MALICIOUS USER DETECTION USING HONEYWORD TECHNOLOGY

Ms. P.V.Ashwathy Devraj[1], R.Jabin Balan[2],S.Kavin Raja[3] ,R.Rajaram[4] ,C.S.Surya[5]
[1]Assistant Professor, Department of Computer Science and Engineering,Karpagam College of Engineering, Coimbatore
[2,3,4,5]Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore
E-mail ID:ashnov22@gmail.com

ABSTRACT

Now-a-days it's effortless act for an antagonist to abduct data in the password hash files and to crack the hidden hash passwords. The threat of user accounts at risk continues to extend rapidly. Due to cybersecurity at risk, new mechanisms need to be developed and implemented. Juels and Rivest introduces a new method to detect the password breach known as "Honeywords".A batch of duplicate passwords are engender by the algorithm of honeyword generation.As the result, the databases consist of exact passwords and invalid passwords for every user account. For the adversary, when a password file is cracked, it increases complexity to gauge the exact password. Honeyword model pop-ups a notice when the honeyword is attempted, reporting the password file violation. Thus, An enormous risk of an antagonist being disclosed. . In this model, decoy mechanism implemented to cover of knowledge from an unapproved or illegal user and to track and detect the IP address of unauthorized user to take action against the malicious user. Added to that an extra feature of inserting a virus code in decoy data to get details of the attacker or system is introduced.

1. INTRODUCTION

Detection – observing the existence of any failure is known as Detection. Reaction – Action taken to face the failure is known as Reaction. System occupies a place in every sectors and plays vital role of in the modern world. As all the data is stored in the system, it is necessary to secure the system with appropriate security methods. In beginning, authentication method is widely used to prove better standards like security and reusability is authentication supported password. It is necessary to ensure the passwords to be closed with high protected and secured to prevent various attacks caused by the antagonist.In this modern world many companies stock their essential data in databases. It is effortless act for a trespasser to urge the username and password by using existing and new password hacking techniques. To prevent password related flaws and issues, a new method called Honeyword concept was developed. Initial passwords must be secured by a desirable appropriate defense method and stocked with their puzzled values calculated through the mechanisms

generated by honeyword. Hence, it is designed for an antagonist it increases the complexity to implement hashes to receive a plaintext password. The extra view is that a secure organization should perceive to not take appropriate actions or to check that the keyword file discovery occurred .We specialize in the latter problem and impact false passwords or accounts to detect password leakage as a simple and cost-effective solution.

When a user sends a login request, the login server must decide the order between the users, and hence the order between her sweet words of the password sent.The login server searches for honeywords and sends the user and his password a message of the form to a secured server. The honey checker will decide if the given word could also be a password or a honey word. If a honey word is provided, an alarm will be raised or an action taken that's previously selected**.**The honey checker cannot recognize password or honey words close to the user. It maintains one server containing Completed from Only the order of the user's essential sweet word password. In our model, we are implementing the decoy mechanism for cover of knowledge from an unauthorized user and also tracking the IP of the detected user to require action against the malicious user. Added to that an extra feature of inserting a virus code in decoy data to get details of the attacker or gain access of the attacker system. The virus code can even get vital information such as Cookies,Operating System of the attacker and location of the attacker. We use the following methodologies in thismodel Honeywords are false or decoy passwords created with various generation algorithms. It is a group ofwords generated by using a suitable algorithm for the password which is User submitted for a specific account.

The honeywords aregenerated for every password of users in the system. Honeywords are generated using algorithm generator.The unauthorised access canbe detected by using this method.The detected intruders are blocked by using their IP as a reaction towards the malicious user detection.The Data Decoy Mechanism is additionally called Fog Computing. This definition is implemented primarily to confuse the attacker and make it difficult for him to differentiate between the sensitive data (worth data) from the irrelevant data (worthless data). It helps to ensure the user's real data is not misused.False (Decoy) files are made available by the honeyword generation scheme only with unauthorized access. IP Blocking IP address blocking is used to prevent an unauthorized user's access. It is important for this concept to be incorporated into the honeyword model to ensure machine protection.Blocked IP address can be attached to the blacklist to prevent device abuse and to keep it secure from various types of attack.

II.LITERATURE SURVEY

1. Measuring the power of a password by simulating password cracking algorithms:

From the many notable findings it is noted about the comparative power of various compositional policies. Although NIST considers basic16 and detailed equivalents, we considered it to be superior to large numbers of guesses.Through integrating prior results, it is clear that basic16 is also simpler for users, and it suggest that basic16

is the best policy option. We also found that the efficacy of a dictionary test strongly depends on dictionary selection; In particular, an outsized blacklist created using state-of – the art password guessing techniques is much simpler than a standard dictionary to prevent users from easily selecting guessed passwords.

2. Wide-ranging analysis of Internet login habits:

The results of an outsized password scale analysisand re-use of passwordhabitsover a period of time half a million people were interested.A client portion reported a spread of password power, use and frequency metrics on user machines. This helps us to quantify or approximate these amounts because each and every user has the usual number of passwords
and average accounts includes,what proportion of passwords they forms by day, how often are passwords exchanged between sites, and how often they are forgotten.

The extensive data on the strength of the password, the styles and lengths of the passwords chosen and how they differ by site.The data reveals that passwords play a significant role in the online experience of the user and provides various insights into other large-scale studies of their type.

3. Examination of a new mechanism for defense:

The decoy passwords i.e. Honey words used to characterize hash password database attacks. For each and every user account the valid password was kept in the form of honey words. If attackers target passwords i.e. honeywords, it would not make sure that it is a real password or honeyword. Cracking the password hash along with developments within the graphical processing unit (GPU) technology is less complicated. Entering which has a honey word to login will cause an alarm that notifies the administrator of a password breach of the file.

4. Cracking password Using Probabilistic Context-Free Grammar:

It could be a worrying job by using a dictionary based Crackling parole assault and choosing a exact word to bypass the password. The tendency to address a substitution technique generating parole structures in order of highest chance. They first mechanically produced a probabilistic context free descriptive linguistics mainly based on a coaching set of passwords previously disclosed.

The parole guesses were Used in cracking parole and descriptive linguistics were made for The laws of word-mangling and it conjointly showed that this solution seems a more realistic one approach cracking paroles relative to techniques for setting real passwords and by testing with tools.

5. Internet Password Habits A Wide Scale Study:

The subject of the utilization In the computer security literature, passwords and alternatives for authentication were studied at length. The web users Login patterns got far less coverage. Various attacks on password schemes are an early analysis of user password behaviors on a UNIX sharing

system; then compile a list of 3289 passwords obtained from a wide number of users. It is found that almost 90% the passwords were extremely weak: too small, containing only lower case letters, single digits or a combination of both, or easily found in dictionaries or name lists. In a way, the results that we present update and expand this research with much more data. Although much has improved since 1979 (e.g. it is very popular to have a minimum of 6 characters), it is just as true that many users continue to select the weakest possible password, unless compelled to do otherwise.

The poor passwords, such as names accompanied by a single digit, were commonly used in a number of machines they tested in a corporate network. A report stated the ability to crack about half a percentage of passwords in use by brute force attack, again on a Unix system. We questioned users about password memorability, and also found that choosing hard-to-remember safe passwords is proving a difficult task for many users. Previous results on the strength of passwords reinforce and expand these studies to a new study on the memorability and protection of passwords.

The survey included 288 students; a third was asked to select a password (given certain password rules), a third was assigned random passwords and a third was asked to select a password using a phrase backed by mnemonic.Among their results was that randomly assigned passwords and phrase-based passwords were similarly cracked by dictionary attacks, but phrase-based passwords were much easier to remember. There are several studies that use questionnaires about user access behaviors. A good summary of recent surveys is this is a really helpful compendium of user responses to questions about their password use, reuse, and forgetting behaviors at major institutions as well as a list of password policies. Through surveying users, most of the data in is collected. The analysis tests, through comparison, what they actually do, rather what they say they do.

III.EXISTING SYSTEM & RESULTS

The user_id and password is used to validate the authentication of users in many applications. If the password is hacked, then the attacker can take important data from the user account. This hack activity happen by taking the password files from the data.The password hacking is a major issue and it leads to numerous security threads.In the existing systems they just checked the password breach and identified how to design the honeyword algorithm for password checking and they were just left with no proper method to block the intruder from further stealing of data from the system.

IV. PROPOSED SYSTEM

The idea behind honeywords is to create a relation between the real password and decoy hashed passwords, such that for every user the latter look like real passwords. The honeywords are these decoys. An attacker can recognise the presence of honeywords in a password file, as it is very unusual to have multiple passwords for a single user account. However, even if the attacker can crack multiple passwords associated with a user, he or she does not know which are honeywords, and which are the real ones.

The proposed mechanism can distinguish the user password from honeywords for the login routine and will redirect user to decoy data. If a honeyword is matched then the attacker will get access to the decoy data and the intruder camera will capture the photo of the attacker.

V.ALGORITHM

Step1: Register a new account in the system with an appropriate username and password.

Step2:The honeyword generating algorithm uses a combination algorithm for each user's password.

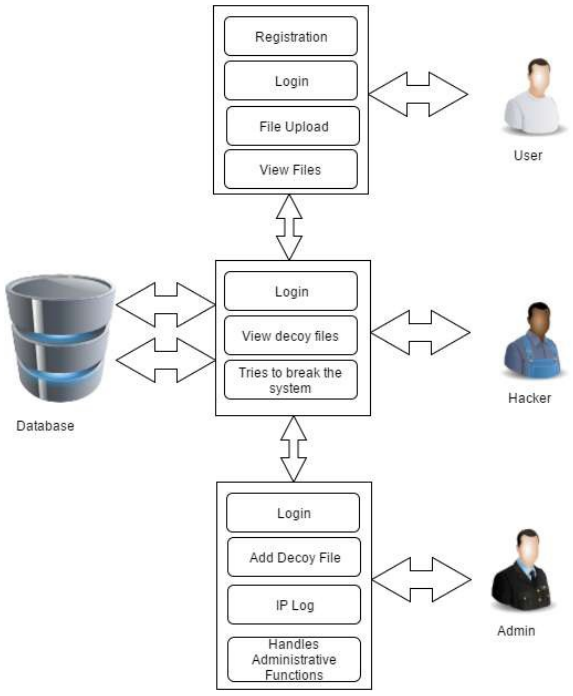
Step3:The user can store their files in the system.

Step4: If an intruder tries to use any of the combination of the user's password,then the honeyword checker will check for honey words for 3 times and if it matches the honeywords generated by the algorithm.

Step5: Then the intruder gets access to the decoy data of the system which is similar to the original data

Step6: The IP address of the intruder is blacklisted and the intruder will not be able to access the system henceforth.

VI.BLOCK DIAGRAM



VII.CONCLUSION

The main aim of the project is validating whether data access is permitted or not when abnormal information access is detected and taking appropriate action against unauthorized access detection.Basically, confusing the attacker with fake information.The user's real data is protected by this method.

We propose a totally different approach for securing the info using decoy information mechanism.We use this honeyword technology to launch deceptive attacks against wicked insiders,preventing them from distinguishing the particular real customer data from fake irrelevant data.The addition of IP tracking module and virus code insertion within the decoy data during this proposed model helps to dam the unauthorized access and therefore the user

can get vital information about the attacker and thus providing the higher system security.

VIII.FUTURE WORKS

Further providing a better approach to the security of the system,we are going to introduce intruder camera which will access the system's webcam by default and provide the user with the photo of the intruder which will be more useful to take necessary action against the attacker.Added to that,a better way of communicating the user by means of SMS and Email along with the intruder details,IP and photo captured by the webcam will be sent to respective user.Added to that an extra feature of inserting a virus code in decoy data to get details of the attacker or gain access of the attacker's system will be introduced.

IX.REFERENCE

[1].M. Dennis and Justin Cappos, "Understanding password database compromises,"Dept.of f 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.

[2].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.

[3].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

[4]Password Cracking Using Probabilistic Context-Free Grammars"Authors: M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek.

[5]Examination of a new defense mechanism: Honey words"Authors: Z. A. Genc, S. Kardas, and M. S. Kiraz

[6]J. Bonneau. Guessing human-chosen secrets. PhD thesis, University of Cambridge, May 2012.

[7] B. M. Bowen, S. Hershkop, A. D. Keromytis, and S. J. Stolfo. Baiting inside attackers using decoy documents in SecureComm, pages 51–70, 2009.

[8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts belong to us: automated identity theft attacks on social networks. In WWW, pages 551– 560, 2009.

[9]C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. IEEE Security & Privacy, 10(1):28–36, 2012.

[10]Erguler, Imran. "Achieving flatness: Selecting the honeywords from existing user passwords." IEEE Transactions on Dependable and Secure Computing 13.2 (2016): 284-295.

[11] .P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T.Vidas, L. Bauer, N. Christin, L.F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In IEEE Symposium on

Security and Privacy (SP), pages 523–537, 2012.

[12] Defense Information Systems Agency (DISA) for the Department of Defense (DoD). Application security and development: Security technical implementation guide (STIG), version 3 release 4, 28 October 2011

[13]. A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In SOUPS, pages 1–12, 2009.

[14] D. Malone and K. Maher, "Investigating the Distribution of Password Choices," in Proceedings of the 21st International Conference

[15] Paul. Update: LinkedIn confirms account passwords hacked. PC World, 6 June2012.

on World Wide Web, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 301–310. [Online].

[16] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," in Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques–EUROCRYPT'03, ser. Lecture Notes in Computer Science, vol. 2656. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 294–311.