Malicious user detection using honeyword and IP tracking

Ms. Komal Naik
M.E. Student, Department of Computer, SLRTCE-Mumbai University, Mumbai, Maharashtra, India
komalnaik20@gmail.com

Prof. Varsha Bhosale
Associate Professor, Department of Information Technology, VIT-Mumbai University, Mumbai, Maharashtra, India
varsha.bhosale@vit.edu.in

Prof. Vinayak D.Shinde
Assistant professor, Department of Computer, SLRTCE-Mumbai University Mumbai, Maharashtra, India
vdshinde@gmail.com

Abstract **-** Now-a-days it has become very easy for an adversary to steal the password hash file and crack the hash passwords. Thus, the threat for each user accounts continues to increase rapidly. As the cybersecurity threats are increasing, new mechanism needs to be developed. To detect the password file breach, Juels and Rivest had introduced the concept of decoy passwords known as "Honeywords". For every user account, set of false passwords are generated using honeyword generation techniques. So, the hashed password databases consists of actual passwords and false passwords. For an adversary, when a password file is cracked, it becomes difficult to judge the real password. Honeyword model sets off an alarm if any of the honeyword is entered, notifying about the password file breach. Thus, there is a huge risk of an adversary being detected. In our model, we are implementing the decoy mechanism for protection of data from an unauthorized user and also tracking the IP of the detected user to take action against the malicious user.

Keywords- *Blocking, Decoy, Honeywords, IP, Intruder.*

*****

I. INTRODUCTION

Prevention and Detection of an unauthorized access of the system is called as Computer Security. For securing the system is necessary to follow three steps.

- Prevention – Stopping the action from happening or occurring is called as Prevention.
- Detection – Noticing the presence of some failure is called as Detection.
- Reaction – Responding to the failure is called as Reaction.

Everywhere the system has become an important element of day to day life. As all the relevant data is stored on the system, it necessary that system should be secure enough. The most widely used authentication method which proves better in standards such as usability and security is authentication based on Password. It is important that passwords must be protected and secure enough to avoid different attacks. Now-a-days many companies store their important data in databases [1]. It is very easy for an intruder to get the username and password by using emerging and new password cracking techniques. So for avoiding password related issues, Honeyword concept was introduced.

A. Honeywords

Honeywords are false or decoy passwords which are generated using different generating algorithms. It is a set of words which are some wat similar to the password submitted by the user for a particular account. For every user account the set of honeywords are generated. Honeywords are generated using generator algorithm. Honeywords concept was introduced to detect the failure and an unauthorized access. In our system, we are introducing the concept of IP Blocking as Reaction towards the detected intruders.

B. Decoy Data

Decoy data mechanism is also called as Fog Computing. This concept is basically introduced for confusing the attacker and making difficult from him to distinguish between the sensitive data (worth data) from the irrelevant data (worthless data). It helps in securing the real data of the user from being misused. Fake (Decoy) files are made available only when unauthorized access is detected by the honeyword generation scheme.

C. IP Blocking

IP address blocking is used for disabling the access of an unauthorized users. It is very important for introducing this concept in honeyword model for maintaining the security of the system. Blocked IP address can be added in blacklist for avoiding the misuse of the system and keeping it secure from various types of attacks.

II. LITERATURE SURVEY

A. The Dangers of Weak Hashes

K. Brown[2] says that for a secure system it is necessary that good methods for hashing should be implemented. Many companies which didn't follow good hashing methods had compromised there password files which had effected them a lot. Due to password leaks the confidential data of the companies as well as the users was available to the hackers. Thus, it was concluded that strong hashing mechanism need to be implemented for the security purpose.

B. Achieving Flatness: Selecting the Honeywords from Existing User Passwords

In this study, Imran Erguler [3] examine the honeyword model and highlights some issues. They introduce a different approach towards the honeyword system. Here the system selects the already existing passwords as the honeywords to confuse the intruder and put him at a high risk of detection. Since the honeywords selected are already existing passwords for various user accounts the storage cost is reduced.

C.Honeywords: Making Password-Cracking Detectable

Juels and Rivest have extended the concept of honeyword model. In this model, for every user account a set of honeywords are maintained [4]. These honeywords are generated using honeyword generator algorithms. They have used a server named honeychecker which is used to check whether the password which is entered by the user is a honeyword or not. If the password entered is a honeyword and not a real password then the server sets off the alarm. But in this system some possible attacks were highlighted such as password guessing attack, attacking the honeychecker etc.

D.FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology.

They have proposed a new approach for securing the data on the cloud by using the fake (decoy) information technology. This different approach of confusing the intruder with a fake data is called as Fog Computing [5]. The motive behind this technology was just to keep the real and sensitive data safe from the hands of malicious users. The decoy provides (a) validating whether the access to the data is authorized when malicious entry is detected and (b) confusing the intruder with fake information.

E. Nymble: Blocking Misbehaving Users in Anonymizing Networks

Patrick P. Tsang and Apu Kapadia [6]says that IP address blocking is a type of security which is used for securing the web services, servers etc. It blocks that IP address if any malicious behaviour is observed or detected from that particular IP. Blocking the IP of authorized as well as unauthorized users for whole time is not correct. To overcome this issue they have categorized the IP address and the most dangerous IP address is the added in the blacklist.

III. RELEVANCE OF THE HONEYWORD MODEL

Most businesses today know the need to have a strong data security strategy to protect themselves, their employees and their customers from various security threats. Generally many companies and software industries store their data in ORACLE or Mysql or may be other. So, for entry into the system which is required is user name and password. Once a password file is sacked, by the password cracking technique it is easy to get most of the passwords. In previous years many companies like LinkedIn, Yahoo, and eHarmony were affected due to password leaks because of following weak security practices. To increase the security the honeywords concept was introduced. In honeyword system it is sure that the attacker will be detected. But due to some reason, till now no action was taken against the unauthorized access detected.

The proposed system tries to fill this void by proposing a new technique where we detect the unauthorized user and block him with the help of his IP address and we also protect the sensitive and relevant data of the user by providing the fake worthless data to the adversary.

A.Our Approach

We use honeywords mechanism to launch disinformation attacks against unauthorized insiders, preventing them from distinguishing the original sensitive customer data from fake worthless data. In this work we will use an already well-established method of honeyword generation and have used a logic of ASCII to generate honeywords and SHA-256 algorithm for hashing. The attempted use of a honeyword for login will set off an alarmto the administrator and user about the password file breach. After more than 3 incorrect attempts the unauthorized user will be given access to decoy files. System will also keep track of IP.Using IP tracking we can avoid unwanted request from a single system thus reducing the unnecessary computation.

ISSN: 2321-8169
114 - 117

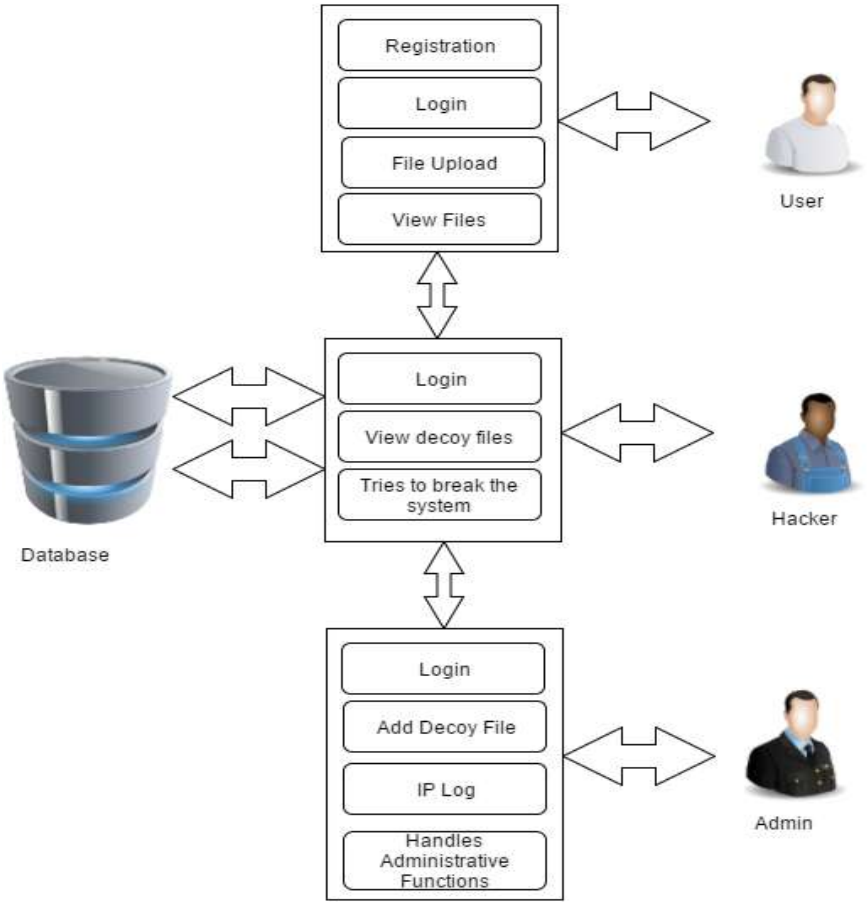

Figure 1: Proposed Honeyword Based System.

IV. RESULTS AND DISCUSSION

A person who has an authorized access to the system is said to be a user. Here, User is going to register into system. While registration, for the given password by the user the system generates honeywords using honeyword generation technique.

User login into the system using his unique email id and password. If password matches with the hash of the original password then user gets access to the system. For a valid login, the access to his actual data will be given.

If the adversary exceeds the count of greater than three than that user is blocked.

Hacker tries to login into the system. If he enters any honeyword then the alert is given to the Actual user and the admin through an email.

And if suppose he try combination of password or any honeyword and it goes more than three attempt then he get access but to the decoy files. Decoy files are fake files which are displayed to the intruder when a failure or an unauthorized access is detected.

For every login, whether the attempt is valid or invalid the IP is tracked. Log of number of attempts is also maintained in the database for every user id which will be help us to take necessary action.

V. CONCLUSION

The main aim of project is validating whether data access is authorized or not when abnormal information access is detected and taking appropriate action against unauthorized access detection.

Basically, confusing the attacker with fake information. This protects against the exploitation of the user's real data. We propose a completely different approach for securing the data using decoy information mechanism. We use this honeyword technology to launch deceptive attacks against wicked insiders, preventing them from distinguishing the actual real customer data from fake irrelevant data. The addition of IP tracking module in this proposed model helps to block the unauthorized access thus providing the better system security.

VI. REFERENCES

[1] M. Dennis and Justin Cappos, "Understanding password database compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, 2013.

[2] Brown and Kelly, "The dangers of weak hashes," SANS Institute Infosec Reading Room, November 2013.

[3] I. Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," *IEEE Transactions on Dependable and Secure Computing, IEEE*, vol. 13, no. 2, p. 284 – 295, February 2015.

[4] A. Juels and R. L. Rivest, "Honeywords: Making Password cracking Detectable," *In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, p. 145–160, November 2013.

[5] D. C. Saste, " FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology," *International Journal of Computer Technology & Applications*, vol. 5, Sept-Oct 2014.

[6] P. T. P. and . A. Kapadia, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 256 - 269, 2011.

[7] Bonneau and Joseph, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," *In 2012 IEEE Symposium on Security and Privacy*, pp. 538-552, 2012.

[8] Herley, C. and Florêncio, D, Protecting financial institutions from brute-force attacks," *In IFIP International Information Security Conference, Springer US.*, pp. 681-685, September 2008.