Keywords: Honey word; Authentication; Decoy Document; Tweaking-digits; Hybrid.

I. INTRODUCTION

Generally, the software industries and companies stored their data in database [6]. For using a system requires user name and password which are stored in encrypt form in database. If a password file is stolen, by using the password cracking technique it is easy to get most of the Plaintext passwords. So for avoiding it, there are two issues that overcome these security problems: First, passwords must be protected and secure by using the appropriate algorithm. And the second one is that a secure system should detect the entry of unauthorized user in the System. In the existing system focus on the creating honeyword for the password and give security to the password file. In existing system first give the security to the password file as making password file hashed. But the getting plain text from the hashed file is easy so the in next system the concept of honeyword generation is come. In that system it gives false password with correct password and hashed this file. But only the security provided to the password file is not sufficient so the security provide to the document itself is the important one. So in the proposed system we focus on the honeywords i.e. Fake words for the document. The administrator purposely creates user accounts and detects a password disclosure; if any one gives the any wrong information at the time of login it is easily to detect the admin. According to the study, for each user incorrect login attempts and alarm gives to admin, i.e. malicious behavior is recognized. In proposed system, we create the honey document when the unauthorized user is detected. We analyze the honeyword approach and give some remarks about the security of the system. When unauthorized user attempts to enter the system and get access the database, the alarm is triggered and gets notification to the administrator, since that time unauthorized user get decoy documents. I.e. fake database.

A. Honeywords

A simple but clever idea is the insertion of false words called as honey words associated with each user's account. When an adversary gets the password file, she recovers many passwords because of creating false words (honeywords) for each account and she cannot be sure about which password is correct. Hence, the cracked password files can be detected by the system administrator if a login attempt is done with a honey word by the adversary. Honey word generator algorithm Gen(). Note that strength and effectiveness of the method is directly related to how the Generator algorithm is constructed. Therefore, the authors introduce a definition as the flatness of algorithm such that it measures the chance of an adversary in picking the correct password from the sweet words[1].Because the chance of getting correct password in existing system, in proposed work we generate honey word for the document which is attacked by attacker. Here we change the content of the document mean generate honey words for the words in that document.

B. Decoy Documents

Decoy document is nothing but the false document means that document which contains bogus information instead of original data. And this document is generated only when any abnormal information access is detected. With the decoy document we confusing attacker.

C. Honey word Generation Methods and Discussions

The authors [2] categorize the honey word generation methods into two groups. i.e The first category consists of the legacy-UI (user interface) procedures and the second one is modified-UI procedures whose password-change UI is modified to allow better password/honeyword generation. Take-a-tail method is given as an example of the second category. According to this approach a randomly selected tail is produced for the user to append this suffix to her entered password and the result becomes her new password means honeyword. Let a user enter password sport01, and then system let propose '143' as a tail. So the password of the user now becomes

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

sport01143.Although this method strength the password, to our point of view, it is impractical – some users even forget the passwords that they determined. Therefore in the remaining parts, the analysis that we conducted is limited with the legacy-UI method.

D. Hybrid Method

Another method discussed in is combining the strength of different honeyword generation methods, e.g. chaffing-with-a-tweaking-model and chaffing-by-tweaking digits. By using this technique, random password model will yield seeds for tweaking-digits to generate honeywords. In chaffing-by-tweaking method the user password seeds the generator algorithm which tweaks selected character position of the real password for produce the honeywords. Each character of a user password in predetermined positions is replaced by a randomly chosen character of the same type like digit is replaced by digit, letter by letter and special character by special character. Number of positions be replaced is denoted by t.eg..t=3 method for generator algorithm is Gen(k,t) .Another approach is chaffing-by-tweaking digits eg. Password is 23games and t=2 the honeywords are 56games, 77games may be generated [1].

In hybrid method eg. Let correct password be missu3457 then the honeywords can be happy6546, angle3452, apple8761 should be produce as seeds to chaffing-by-tweaking digits. For t = 3 and k = 4 for each seed, the honey word table given below may be:

happy3422	missu1234	apple9876
happy1254	missu3457	apple3276
happy9867	missu6534	apple6345
happy2365	missu1234	apple5234

II.RELATED WORK

Imran E regular [1] said how the honey word is made come into existence the password is stored in honeyword form. The password text record i.e. false password, text record is able to be seen to the computer expert for pleasure, and this is the have rights to (reward) of that systems. In this system the password of the other accounts password is taking as the honeyword. Because of that the honeyword is like as the natural password so the guessing correct password from file is made difficult and also the it require the less space for storing honeyword because in the other method the honeyword is generated other than password. But here password of other account is used as the honeyword. But in this system some drawback has come to mind after the use of this system ,like less checking to make certain process ,is used as in this system ,so all this come to belief by reasoning we make come into existence our proposed System is used for the securing personal and business data.

Juels and Rivest [2] suggested approach which is extending the basic idea of honeyword and also the legitimate accounts, by giving multiple passwords for each account from that the only one password is correct and other used as honeywords. In this system they use honeychecker which is server. If user give the correct password no matter. But if the hashed password file is stolen by the adversary and convert into hash function. But there is effort require for the getting correct password because in this file the honeywords is also stored with the password. At the time of login if adversary enters any honeyword then it check with the honeychecker if the entered password is from the honeypot then set off an alarm. This method directed to stolen files of password hashes attack scenarios. In this system the take a tail method is used for honey word generation. eg(if password is thankyou then honeywords like the thankyou123,thankyou654 ..etc. here 123 and 654 are tail.) .But some attacks possible against this method like general password guessing, targeted password guessing and attacking the honeychecker. It forces the attacker to brute force the hashes one at a time by a D. Mirante and C. justin [7] instead of attacking them as a group.

It provide flexibility with the ability to provide resources. But high seen from the internet-site whereas user login credentials and other facts were put at risk. Thus a work was undertaken to make observations and further research. Cormac Herley describe the how financial institute protecting from brute force attacks. In this paper [6] they give idea of the create large number of honeypot userID-password pairs. In this method if attacker is logged in any honeypot account with fictitious attribute. For getting the account is real or honeyaccount the attacker must attempt to money transfer out. The simplest is directed against a single account: the attacker tries all possible passwords for one user ID until one succeeds. The activity of the attacker in honeypots provide data by which bank get the account is attacked and give information about that to the real account.

This paper introduce a new approach that Password Cracking Using Probabilistic Context-Free Grammars[3]. This grammar allows us to generate word mangling rules, and from them, password guesses to be used in password cracking. our approach was able to crack 28% to 129% more passwords than John the Ripper, a publicly available standard password cracking program. Advantage is this approach seems to provide a more effective way to crack passwords as compared to traditional methods. Disadvantage is approach was able to crack 28%.

This paper described a approach of deception techniques have the demonstrated ability to increase attacker workload and reduce attacker effectiveness. This article has summarized a great deal of information on the history of honeypots and decoys for use in defense of computer systems. Merit of this paper system is The most critical work that must be done in order to make progress is the systematic study of the effectiveness of deception techniques against combined systems with people and computers. Disadvantage is Modern defensive computer deceptions are in their infancy, but they are moderately effective, even in this simplistic state[4].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

III. PROBLEM STATEMENT

To provide the security at time of accessing data, Security is provided by using the honeyword generation method and also detect entry of adversary in system.

IV.PROPOSED WORK

Existing system mainly focus on only the how honeywords are generated. It doesn't provide the other security. In proposed work We propose a different approach for securing data in the system using decoy technology. We monitor data access in the system and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the users real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a System environment. We propose a completely different approach to securing the system using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake data. The proposed method of SECCURE novel honeyword generation approach To reduces the storage overhead can be describe efficiently according to this steps, which is depicted the fig 1.

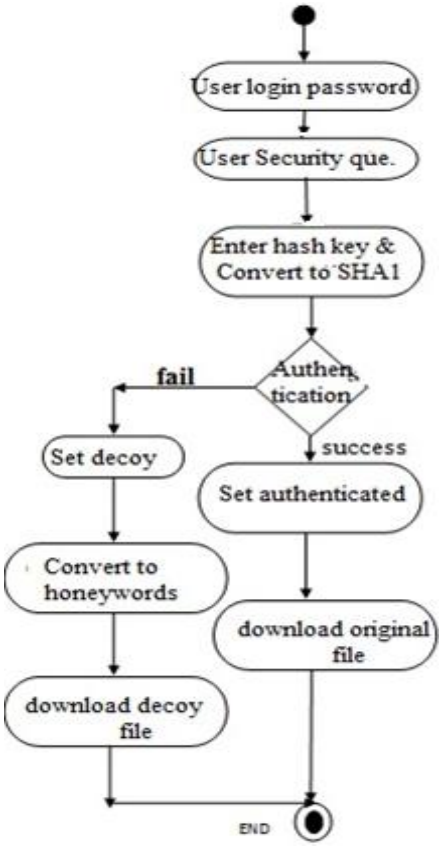

Fig. 1 System Flow

Step 1: user wants to take any file then system asks the username and password. If the password is correct go to next step. But username or password is wrong goes to step 8.
Step 2: Then ask the security question answer may or may not right also goes to next step.
Step 3: Then ask to enter hash value and it convert into SHA-1 value. if the enter value and the database value is same then it getting that user is authenticated.
Step 4: Here check authentication means in all above step the user give right answer means the authentication is success it is able to go further. If authentication is fail then go to step 5.

Step 4.1: Set as authenticated.

Step4.2: Able to download or see the original content of document.

Step 5: Set decoy in this step.
Step 6: Then convert document content to the honeywords.
Step 7: Then attacker get the decoy document not original.
Step 8: Stop.
After this entire steps the attacker not getting that he catch. He thinks that he got the original document. But when authentication fail that time administrator get the attacker attempt and get all the information about that attacker like the physical address, IP address etc..And the take appropriate action.

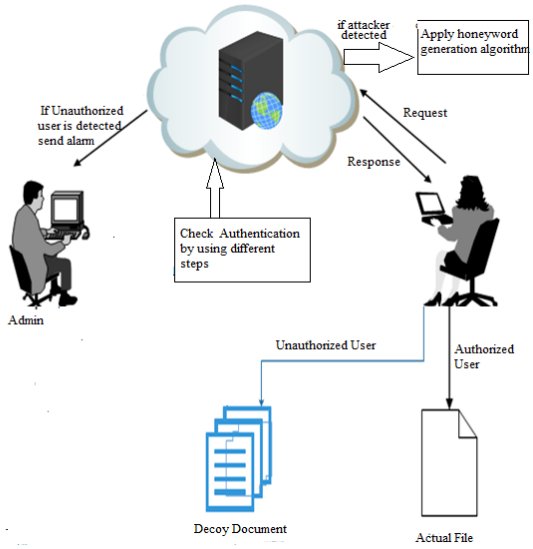

Fig.2 System Overview

V.MATHEMATICAL MODEL

Input: Enter the document name or file which you want.
Output: If user is authorized he get original file. Else original file is converted in the fake file and this file is get by the attacker.

Let us consider we have database 'D' and 'n' is the number of attribute such as user name, user ID etc.
D={A|A ε Information user}
Here D is the set of all A such that A is information of user which is stored on the server.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Consider function STORE (D, SERVER): Here admin enter the user information into the database at server.
Let us consider that the receiver provide us with value 'x' for every input it obtain from the every time login account of the particular user. So we can further assume to have a set to have value 'n' number of detect value at particular instance. Let us denote the current situation in the following manner.
S= {X|□ □ □ X ε DƎ ID for attacker}
Here S is the set all X such that for all X there exits Id for user.
Now for some x value that match with some value inside the database when admin check user account update.
1. GET (D, X, SERVER): Admin get all information about the, user account from server.
2. PUT(X, ATK, SERVER): Here admin will upload attacker information on server.
3. PUTP(X, REPORT, SERVER): Here admin upload daily report on server.

Initialize variables: h0=0x67452301

h1=0xEFCDAB89
h2=0x98BADCFE
h3=0x10325476
h4=0xC3D2E1F0

Initialize hash value for this chunk:
a=h0
b=h1
c=h2
d=h3
e=h4
Main loop
for j from 0 to 79
if 0≤ j≤19 then
f=(b and c) or ((not b)and d)
k=0x5A827999
else if 20≤ j ≤ 39
f=b xor c xor d
k=0x6ED9EBA1
else if 40 ≤ j ≤ 59
f=(b and c) or (b and d)
k=0xCA62C1D6
temp =(a left rotate 5) + f + e + k + w[j]
e=d
d=c
c=b left rotate 30
b=a
a=temp
Add this chunk's hash to result so far:
h0=h0+a
h1=h1+b
h2=h2+c
h3=h3+d
h4=h4+e

Produce the final hash value as a 160 bit number:
hh =(h0 left shift 128) or (h1 left shift 96) or (h2 left shift 64) or (h3 left shift 32) or h4

VI.RESULTS AND DISCUSSION

Weak DoS resistance means that an attacker can submit a honeyword given knowledge of the password with non-negligible probability. Medium DoS resistance means that attack may be possible or may not be possible all the time. Strong DoS resistance means that such attack is unbelievable. Multiple-system protection is the property that compromise of the same user's account in different systems will not immediately reveals distribution of honeywords generated by chaffing-with a tweaking-password-model. The storage costs assume generation of k -1 honeywords. From the above table we getting that the hybrid honeyword generation method is the best considering the all parameters. So in proposed system we use the Hybrid honeyword generation method.* indicates optimization technique is considered in storage cost calculation. In our system the storage cost required only for the number of words in document no any extra storage is required.

Table 1: Comparison of honey word-generation methods

Honey word	DOS Resistance	Storage	Flatness	Multiple method
Tweaking	weak	hN*	medium	No
Password as Honeyword	strong	4kN +hN + 4N	strong	No
Take-a-tail	strong	K	weak	Yes
Our Method	strong	k	strong	Yes
password model	strong	khN	strong	Yes

CONCLUSION

The proposed system helps to introduce an idea of the creating decoy document if the user is unauthorized which is generated by using Hybrid technique of honeyword generation. This technique also gives alarm and information about the attacker. But the attacker is unaware about that he is detected. This technique require minimum storage as compare to unlike existing systems because this technique generate decoy document only when unauthorized user is detected by system otherwise not necessary to generate decoy document. This system protects the data by using honey word and also detects an entry of an adversary in the system. In future work we try to give honey image, so it will provide the strongest security.

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University of Pune. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

REFERENCES

[1] Imran Erguler "Achieving Flatness: Selecting the Honeywords from Existing User Passwords". 10.1109/TDSC.2015.2406707, IEEE Transactions on Dependable and Secure Computing.
[2] 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.
[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. 391–405.
[4] F. Cohen, "The Use of Deception Techniques: Honeypots and Decoys," Handbook of Information Security, vol. 3, pp. 646–655, 2006.
[5] M. H meshekah, 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 2013-13, 2013.
[6] C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in SEC'08, 2008, pp. 681–685.
[7] 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.

BIOGRAPHY

Ms. Manisha B. Kale, is currently pursuing M.E (Computer) from Department of Computer Engineering, Dnyanganga College of Engineering and Research, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from S. B. Patil College of engineering, Indapur, Savitribai Phule Pune University, Pune, Maharashtra, India -411007. Her area of interest is information security.