International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Security Enhancements by achieving flatness in Honeyword for web user passwords

Rohini Wankhade[1], Vishal Ubale[2], Shivam Sharma[3], Shilpa Gite[4]

[1,2,3,4] *Department of Computer, Indira College of Engineering and Management, Pune, India.*

Abstract - *In recent years, all the activities of the countries over the world is carried out Digitally and all the information or data is shared over the network increasing the speed and efficiency of data, but this transformation of data over the digital network has threat of security i.e loosing the data of the users by the third party unauthorized persons or attackers, cyber crime has taking consistent efforts to improve the security over the network as all the scams now a days are carried digitally as the data transformation includes money transfer, online shopping, confidential data, social feeds, etc. As to maintain the security a unique identification value or term called password is given to every user and is asked to keep it secret, but the attacker still steals the password using various techniques so to avoid these threat we are using Honeywords which will be generated by existing user password and if the attackers enter the password from the honeypot alarm is raised over administrator side, also we maintaining the IP and location tracking of the user and proposing a new technique called video click based captcha scheme to authenticate between humans and robots/bots overcoming the problems of graphical password scheme captcha. Thus, this whole architecture protects and secures the data and application over the online network reducing the threats against the unauthorized users.*

Keywords: Authentication, Video Click based Captcha, Honeywords, Tracking, Decoy, Password

1. INTRODUCTION

In recent years the whole world has stored to the Internet world for the latest gadgets which increases the speed and efficiency of the task or any specific work, when we talk about internet world i.e www(world wide web) Information security plays an vital any very important role as it is used to secure and protect the information over the network against the fake users and third party attackers and has many authentication methods such as passwords, patterns, PIN numbers, captcha, etc. The most effective authentication method carried by every system is Password which is very secured and easy for humans to understand and remember, hence security of password is an important aspect when comes to digital network, a password is unique for every user and is a secret key through which user logins any specific system and gain access to that system for carrying out further operations online(eg: online payment) the application development should also maintain the user password in hash codes or in encrypted format in database using various encryption algorithms increasing the security of the password. In recent years many unauthorized password gains are carried out by the attackers or hackers which has leaded access to the confidential as well as sensitive data over the network, as password protects the user from keeping the data safe and strain the authorization limits, we must form the new techniques to make the password more strong and protective as it will be difficult for the hackers to crack it, many companies like yahoo, e-bay, LinkedIn as faced the passwords attacks and the users passwords were revealed. As now a days peoples have fully switched to the Digital network to carry public as well as private activities like online payments, shopping, bank transactions, etc so to avoid the frauds over the internet cyber crime has introduced many techniques to manage or to provide the security from the third party users, attackers and machine robots, hence to avoid these all serious issues we are coming with the new password securing technique called honeywords generation from existing passwords and maintaining the tracks of the user which includes the internet protocol address and location attributes as Country, state, city and to provide security against the Machine bots we are using Video click based captcha authentication. This newly upcoming technique will be robust and cost effective and it will overcome all common attacks including OCR bot attacks which every existing Captcha has failed to achieve.

When comes to Honeywords technique to prevent the passwords, there are two issues that should be considered to overcome these security problems: First, passwords must be protected by taking appropriate precautions and storing with their hash values computed through salting or some other complex mechanisms. Hence, for an adversary it must be hard to invert hashes to acquire plaintext passwords, Honeypot is one of the methods to identify occurrence of a password database breach, In this approach, the administrator purposely creates deceit user accounts to lure adversaries and detects a password disclosure, if any one of the honeypot passwords get used.

Use of decoys for building theft-resistant and the fake password sets are stored with the real user password set to conceal the real passwords, thereby forcing an adversary to carry out a considerable amount of online work before getting the correct information. Recently, Juels and Rivest have presented the honeyword mechanism to detect an adversary who attempts to login with cracked passwords. Basically, for each username a set of sweet-words is constructed such that only one element is the correct password and the others are honeywords, Hence when an adversary tries to enter

into the system with a honeyword, an alarm is triggered to notify the administrator about a password leakage. With this existing security we are tracking the Internet Protocol Address and Location of the user from where he is trying to attempt the fraud, the location included the following entities as Country, State, City. On the other side we are using the Video Based Click Captcha authentication with the help of Plane-axis and RGB's. Thus we propose a new System where a set of existing passwords are used as sweet words by another new user to avoid the various attacks on Passwords i.e realistic honeywords are provided and even if the password is cracked we are maintaining the IP and Location whereas along with this we are introducing new Primitive Video based click Captcha scheme to free our systems of Machines and Robots

2. LITERATURE SURVEY

Imran Erguler.**[7]**This paper explore the much easier to crack a password hash with them advancements in the graphical processing unit (GPU) technology. Once the password has been recovered no server can sense any illegal user authentication (if there is no extra mechanism used). They propose an approach for user authentication, in which some wrong passwords, i.e.,

―honeywords‖ are added into a password file, in order to detect impersonation. The authors in propose an interesting defense mechanism under a very common attack scenario where an adversary steals the file of password hashes and inverts most or many of the hashes. The honeyword system is powerful defense mechanism in this scenario. Namely, even if the adversary has broken all the hashes in the password file, he cannot login to the system without a high risk of being detected. Hacking the honeychecker has also no benefit to the enemy since there is no information about a user's password or honeyword in the honeychecker .

Genc, Z. A., Kardas, S., & Kiraz, M. S.**[1]**This paper describes a new technique to provide the security and protection for the passwords A new honeyword generation algorithm which reliable and scalable results with respect to flatness, Honeywords are generated with the existing user passwords and are also maintained in the honeypot, a cyber attacker who steals a file of hashed passwords cannot be sure if it is the actual password or a honeywords. Furthermore, entering with a honeyword to login will trigger an alarm informing the administrator about a password file opening. "Achieving Flatness: Selecting the Honeywords from Existing User Passwords"

3. EXISTING SYSTEM

Honeywords which is also known as decoy passwords, which are created from users passwords to detect attacks against hashed database. This honey word helps to find the impersonate attacks. Hence, the cracked password files can be detected by the system administrator if a login attempt is done with a honeyword by the adversary. We use the notations and definitions to simplify the description of the honeyword scheme. There are several methods/Algorithms for Generation of honeywords and are Chaffing-by-tweaking, Chaffing-by-tweaking with a password model, Hybrid honeywords Algorithm, Chaffing with "Tough Nuts". Honeywords mechanism is used by many researchers and authors to increase the security of the system or application along with the efficiency of the system, the sugarwords are the special words choosen from the passwords tulp file or the common users passwords which are stored in the database. The password generation for user by combining and carrying operations on the existing users passwords by separating the attributes like special characters, numerical values, alphabets, etc which can be used by the new user to signup and process further, the advantage of using the honeyword as password is when the attacker tries to decoy or make multiple attempts to crack the user security an alarm will be set on the admin side and admin will be notified and hence administrator can take the appropriate actions against the attacker, as honeywords make this possible to track the attacker by alerting the system and also confuses the third party attacker to guess the password because of the combined real passwords and honeywords in a file.

Honeywords prevents the application or systems from many common attacks such as Dos attacks, D-dos attacks, Dictionary attacks, phishing attacks and brute-force attacks, etc. System storage is also low for the system when comparision is between Honeywords and other security algorithms, the efficiency and accuracy of the honeywords is much very impressive as compared with the old techniques. Hence use of honeywords for protecting and making the system secure against password breach is much effective and accurate as per the analysis of the architecture built for the proposed System, the architecture is designed in such a way that honeywords are generated but with the separation of the attributes and existing user password by attaching a tail to the password if required and low maintainance cost. The honey pot is maintained in such a way that when any attacker used the password from honeypot the administrator is inform by raising a alarm on his system, hence in the information security approach honeywords plays an very important role and can be integrated with the new upcoming techniques to provide the grade level security.

4. PROPOSED SYSTEM

In the Proposed System, We are implementing and developing the new techniques with taking existing system of honey words into the consideration, as we are combining the existing of the users and are generating the new sweetwords/Honeywords using chaffing-by-tweaking and pattern generation algorithms which has maximum efficiency of detection and more accuracy compared to the other algorithm combinations(as per references).

We are developing a shopping application where we are providing high-end security with our proposed System, as due to the increasing internet activities over the world there is lack of security issues and hacks because of which there are frequent digital frauds which are taking places. As there are many third party attackers trying to decoy/open the passwords of users over the network and carry the required frauds which can be in terms of Money transaction, confidential data, application, servers, hacks etc, to avoid these all loop holes in the todays internet world we are to use an technique which generates the Passwords called Honeyword from the existing user passwprds which are stored in the databases which will help us when a attackers is trying to guess the password(wrong passwords) or Brute-force or Dictionary attacks there will be alarm set which is managed by the Administrator of the server/System, as soon as the alarm is raised the administrator can block that portal and can find the attacker, as we are also tracking the attacker using Internet protocol address and also by its Country, state, and city.

The Problem occurs with the Network security when managing the applications are Bots, viruses, Trained machines which can be easily injected to the application and it can carry out the attack against the System, to avoid this Captcha was introduced which is used to detect between the Humans and machines which has agained failed to provide the security due to OCR(optical character recognization), OCR is used by the attackers/hackers to read the characters, numbers from captcha which creates a loop hole in the System/application.

Hence once the signup process is completed the login page with the same video is presented in front of user and user has to click on the same click points to proceed further.

Hence we are securing the Application as well as the Network avoiding the public internet frauds by tracking each user and providing security to his/her password safe with the help of administrator and also protecting the Application/system by Bots/machines/robots etc by proposing video click based captcha.

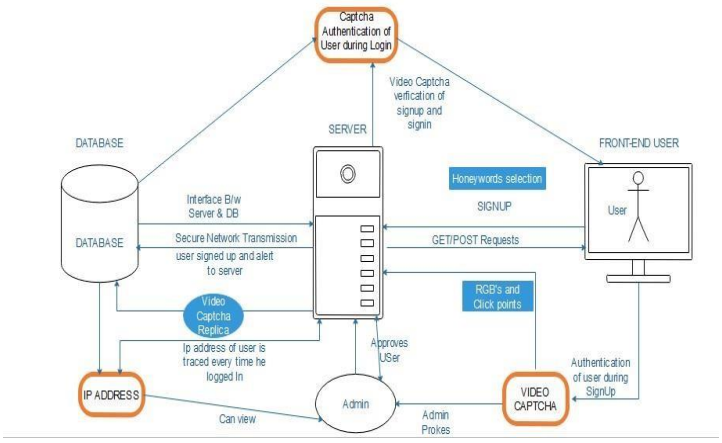

Fig.1: System architecture

5. IMPLEMENTATION

In this system, we are implementing web application with honeyword mechanism to launch disinformation attacks against unauthorized insiders, preventing them from distinguishing the original sensitive customer data from fake worthless data. The attempted use of a honeyword for login will set off an alarm to the administrator and 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. We also provide video based captch for avoiding machine attacks.

6. CONCLUSION

Password security has always been a domain of active research. Honeyword based authentication have proved better results in this domain. The big difference between the traditional methods and when honeywords are used is that a successful brute-force password attack does not gives the attacker confidence that he can log in into system successfully without being detected. Research on better honeyword generation techniques has already been proposed with respect to security, usability, flatness, DOS resistance and storage. The use of decoy data mechanism will secure the confidential data of the authorized users from the hacker. In honeyword based authentication approach, it is sure that the attacker will be detected. The main aim of project is to validate whether data access is authorized or not when abnormal information access is detected. Video Based click CAPTCHA plays again important role when authentication is to be done between robots and humans, Confusing the attacker with decoy data protects from the misuse of the user's real data. The admin keeps the data of the tracked IP' switch them and use them to block access on their network. Use of honeywords is very useful and works for every user account.

7. FUTURE SCOPE

To identify and resolving identities of users across online social network. To detect anonymous user and which one is true user identity and which one are fake accounts.

REFERENCE

[1] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 284 - 295, February 2015.

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

[3] Mirante, Dennis and Justin Cappos, "Understanding PasswordDatabase Compromises," Dept. of Computer Science and EngineeringPolytechnic Inst. of NYU, 2013.

[4]C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in Proc. 23rd Int. Inform. Security Conf., 2008, pp. 681–685.

[5] A. Juels and R. L. Rivest, "Honeywords: Making password cracking detectable," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 145–160.

[6]M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in 30th IEEE Symp. Security Privacy, 2009, pp. 391–405. [5]. F. Cohen, "The use of deception techniques: Honeypots and decoys," Handbook Inform. Security, vol. 3, pp. 646–655, 2006.

[7]Genc, Z. A., Kardas, S., & Kiraz, M. S. (2013). Examination of a New Defense Mechanism:Honeywords. IACR Cryptology ePrint Archive, 2013, 696.

[8]M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, "Improving security using deception," Center for Education and Research Information Assurance and Security, Purdue Univ., West Lafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013- 13, 2013.

[9]D. Malone and K. Maher, "Investigating the Distribution of Password Choices," in Proceedings of the 21st International Conference on World Wide Web, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 301–310. [Online].Available http://doi.acm.org/10.1145/2187836.2187878.

[10] Z. A. Genc, S. Kardas, and K. M. Sabir, "Examination of a New Defense Mechanism: Honeywords," Cryptology ePrint Archive, Report 2013/696, 2013.

[7] A. Acquisti, R. Gross and F. Stutzman, "Privacy in the age of aug-mented reality," Proc. National Academy of Sciences, 2011.

[8] T. Iofciu, P. Fankhauser, F. Abel, and K. Bischoff, "Identifying users across social tagging systems," Proc. of the 5th International AAAI Conference on Weblogs and Social Media, pp. 522-525, 2011.

[9] M. Motoyama and G. Varghese, "I seek you: searching and matching individuals in social networks," Proc. of the 11th inter- national workshop on Web Information and Data Management (WIDM'09), pp. 67-75, 2009.

[10] O. Goga, D. Perito, H. Lei, R. Teixeira, and R. Sommer, "Large-scale Correlation of Accounts across Social Networks," Tech-nical report, 2013.