Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 01, January -2019

Securing systems using Honeywords and QR Code

Prof. Krishna Tayade
heena ghare[1] pallavi ghugel[2] sayali kadu[3] harshal kesarkar[4]

[1]*BE, Student, nmiet talegaon dabhade, Pune, Maharashtra, India*
[2]*BE, Student, nmiet talegaon dabhade, Pune, Maharashtra, India*
[3]*BE, Student, nmiet talegaon dabhade, Pune, Maharashtra, India*
[4]*BE, Student, nmiet talegaon dabhade, Pune, Maharashtra, India*

Abstract: *It is represented the honey word mechanism to observe associate degree opposer who makes an attempt to login with cracked passwords. New password is that the combination of existing user passwords known as honey words. Fake password is nothing however the honey words essentially, for every username a collection of sweet words is built specified only 1 part is that the correct password and also the others area unit honey words (decoy passwords). Hence, once an opposer tries to enter into the system with a honeyword, associate degree alarm is triggered to advise the administrator a few password outflow. Honey words to observe attacks against hash password information. for every user account the legitimate password hold on in variety of honey words. If assaulter Attack on password i.e. honeys words it can't be positive it's real positive identification or honeyword. during this study, we tend to to look at intimately with careful attention the honey word system and gift some comment to focus be used weak points. additionally concentrate on pragmatic positive identification, scale back storage price of password, and alternate ay to selection the new password from existing user positive identification. we tend to also are planning the new approach here we'll produce the QR Code for the money transfer, rather than OTP once QR code is scan by banking industry the quantity can transfer to individual account.*

Keywords: *Authentication, honeypot, honeywords, login, passwords, password cracking , QR code*

INTRODUCTION

In this there ar two problems ought to|that ought to be thought-about to beat these security problems: initial passwords should be protected by taking applicable precautions and storing with their hash values computed through seasoning or another advanced mechanisms. Hence, for associate someone it ought to be onerous to invert hashes to amass plaintext passwords. The second purpose is that a secure system ought to discover whether or not a word file revelation incident happened or to not take applicable actions. throughout this study, we tend to tend to specialise in the latter issue and alter pretend passwords or accounts as an easy and price effective answer to find compromise of passwords. once a user sends a login request, the login server will verify the order of her among the users, and so the order of the submitted word among her sweet words. The login server sends a message of the form to a secure server that's named “honeychecker”, for the user and her sweet word. The honey checker will verify whether or not or not the submitted word could also be a word or a honey word. If a honey word is submitted, then it will raise associate alarm or take associate action that is antecedently chosen . The honey checker cannot acknowledge one thing regarding the user’s word or honey words. It maintains one info that contains exclusively the order of truth word among the user’s sweet words

LITERATURE SURVEY

1.Strengthening password Security through Honeyword and HoneyEncryption Technique
Authors: Mrs.Vasundhara R.Pagar Mrs.Rohini G.Pise
Description: In digital era people’s sustenance is totally rely upon net because of speedy growth of it. net services square measure wide utilized by business, government, people. Communication with the various net services is going on through authentication i.e. user name and positive identification. however net services have become vulnerable because of easy hacking of web site through weak positive identification. positive identification is important key to induce authorization however hackers square measure abundant fortunate in positive identification cracking because of the weak positive identification selected by user. To strengthen the positive identification storage, projected system uses Honeyword technique in conjunction with Honeyencryption. Honeywords square measure phoney positive identifications that square measure hold on with original password to lure the offender. just in case offender got the positive identification file however he cannot guest that is that the original positive identification. Alarm is generated to the legitimate user instantly if offender is making an attempt to access the account either one among the Honeyword or wrong positive identification. For cryptography of positive identification Honeyencryption technique is applied that provides a lot of security to positive identification. each try of cryptography of positive identification provides incorrect or false plaintext that confuses the offender with original positive identification. the aim of this study is secure on-line communication by providing robust positive identification security and avoids misuse of user monetary and private information by offender.

2.Generation of Secure and Reliable Honeywords, Preventing False Detection
Author : Akshima_, Donghoon Changy, Aarushi Goelz, Sweta Mishray, Somitra Kumar Sanadhyax
Description: Breach in positive identification databases has been a frequent phenomena within the software package business. usually these breaches go undetected for years. Sometimes, even the businesses concerned aren't tuned in to the breach. Even when they're detected, business such attacks won't invariably be within the best interest of the businesses. This demand a powerful breach detection mechanism. Juels et al. (in ACM-CCS 2013) recommend a technique referred to as 'Honeywords', for detection positive identification information breaches. Their plan is to get multiple pretend passwords, referred to as honeywords and store them in conjunction with the important positive identification. Any login try with honeywords is known as a compromise of the positive identification information, since legitimate users aren't expected to grasp the honeywords akin to their passwords. The key elements of their plan square measure (i) generation of honeywords, (ii) typo-safety measures for preventing false alarms, (iii) alarm policy upon detection, and (iv) testing strength of the system against numerous attacks. during this work, we tend to analyze the restrictions of existing honeyword generation techniques. we tend to propose a brand new attack model referred to as 'Multiple System Intersection attack considering Input'. we tend to show that the 'Paired Distance Protocol' projected by Chakraborty et al., isn't secure during this attack model. we tend to conjointly propose new and a lot of sensible honeyword generation techniques and decision them the 'evolving-password model', the 'user-profile model', and also the 'append-secret model'. These techniques deliver the goods 'approximate flatness', implying that the honeywords generated victimisation these techniques square measure indistinguishable from passwords with high chance. Our projected techniques overcome most of the risks and limitations related to existing techniques. we tend to prove flatness of our 'evolving-password model' technique through experimental analysis. we offer a comparison of our projected models with the present ones below numerous attack models to justify our claims.

3.an Introduction To QR Code Technology.
Author : Sumit Tiwari
Description : QR i.e. "Quick Response" code may be a second matrix code that's designed by keeping 2 points into account, i.e. it should store great amount of knowledge as compared to 1D barcodes and it should be decoded at high speed victimisation any hand-held device like phones. QR code provides high information storage capability, quick scanning, position readability, and plenty of alternative blessings as well as, error-correction (so that broken code can even be scan successfully) and completely different style of versions. completely different types of QR code symbols like brand QR code, encrypted QR code, iQR Code also are accessible in order that user will select among them consistent with their would like. currently recently, a QR code is applied in numerous application streams associated with selling, security, lecturers etc. and gain quality at a very high pace. Day by day a lot of individuals have gotten tuned in to this technology and use it consequently. the recognition of QR code grows apace with the expansion of smartphone users and therefore the QR code is apace incoming at high levels of acceptance worldwide

4.Secured Graphic QR Code with Infrared Watermark
Author: Yu-Mei Wang1,a, Chia-Tsen Sun1,b, Pei-Chun Kuan1,c, Chun-Shien Lu2,d, Hsi-Chun Wang1,e
Description: The barcode is a very important link between world and therefore the virtual world these days. one among the foremost common barcodes is QR code, that its look, black and white modules, isn't visually pleasing. The QR code is applied to product packaging and campaign promotion within the market. There ar a lot of and a lot of stores mistreatment QR code for dealing payment. If the QR code is altered or lawlessly duplicated, it'll endanger the knowledge security of users. Therefore, the study uses infrared watermarking to introduce the infrared QR code info into the express QR code to strengthen the anti-counterfeiting options. the express graphic QR code is made by knowledge concealment with error diffusion during this study. With the optical characteristics of K, one among the four written ink colours CMYK (Cyan, Magenta, Yellow, Black), solely K is rendered in infrared. Hence, we tend to use the infrared watermarking to introduce the implicit QR code info into the express graphic QR code. General QR code reader is also wont to interpret express graphic QR code info. As for implicit QR code, it wants the infrared detector to extract its implicit QR code info. If the QR code is lawlessly traced, it'll not show the hidden second QR code underneath infrared detection. during this study, infrared watermark hidden within the graphic QR code will enhance not solely the aesthetics of QR code, however additionally the anti-counterfeiting feature. It can even be applied to printing connected fields, like security documents, banknotes, etc. within the future.

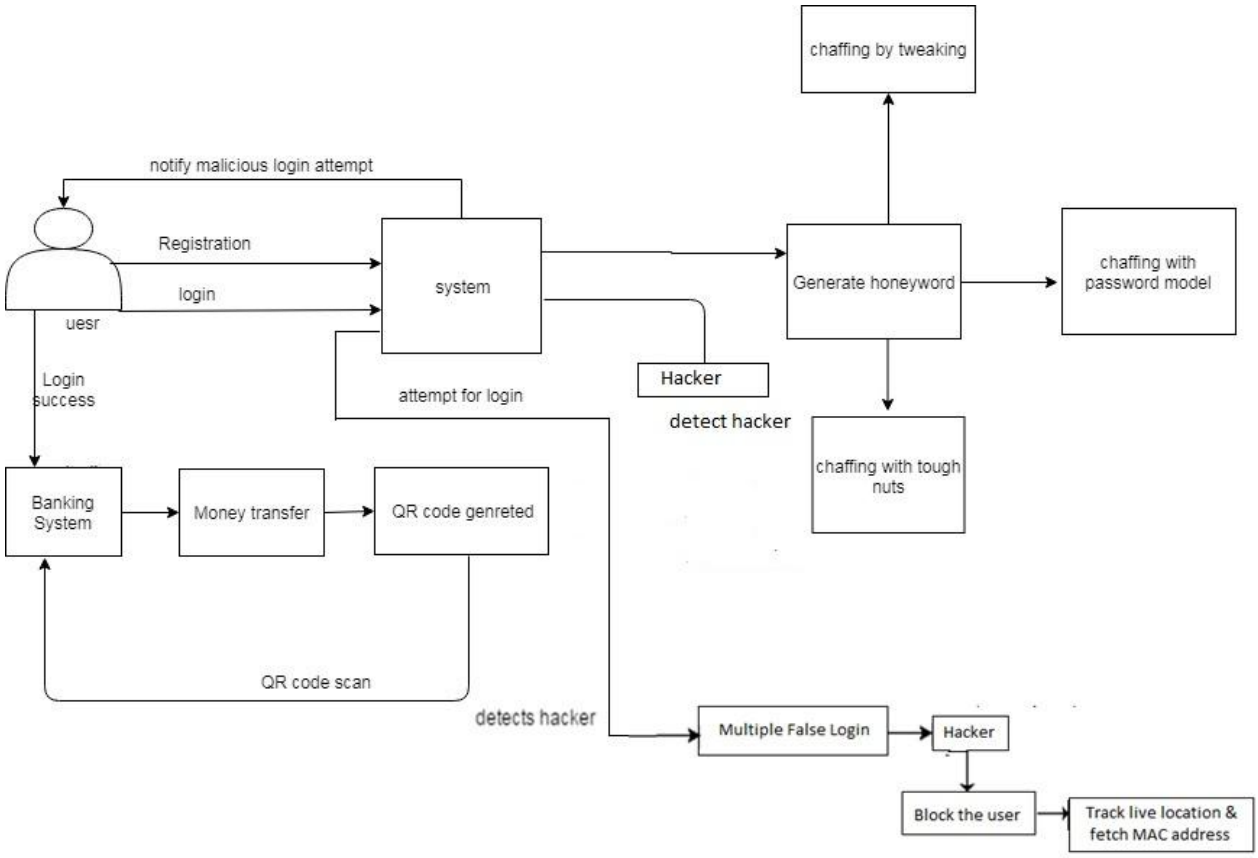
5.Securing Cookies with a mack Address Encrypted ring.
Author: Heng Chinese, Weiting Chen, Zhongjie Ren
Description: Most net services suppliers use cookies to alter the customers' access to the web site. A cookie contains a user's and vital identification which may be wont to establish the user. However, cookies don't seem to be as safe as we tend to take it with a pinch of salt. There ar still some potential safety hazards in cookies. as an example, the contents within the cookies is simply modified, so it'll lead to some safety threats to the user or the web site. This paper proposes a brand new cookie security policy supported a mack address encrypted ring. It will create the cookies have higher confidentiality and better potency. it's additionally straightforward to deploy and meets the user's higher security needs. Most net services suppliers use cookies to alter the customers' access to the web site. A cookie contains a user's privacy and vital identification which may be wont to establish the user. However, cookies don't seem to be as safe as we tend to

take it with a pinch of salt. There ar still some potential safety hazards in cookies. as an example, the contents within the cookies is simply modified, so it'll lead to some safety threats to the user or the web site. This paper proposes a brand new cookie security policy supported a mack address encrypted ring. It will create the cookies have higher confidentiality and better potency. it's additionally straightforward to deploy and meets the user's higher security needs.

SYSTEM OVERVIEW

In this study, we specialise in the safety issue and manage faux passwords or accounts as an easy and value effective answer to note compromise of passwords. king protea is one altogether the ways to identify incidence of a parole information breach. throughout this approach, the administrator by choice creates deceit user accounts to lure adversaries and detects a parole speech act, if anyone of the king protea passwords get used. throughout this paper we've projected a unique honeyword generation approach that reduces the storage overhead and conjointly it addresses majority of the drawbacks of existing honeyword generation techniques. projected model relies on use of honey words to notice password-cracking. we propose to use indexes that map to valid passwords within the system. The contribution of our approach is twofold. First, this methodology needs less storage compared to the initial study. among our approach passwords of various users ar used as a result of the fake passwords, therefore guess of that parole is faux which is correct becomes a lot of sophisticated for an somebody.

PROPOSED SYSTEM



CONCLUSION

We have analyzed the protection of the honeyword system and self-addressed kind of flaws that need to be handled before palmy realization of the theme. during this respect, we've found out that the strength of the honeyword system directly depends on the generation algorithmic program, i.e., flatness of the generator algorithmic program determines the prospect of identifying the correct secret out of many sweetwords. Another purpose that we would value more highly to stress is that printed reaction policies simply just in case of a honeyword entrance are going to be exploited by associate degree mortal to appreciate a DoS attack. this could be an important threat if the prospect of associate degree mortal in touching a honeyword given the many parole is not negligible. To combat such a drag, to boot known as DoS resistance, low probability of such an event ought to be secure. this might be achieved by victimization unpredictable honeywords or fixing system policy to attenuate this risk. Hence, we have noted that the protection policy need to strike a balance between DoS vulnerability and effectiveness of honeywords. what's additional, we have incontestible Keylogging or

keyboard capturing is that the activity of recording (or logging) the keys smitten on a keyboard, ordinarily throughout a closelipped technique that the individual utilizing the keyboard is unconscious that their activities square measure being determined. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There square measure varied Keylogging techniques, extending from hardware and package based mostly methodologies to acoustic examination. likewise as human in authentication protocols, whereas guaranteeing, is not straightforward in light-weight of their restricted capability of calculation and remembrance. we tend to tend to exhibit however careful image outline can improve the protection likewise as a result of the convenience of authentication. we tend to propose a pair of visual authentication protocols: one may well be a one-time-password protocol, and thus the opposite may well be a password-based authentication protocol. Our approach for real arrangement: we tend to tend to had the aptitude attain to associate degree abnormal state of straightforward use whereas fulfilling demanding security necessities.

REFERENCES

[1] D. Mirante and C. Justin, "Understanding password database compromises," Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, New York, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.
[2] A. Vance, "If your password is 123456, just make it hackme," New York Times, Jan. 2010.
[3] K. Brown, "The dangers of weak hashes," SANS Institute InfoSec Reading Room, Maryland US, pp. 1–22, Nov. 2013, [Online]. Available: http://www.sans.org/reading-room/ whitepapers/authentication/dangers-weak-hashes-34412.
[4] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in Proc. 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.
[6] 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.
[7] C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in Proc. 23rd Int. Inform. Security Conf., 2008, pp. 681–685.
[8] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-resistant password management," in Proc. 15th Eur. Conf. Res. Comput. Security, 2010, pp. 286–302.
[9] A. Juels and R. L. Rivest, "Honeywords: Making passwordcracking detectable," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 145–160.
[10] M. Burnett. The pathetic reality of adobe password hints. [Online]. Available: https://xato.net/windows-security/adobe-passwordhints,2013.

