Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Approach for High Level Security Using Honeywords

Prashant Dhas[1], Ismail Mohammed[2]
[1]Student, [2]Faculty
[1, 2] Alard College of Engineering and Management,
Pune, MH, India

Abstract: ***The new developments in the field of information technology offered the people enjoyment, comforts and convenience,but there are many security related issues. 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 stolen or theft by using the password cracking techniques and decryption technique it is easy to capture most of the plaintext and encrypt passwords. For troubleshoot this here we create the honeyword password, i.e. a False password using a perfectly flat honeyword generation method, and try to attract illegal or unauthorized user. Hence that time we detect the unauthorized user. Here we also protect the original data from unauthorized user.***
As mentioned above, in this project we have used Honeywords also called as Sweet Password Security Strategy.

Keyword: Honeywords, Honeypot, Login, OTP, Authentication, Password cracking, Passwords, Decoy Documents.

I. 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 honeywords i.e. fake passwords and accounts. The administrator purposely creates user accounts and detects a password disclosure, if any one of the honeypot 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 Honeypot accounts, i.e. malicious behavior is recognized. In proposed system, we create the password in plane text, and stored it with the fake password set. 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.

II. LITERATURE SURVEY

Imran Erguler said that how the honeyword is created; the password is stored in honeyword form. The password file i.e. false password file is visible to the hacker, and this is the Merits of that systems. But in this system some drawback has occur after the use of this system, like less authentication process, is used as in this system, so all this conclude we create our proposed System, is used present novel approach for securing personal andbusiness data[1].
Honeyword i.e. false password forces to attacker to brute force the hashes one at a time by a D.Miranteand C.Justin, instead of attacking them as a group. High profile website intrusion is occurred whereas user login credentials and other data were compromised. Thus a study was undertaken to research information posted on the web concerning recent, is done [2].
The Internet and Web technologies have originally been developed assuming an ideal world where all users are honorable. However, the dark side has emerged and bedeviled the world. This includes spam, malware, hacking, phishing, denial of service attacks, click fraud, invasion of privacy, defamation, frauds, violation of digital property rights, etc. The responses to the dark side of the Internet have included technologies, legislation, law enforcement, litigation, public awareness efforts, etc. In this paper, they have explored and provided taxonomies of the causes and costs of the attacks, and types of responses to the attacks [3].
There have been several high publicity password leaks over the past year including LinkedIn, Yahoo, and eHarmony. While you never want to have vulnerabilities that allow hackers to get access to your password hashes, you also want to make sure that if the hashes are compromised it is not easy for hackers to generate passwords from the hashes. As these leaks have demonstrated, large companies are using weak hashing mechanisms that make it easy to crack user passwords. In this paper they have discussed the basics of password [4].
Choosing the most effective word-mangling rules to use when performing a dictionary-based password cracking attack can be a difficult task. In this paper they have discussed a new method that generates password structures in highest

probability order. They have first automatically created a probabilistic context-free grammar based upon a training set of previously disclosed passwords. This grammar then allows us to generate word-mangling rules, and from them, password guesses to be used in password cracking. They also haveshown that this approach seems to provide a more effective way to crack passwords as compared to traditional methods by testing our tools and techniques on real password sets. In one series of experiments, training on a set of disclosed passwords, their approach was able to crack 28% to 129% more passwords than John the Ripper, a publicly available standard password cracking program [5].

III. PURPOSE AND SCOPE

- The main aim of project is to validating whether data access is authorized or not when abnormal information access is detected.
- Confusing the attacker with fake information.
- This protects against the misuse of the user's real data.
- We propose a completely different approach to securing the cloud 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 worthless data.

.

IV. PROJECT OBJECTIVE

The proposal is for "Making Data Inconspicuous In system" to avoid the attack of Insider on confidential and important data. We propose a simple method for improving the security of hashed passwords. The maintenance of additional "honeywords" (false passwords) associated with each user's account. An adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeyword. The attempted use of a honeyword for login sets off an alarm. An auxiliary server (the "honeychecker") can distinguish the user password from honeywords for the login routine, and will set off an alarm if a honeyword is submitted

V. MATHEMATICAL MODEL

Considering that we have database 'D' and 'n' number of attribute such as user name, user id etc.
D = {A|A ε Information of user}
Here D is the set of all A such that A is information of user which is to be store on server
Consider following function STORE (D, SERVER):

- Here admin enters the user information into 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 's 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 D ∃ 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's information on server.
3. UTP(X,REPORT,SERVER) : Here admin upload daily report on server.

VI. CONCLUSION AND FUTURE SCOPE

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 illegallyaccesses someone's documents in a system service. Decoy documents stored in the system alongside the user's real data also serve assensors 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. In the future, 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 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.

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] D. Mirante and C. Justin, "Understanding Password Database Compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TRCSE-2013-02, 2013.
[3] A. Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times,vol. 20, 2010.
[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 Probabilistic Context-Free Grammars," in Security and Privacy, 30th IEEE Symposium on. IEEE, 2009, pp. 391–405.

