International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Effective Approach to Detection of Password File Using Honeywords

Dipali Dhumal[1], Shyam Gupta[2]

[1]PG Student, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

[2]Professor, Computer Department, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

Abstract: ***Today"s technical world has improved a lot, but there are many security related issues. One of them is password files. password files has got a lot of security problem that has affected millions of users as well as many companies. password file is generally stored in encrypt 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.***

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

1. 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 encrypt 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.

2. Literature Survey

S. No	*Title*	*Name of author*	*Year*	*Publisher name*	*Techniques used*	*Advantages*	*Disadvantages*	*remarks*
1	Understanding Password Database Compromises	D.Mirante and C. Justin	2013	Department of Compute r Science and Engineer ing Polytech nic Institute of NYU	It forces the attacker to brute force the hashes one at a time, instead of attacking them as a group	offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown	high profile website intrusions, wherein user login credentials and other data were compromised	A study was undertaken to research information posted on the web concerning recent, high profile website intrusions
2	If Your Password is 123456, Just Make It Hackme	The Dangers of Weak Hashes	**2013**	SANS Institute InfoSec Reading Room, Tech. Rep., 2013	basics of password hashing, look at password cracking software and hardware, and discuss best practices for using hashes securely	hashes are compromised it is not easy for hackers to generate passwords from the hashes	Password leaks are becoming a common occurrence on the internet with several large scale leaks happing every year	• Don"t try to create your own hashing algorithm • Don"t use outdated algorithms (such as MD5 or SHA1) • Use SHA2 or similar strength algorithm

3	M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek	Password Cracking Using Probabili stic Context- Free Grammar s	2009	Password Cracking Using Probabili stic Context- Free Grammar s," in Security and Privacy,30th IEEE Symposi um on. IEEE,2009,	This grammar allows us to generate word-mangling rules, and from them, password guesses to be used in password cracking	This approach seems to provide a more effective way to crack passwords as compared to traditional methods	approach was able to crack 28%	our approach was able to crack 28% to 129% more passwords than John the Ripper, a publicly available standard password cracking program.
4	F. Cohen	The Use of Deception Techniques: Honeypots and Decoys	**2006**	Handboo k of Informati on Security, vol. 3, pp. 646–655, 2006	deception technique s have the demons t rated ability to increase attacker workload and reduce attacker effectiveness	The most critical work that must be done in order to make progress is the systematic study of the effectivenes s of deception techniques against combined systems with people and computers.	Modern defensive computer deceptions are in their infancy, but they are moderately effective, even in this simplistic state	This article has summarized a great deal of information on the history of honeypot s and decoys for use in defense of computer systems.
5	M.H. Almeshek ah , E. H. Spafford, and M. J. Atallah	Improving Security using Deception,	2013	Center for Education and Research Informati on Assuranc e and Security, Purdue Universit y, Tech. Rep. CERIAS Tech Report 2013-13, 2013	We explore complex relationships among protection techniques ranging from denial and isolation, to degradation and obfuscation, through negative information and deception, ending with adversary attribution and counter-operations.	outlined a new classification scheme for deception techniques in cyber security	have shown how some of these techniques have been known and used for many years, but that the field is under-developed	explained how systems can be augmented to use deception and false information to protect them and their data, to degrade attacks, to expose attackers, to enhance attribution, and possibly to be used to damage or degrade attacker capabilities.
6	C. Herley and D. Florencio	Protecting financial institutio ns from brute-force attacks	2008	Microsoft Research One Microsoft Way Redmond, WA	show that is simple to ensure that a brute-force attacker will encounter hundreds or even thousands of honeypot accounts for every real break-in.	activity in the honeypots provides the data by which the bank learns the attackers attempts to tell real from honeypot accounts, and his cash out strategy.	examine the problem of protecting online banking accounts from password brute-forcing attacks.	In a brute-force attack repeated credential pairs are tried in an attempt to gain access to an account. The simplest is directed against a single account: the attacker tries all possible passwords for one userID until one succeeds.
7	H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh	Kamouflage: Loss-resistant Password Manage ment	2008	Computer Security– ESORIC S 2010. Springer, 2010, pp. 286–302	Introduce Kamouage: a new architecture for building the ft-resistant password managers. An attacker who steals a laptop or cell phone with a Kamouage-based password manager is forced to carry out a considerable amount of online work before obtaining any user credentials.	replacement for the built-in Firefox password manager, and provide performance measurements and the results from experiments with large real- world password sets to evaluate the feasibility and effectiveness of our approach	presented a system to secure the password database on a mobile device from attacks that are often ignored by deployed password managers.	Kamouage is well suited to become a standard architecture for password managers on mo-

3. 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.

4. Project Objective

The proposal is for *"Making Data Inconspicuous In system"* based applications for the purpose 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.

5. 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

$S = \{X| \square \; X \varepsilon D \; \exists$ 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) PUTP(X,REPORT,SERVER) : Here admin upload daily report on server.

6. 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 illegally accesses someone‟s documents in a system service. Decoy documents stored in the system alongside the user‟s real data also serve as sensors 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 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 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] 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] A. Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times, vol. 20, 2010
[3] K. Brown, "The Dangers of Weak 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 2013-13, 2013.
[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. 286–302.
[9] 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. 145–160. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516671
[10] M. Burnett, "The Pathetic Reality of Adobe Password Hints," https://xato.net/windows- security/adobe-password-hints.