ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

SECURE USER AUTHENTICATION USING HONEYWORDS

M.S.Saravanan, A.K.SharathSanthosh
Professor, Department of CSE & IT, Saveetha School of Engineering, Saveetha University, Chennai, India
I-M.E, Department of Computer Science and Engineering, Saveetha School of Engineering,
Saveetha University, Chennai, India.
Email: saranenadu@gmail.com

Received on: 02.10.2016 *Accepted on: 28.10.2016*

Abstract

Nowadays when it comes to the field of security the common theme is that manyhashed password are vulnerable to hackers. The security of the password of a user faces too many security problems because, these passwords give the hacker a way to exploit or misuse the account without being detected. The only way the hacks can be found is when the damage is noticed by the users after logging into their accounts and notifies the changes. So the system provides very few or no detection mechanisms in order to detect the attacks against hashed password databases. In the year 2013, Mr. Ari Jules and Mr. Ronald L. Rivest came up with the idea of using Honey-words in the password file.A honey word is nothing but false password.

The honeyword approach is one where the real password is stored along with a certain amount of fake passwords in order to detect the presence of an attack. So when the attacker has the password file he might get confused as to what is the real password. When the honeyword is entered an alarm is triggered and a notification is sent to the administrator.

Keywords: Security, Vulnerable, Hackers, Password, Attack.

1. Introduction

When it comes to user account management the system should have strong password policies and it must detect attacks to password file before it harms the system. Disclosure of password files are a very serious security threat because once these password stolen the security of the entire system is in jeopardy because it exponentially increases the chances of the system being attacked. By the use of honeywords the admin purposefully creates fake passwords by using honeypots [1]. This is done in order to confuse the attacker and letting him to guess which the correct password might be. Honeypot is the mechanism which detects the presence of a hacker. So, when the hacker choses the honeyword instead of the real password the alarm is triggered and the admin of the system is alerted [2]. And also the advantage of using honeyword is that by the creation of a separate page for when the hacker uses a honeyword he can be tricked into thinking that he has gained access into the actual page which the system can in turn use to gain information from the hacker such as IP address, location etc. and can be sent to the administrator so that they can take the necessary actions. This approach is not very complex but yet it is very effective as it puts the hacker in the danger of being exposed .In this paper we look at what honeywords are how are honeywords generated and how they can be used to ensure the security of the passwords and ensuring user security [3].

2. The Overview of Attack Scenarios

There are many attack scenarios relating to passwords security attacks. These types of attack techniques are often utilized by the hacker in order to gain access to user accounts. These scenarios give us a brief idea of. Here six of such possibilities are given in order to get a brief idea about what type of attacks can the passwords can be subject to [4]. These scenarios help us in understanding how honeyword methodology is used to secure the system accounts they are:

A. Stolen Files of Password Hashes - Consider that an attacker is by one means or another ready to take the record of password hashes, and unravel for some passwords utilizing disconnected animal power calculation. He may all the more by and large have the capacity to take the secret key hash records on numerous frameworks or on one framework at different times [5].

B. Effectively Guessable Passwords - A considerable part of clients pick passwords so ineffectively that a foe can effectively imitate at any rate a few clients of a framework by endeavoring logins with basic passwords. Propose tending to this risk by obliging clients to utilize unprecedented passwords.

C. Visible Passwords- The client's secret word is traded off at the point when a foe sees it being entered (shoulder surfing), on the other hand a hacker sees it on a yellow stickier on a screen. A one-time secret key generator, for example, RSA's SecurID token gives great assurance against this risk.

D. Same Password for many Systems and Services - A user might use the same login information on different services or different systems. Considering that the account is no longer useful for logging in one system then it will also become useless in all the other systems.

E. Password Stolen from User - This scenario explains by itself. Here the hacker instead of attacking the system may compromise the end-point devices such as mobile laptops etc,.By compromising such devices the attacker might be able to learn about the user passwords and will have the power to misuse it.

F. Password Change Compromises - This scenario is one where the attacker learns the user passwords at the time when the user wants to change or modify the password as gaining knowledge about the password when being entered is much easier than gaining knowledge about the already existing password

3. The Working module of Honeyword and Honeychecker

In this section the honeywords and the honeychecker modules were introduced to identify the password hacking, through which the detected alert can be used for the user to get acknowledge for the effective care in any situation [6].

A. Honeyewords - The idea behind honeyword is a simple but effective one. It is nothing but the usage of fake passwords in order to trick the user into making a mistake by forcing him into making a mistake by making him guess the correct password from the honey pot and when the honeyword is chosen instead of the correct user password the hacker is being detected and the alert is sent to the administrator [7].

But it does not always detect the activity of a hacker the reason behind this is that if the attacker guesses the correct password then he is given access to the account and the attacker will gain access to the system without being detected and the security mechanisms will become ineffective. So in order to ensure that it does not happen proper encryption techniques should be performed.

The passwords that are present in the file are given in order to confuse the attacker but, we also know that these passwords are generated by the use of honeypot. When it comes to system generated password there is a risk of those passwords may not make any sense. So, when the attacker gets hold of the password the guessing of the password becomes much easier when the passwords are computer generated when they are compared with the password that a user might give [8]. Therefore there are certain honeyword generation techniques that are used in order to provide more realistic honeywords in order to confuse the hacker as much as it can. A.Jules and R.L.Rivest categorize the honeyword generation into two stages. The first stage involves the legacy-UI strategies also known as user-interface strategies and the second stage involves modified UI techniques which contains password change UI which can be modified to allow better password/honeyword generation [9].

B. Honeychecker - The honeychecker is assumed to be an auxiliary secure server in order to help with the usage of honeywords [10].The honeychecker is a different hardened PC framework where such mystery data can be put away. We accept that the PC framework can speak with the honeychecker when a login endeavor is made on the PC framework, or when a client changes her watchword.

We expect that this correspondence is encrypted and/or authenticated. The honeychecker ought to have broad instrumentation to distinguish inconsistencies of different sorts. The honeychecker also capable of producing alarms so when the honeychecker finds an instance where the honeyword is used the alarm is sent to the admin system and alerted. Depending on the policy chosen the honeychecker may or may not react to the admin system.

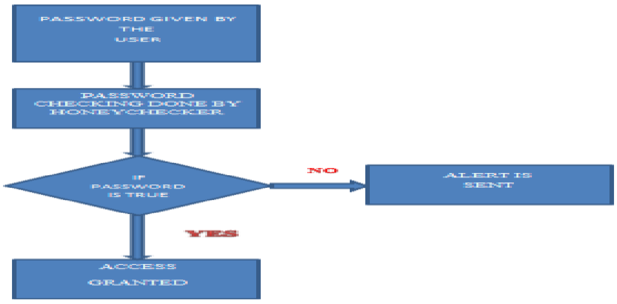
PASSWORD GIVEN BY THE USER
PASSWORD CHECKING DONE BY HONEYCHECKER
IF PASSWORD IS TRUE
NO
ALERT IS SENT
YES
ACCESS GRANTED

Figure 1. Honeyword working module.

In the above figure 1, it shown that the password entered by the user has given a password for a particular account. The authenticity of the password is checked by the honeychecker. If the password is the original one then the access is granted for that particular account and if the password entered is a honeyword then the honeychecker sends an alert to the admin about the presence of an attacker.

4. Honeyword Password Generation Methods

Honeyword generation methods can be classified into two types namely the Legacy-UI procedure and the Modified-UI procedure. In the Legacy-UI techniques the passwords change UI is unaltered i.e. it takes the same secret word entered by the client for honeyword generation.In the Modified UI method the password change UI is altered to permit better nectar word era. The client's genuine secret key is altered to end with an arbitrarily picked quality to structure another client secret word. Take-a-tail technique is an illustration of this classification.

A. Chaffing by tweaking-In this technique, the client password seeds the generator calculation which changes chose character positions of the genuine password to deliver the honeywords. Using chaffing by tweaking methodology, the utilizing customer secret key creates Honeywords. To begin with take secret word from client after that select position of character which ought to be from beginning or from terminating position. After the selection of that position we rearrange the characters from the password. There is some farthest point while era of honeyword in light of the fact that if it doesn't there is chance that honeywords distribute parts of the memory while creating honeywords. Each character of a user password in predetermined positions is supplanted by a discretionarily picked character of the same sort: digits are supplanted by digits, letters by letters, and outstanding characters by uncommon characters. There is each other system with respect to this strategy i.e. "teasing by-tweaking-digits". It changes the last t positions having digits. Regardless, various customers have the penchant to pick the secret word having one of a kind date. For example, birthdate, chronicled event or remembrance dates. In the end, chaffing by tweaking is used, it can offer sign to a foe to isolate the right secret key. In this way, teasing by tweaking is not prepared to fulfil the purposes of honeyword arrangement.

B. Chaffing-with-a-password model-In this approach, the generator algorithm takes the password from the client and depending on a probabilistic model of genuine passwords it creates the honeywords. This model permits the generator calculation to acknowledge the password from the client and to deliver the honeywords in view of a probabilistic model of genuine passwords. This model is given as a case for the strategy named as the demonstrating language structure. This model comprises of the password, broken into character sets. On the off chance that the username and the password are co-related, the password can be effortlessly recognized from the honeywords.

C. Chaffing with tough nuts- A tough nut can be defined as the extras text that is added to plain text.In this type of honeyword generation technique framework embed some intense word into the password, so it is hard to find the passwords from hash files. So at whatever point the password is embedded by client there is some unique string and salt with the correct password so around then it's hard to get unique secret key. Utilizing this strategy there is chance that aggressor disregard the intense nuts.

D. Hybrid method-The hybrid method is nothing but the technique of combining various honeyword generation techniques. With help of hybrid strategy creates more mind boggling honeywords which does not split effortlessly by adversary in light of the fact that each time enemy considers that one of honeyword generation technique so every time the hacker tries to break characterized philosophy yet it's hard to consider what number of system consolidates to produces honeyword.

5.Policy Choices for Password

5.1 Password eligibility: When a user is creating an account the system sometimes may not accept the password that was given by the user because it does not reach the eligibility criteria set by the administrator for the system .some of them are given below:

A.Password Syntax -A password might be required to have minimum length, inclusion of numbers or even adding a special symbol. So, when these rules are not followed then the system will reject the password given by the user.

B.Dictionary words - Some passwords may not be accepted as they may be words from a dictionary or a simple variant of them.

C. Most-common passwords: Some passwords may not be accepted because they are most popularly used and the accounts which are using those passwords are prone to more frequent attacks.

D.Popular passwords: Sometimes even a unique password may not be accepted if most users are using the same password or similar ones.

5.2. Failover

The computer system is designed to possess a "failover" mode in order that logins will proceed more-or-less as was common even if the honeychecker has failing or become inaccessible. In failover mode, honeywords area unit quickly promoted to become acceptable passwords; this prevents denial-of-service attacks ensuing from attack on the honeychecker or the communications between the system and also the honeychecker. The cost in terms of exaggerated word guess ability is tiny. Temporary communication failures is self-addressed by buffering messages on the pc system for later delivery to and process by the honeychecker.

5.3. Per-user policies

The administrator may also deploy various policies for various users. By, doing this the administrator tries to make sure that each user have their own unique passwords. This is a very commonly used policy employment as well.

A.Honeypot Accounts- Honeypot accounts provide great help with the honeyword encryption because these account help in distinguish a theft from a DoS attack. The identity as to which are the honeypot accounts from the total number of accounts is only known to the honeychecker.

B.Selective Alarms- It might be useful raise caution on the off chance that there are honeyword hits against director accounts on the other hand other especially touchy records, even at the danger of additional affectability to DoS assaults. Arrangements needn't (and maybe shouldn't) be uniform over a client bases.

6. Conclusion

In This article we have discussed about honeywords and how they can be used to protect the user information. The major advantage of honeyword is that unlike any other type of encryption mechanisms it not only protects the user data but also helps us in tracking down the attacker. The other factor which really separates honeyword from its counterparts is that it can be used in the current system employed and can also be used separately for each account. Another major benefit of using this technique is that different honeyword generation methods can be used for different accounts in the same system, so when the attacker finds the password generation method of one file it may not be applicable for the other password files as well. However this mechanism is not entirely secure because there is a chance that the attacker who has stolen the password files can indeed access the account if he guesses the correct password. But the usage of honeywords the attacker will think twice before using the password because if the wrong password is chosen then there is the risk of him being detected. The honeychecker checks the password given and detects if the person trying to access an account is indeed an authentic user or an attacker. But detection only is not enough as the attacker can try to access the account again from the same or different system. Therefore for this mechanism to work as efficiently as it can along with detection and tracing should also be enabled.

References

1. A. Juels and R. L. Rivest, “Honeywords: Making Password-cracking Detectable,” in Proceedings of the 2013.
2. 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.
3. D. Mirante and C. Justin, “Understanding Password DatabaseCompromises,” Dept. of Computer Science and EngineeringPolytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02, 2013.
4. M.S.Saravanan, R.Sheshadri, et.al., “A Role of Intrusion Detection System for Wireless Sensor Network using various Schemes and Related Issues” Published in American Journal of Applied Sciences by Science Publications, USA. Vol.9, Issue.10, July’ 2013, pp.979-98, ISSN:1546-9239.
5. G. Notoatmodjo and C. Thomborson, “Passwords and Percep-tions,” inProceedings of the Seventh Australasian Conference on InformationSecurity–AISC 2009. Australian Computer Society, Inc., 2009, pp. 71–78.
6. D. Florencio and C. Herley, “A Large-scale Study of Web Pass-wordHabits,” inProceedings of the16th international conference on WorldWide Web. ACM Press, 2007, pp. 657–666.
7. Imran Erguler,” Achieving Flatness: Selecting the Honeywords from Existing User Passwords”, DOI 10.1109/TDSC.2015.2406707, IEEETransactions on Dependable and Secure Computing.
8. M. Raza , I. Muhammad, S. Muhammad and H. Waqas, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," World Applied Sciences Journal @IDOSI Publications, vol. 19, no. 4, pp. 439-444, 2012.
9. J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In IEEE Sump. Security and Privacy, 2012.
10. D. Elser and M. Pekrul. Inside the password-stealing business: the whoand how of identity theft, 2009.