A Survey On Generation of Secure and Reliable Honneyword to prevent False Detection

Rupesh Nale[1], Akash Mane[2], Harshal Nanekar[3], Litesh Shinde[4], Prof. Chetana Baviskar[5]
[1,2,3,4] B.E. Student Dept.of Computer of Engineering Alard College of Engineering and Management, Pune
[5]Asst. Prof. Dept. of Computer of Engineering Alard College of Engineering and Management, Pune

Abstract:- A data breach is the intentional or unintentional release of secure or private confidentional information to an untrusted environment. Usually these breaches go undetected for so many years. Sometimes even business concerned don't seem to be awake to the breach. So it concerns robust breach detection mechanism. Juels et al. recommend way referred to as 'Honeywords'[6].Their plan is to get multiple pretend passwords,referred to as honeywords and store them in conjunction with important word. Sometimes the any login try with honeywords is identified as compromise of word info, so users don't seem to be expected to grasp honeywords corresponding to their passwords.
In the work system may have tendancy to analyze the restrictions of existing honeyword generation techniques. That may have tendancy to propose brand new attack model referred to as 'Multiple system intersection attack considering input'.That have tendancy to show the 'Paired distance protocol' projected by chakra borty is not secure during this attack model.To overcome that above mentioned problem.The new system may be helpful known as honeyword.In the honeyword system there is one most important thing is MAC address.If the MAC address of device change then the user will get OTP on the registered number and if the MAC address remains same then the OTP will not be generated. So that advancement in the project increases the level of security of data.

Keywords: - Password, Honeywords, MAC address, Authentication, Security.

Introduction: - Before the honeyword system there may be problem that someone can try to attack on the system and in few cases system will be crashed. But to overcome the crashing of system there may be one systm known as honeyword. Honeyword is generating the multiple fake passwords from real one.There is also one concept is data breach. It is the security incident in which sensitive, protected or confedential data is copied, viewed, transmitted or used by individual unauthorized to do so.

To improve the security level here uses MAC address. Through that MAC address if MAC address of device is changed then user will get OTP on registered number and if MAC address is same then OTP will not be sended there was directly login in the system.

Literature Survey: -

[A] Entropy Technique :- The evaluation of large password data sets by collecting massive password data set and analyzing it in mathematical manner. In previous paper Shannon entropy and guessing entropy not worked with any realistically sized sample. So they developed partial guessing metrics including new variant of guess work parameterized by attacker desired success rate [1].

[B] Password: - The study of password used and password reused habits. They measured average number of password and average number of accounts each user has as well as measured number of times user enters password per day[2].

[C] Spam technique: -The characteristics of spam and technology used by spammers. They observed that spammers use software tools to send spam with attachment. To track and represent characteristics of spam and spammers they setup spam trap in their mail server[3].

[D] Hash Password:-Hash passwords are used to improve security. For user aunthentication false passwords are added in hashed password file. i.e.honeywords. They analyzed the honeyword

system according to both functionality and security perspective. They also elaborated how system will respond to six password related attackers. Improvement for honeyword is described briefly. i.e. Number of honeywords, typo safe honeyword generation and old password problem[4].

Proposed Work:- In the system to create the honeyword from real password there is the combination of alphabets, digits, special characters. For making strong honeyword alphabets are replaced by alphabets, Digits are replaced by digits and special characters are replaced by special characters. After producing this the output of this should get stored in hashed password file with 19 honeywords and one original password.

Architecture Diagram:-

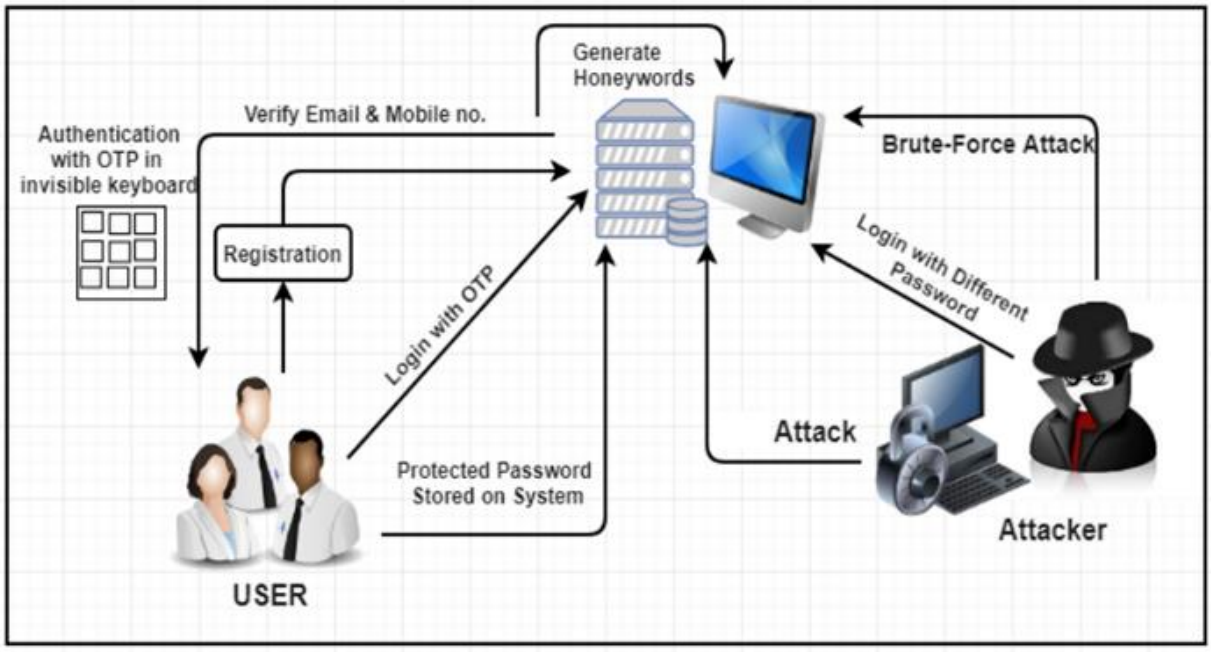

Figure 1:- Architectural diagram of honeyword.

Figure 1 shows architectural diagram of honeyword . It consist of user, system, attacker.User can firstly do registration after that user can login with OTP and protected password stored on system. Then system checks and verify Email and Mobile number. Attacker can do brute force attack there is also invisible keyboard in this system.

Conclusion :- Honeyword is the concept to protect data through multiple passwords. If hacker tries to hack data he get list of multiple passwords and uses MAC address to recognize the user. If MAC address changed the user will get OTP on registered mobile number and if someone else tries to login the system, it will come to know about the hacker.

REFERENCES :-

[1] The Science of guessing: analyzing an anonymized corpus of 70 million passwords. Joseph Bonneau.

[2] A Large-Scale Study of Web Password Habits. Dinei Florencio and Cormac Herley.

[3] An In-Depth Analysis of Spam and Spammers, DhinaharanNagamalai, Beatrice Cynthia Dhinakaran and Jae Kwang Lee.

[4] Examination of a New Defense Mechanism: Honeyword ZiyaAlperGenc, SuleymanKardas and Mehmet SabirKiraz.

[5] Explicit Authentication Response Considered Harmful. Lianying Zhao and Mohammad Mannan.

[6] A. Juels and R. L. Rivest, "Honeywords: Making Password-cracking 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

[7] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 538– 552.

[8] L. Zhao and M. Mannan, "Explicit Authentication Response Considered Harmful," in Proceedings of the 2013 Workshop on New Security Paradigms Workshop–NSPW '13. New York, NY, USA: ACM, 2013, pp. 77–86. [Online].

[9] 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 Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 523–537.

[10] J. Bonneau and S. Preibusch, "The Password Thicket: Technical and Market Failures in Human Authentication on the Web," in WEIS, 2010.

[11] G. Notoatmodjo and C. Thomborson, "Passwords and Perceptions," in Proceedings of the Seventh Australasian Conference on Information Security–AISC 2009. Australian Computer Society, Inc., 2009, pp. 71–78.

[12] D. Florencio and C. Herley, "A Large-scale Study of Web Pass-word Habits," in Proceedings of the 16th international conference on World Wide Web. ACM Press, 2007, pp. 657–666.

[13] 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.

[14] 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