International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Securing System using Honeyword and MAC Address

Heena Ghare[1], Pallavi Ghuge[2], Sayali Kadu[3], Harshal Kesarkar[4], Krishna Tayade[5]
[1, 2, 3, 4]BE Students, Computer Department, NMIET, Pune
5Assistant Professor, Computer Department, NMIET, Pune

Abstract: ***To overcome the problem of online transaction fraud, introducing a honeyword mechanism to detect an adversary who attempts to log in with cracked passwords. A new password is a combination of existing user passwords called honeywords. Fake password is nothing but the honeywords basically, for each username a set of sweet words is constructed such that only one element is the correct password and the others are honey words (decoy passwords). 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. Honeywords are used to detect online transaction frauds. Each user account has a legitimate password stored in the form of honeywords. If attacker Attack on password i.e. honeys words it cannot be sure it is real password or honeyword. In this study, we to examine in detail with careful attention to the honeyword system and present some comment to focus be used weak points. Also, focus on pragmatic password, reduce storage cost of password, and an alternate way to choose the new password from existing user passwords. We are also designing the new approach here that we will generate the QR code for money transfer instead of OTP once QR code is scan by the banking system, the amount will be transferred to the respective account.***
Keywords: Honeyword Password security, QR code, IP Tracing, MAC Address Tracing, Live Location

I. INTRODUCTION

Nowadays there is rapid growth in usage of the Internet, it has become one of the most prominent channels for communication among the mass. In this 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 with some complex mechanisms. Hence, for an adversary, it must be hard to invert hashes to acquire normal plain passwords. The second point is that a secure system should detect whether a password file exposure incident happened or not to take appropriate actions. In this study, we focus on the latter issue and deal with fake passwords or accounts as a simple and cost-effective solution to detect a compromise of passwords. When a user sends a login request, the login server will determine the order of her among the users, and the order of the submitted password among her sweet words.

The login server sends a message of the form to a secure server which is called “honey checker”, for the user and her sweet word. If a honeyword is submitted, then it will take an action that is previously chosen. The honey checker cannot know anything about the user’s password or honeywords. It maintains a single database that contains only the order of the true password among the user’s sweet words. The Qr code is a matrix type of bar code or two-dimensional code that can store data or information. QR Code is designed to be read by smartphones. QR stands for “Quick Response” as the name itself indicating that the code contents should be decoded very quickly with high speed. The QR code is first designed in 1994 for the automotive industry in Japan. It is a machine-readable optical label that contains information about the item to which was it attached. The QR Code is used for various application stream related to marketing, security, academics, etc. QR Code can handle a range of data, not only the alphabetic character but also numbers. QR Code stores the data horizontally and vertically, it is capable to contain alphabetic characters over 100 times the amount of data held by traditional id barcode. Benefits using QR Code are fast reading speed, high accuracy, and considerable small physical size. Because of all these benefits, the QR Code is more popular nowadays. Nowadays it is most accessible due to availability of decoding software on portable devices such as mobile phone such as the opportunity for users to create a code through QR Code generator websites. A tendency for codes capable of holding more information is rising nowadays. QR Code information capacity depends on the version, ranging from version 1 to version 40. For each version has a different number of modules. Each of them has a different data capacity according to the amount of data and character. Nowadays most of all people use their mobile phones for the online transaction. Mobile browser is a device which enables the user to view websites on their own hand-held device whereas mobile apps are the ones that are to be downloaded on the user’s mobile phone in such a way that once downloaded it may be used anytime and anywhere.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. SYSTEM OVERVIEW

A. Honeyword

An adversary can often use brute-force search to crack the user's password, thus allowing the adversary to impersonate the user. Password cracking is successful in a recent cyber espionage campaign against the New York Times. Ari Juels and Ronald L. Rivest suggested the approach of having multiple passwords for each account, one of them is genuine and others are bogus passwords. Bogus passwords are called as Honeywords. Honeywords are the fake passwords generated by using the following methods:

1) Chaffing with Tough nuts: The numbers and positions of tough nuts are selected randomly. It is expected that the adversary cannot size the whole sweet word set and some sweet words will be blank for her, thereby deterring the adversary to realize her attack. In such a situation the adversary may pause to attempt to login with cracked passwords.

2) Chaffing with Tweaking: Each character of a user password in predicated positions is replaced by a randomly chosen character of the same type like digits are replaced by digits, letters by letters, and special characters by special characters. The number of positions to be tweak is denoted as it should depend on systems policy etc.

3) Chaffing with password model: It is combining the strength of different Honeyword generation methods, e.g. chaffing--a-password-model and chaffing-by-tweaking-digits. By using this technique, a random password model will yield seeds for tweaking-digits to generate Honeyword.

B. MAC Address

The media access control (MAC) address is also called the Hardware address. It is a unique address for each network interface controller (NIC) card (set by Manufacturer). MAC address is a 48-bit number written in hexadecimal format (4bit digits). Hexadecimal format converts every 4 bits into a single digit. The 4 bits require 16 combinations (takes values from 0-15), the digits (0-9, A, B, C, D, E, F) are used. hence the MAC address is 48 bits, it will be written in 12 hexadecimal digits. For example : 68:05:CA:03:19:9C. The machine should have a table that maps the IP address & MAC address within its subnet, this table is nothing but the Address Resolution Protocol (ARP) table.

C. IP Address

The IP address can change depending on the network environment. The IP address identifies the connection of a computer on the internet. There are two types of internet protocol that is, IPv4 is 32 bit & IPv6 is a 128 bits address. RARP protocol can retrieve the IP address of the device.

D. Modules

1) User

a) *Registration:* User will register to the system, at the time of registration user will enter the 3 Honeywords. Also, the system will generate no. of Honeywords with the help of user password by three methods: Chaffing with Toughnut, Chaffing with Tweaking, Tail B.

b) *Login:* If the user entered the right username and password is the honeyword which is generated at the time of registration then the system will allow the user next two times to enter his correct password. Even if after giving three chances user enters the honeyword then the system will lock the account. And he has waited for activation form admin. If the user entered a right username but if the password is wrong also password is not a honeyword then the system will block that particular user and request to admin for activating the account.

2) Admin

a) Admin will activate the blocked user account.

b) Admin will protect the passwords by using Honey Encryption method.

c) The honey encryption methods used by using some passwords+keys.We have generated many to many relationships. And Compare to each key with seed space. Then XOR operation performed.

3) Hacker

a) Hacker will login into the system.

b) Then the hacker will get wrong passwords for a requested user.

4) Honey Tracker

a) It will track the user’s record i.e. number of wrong passwords and number of honeywords for particular user login.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

III. SYSTEM ARCHITECTURE

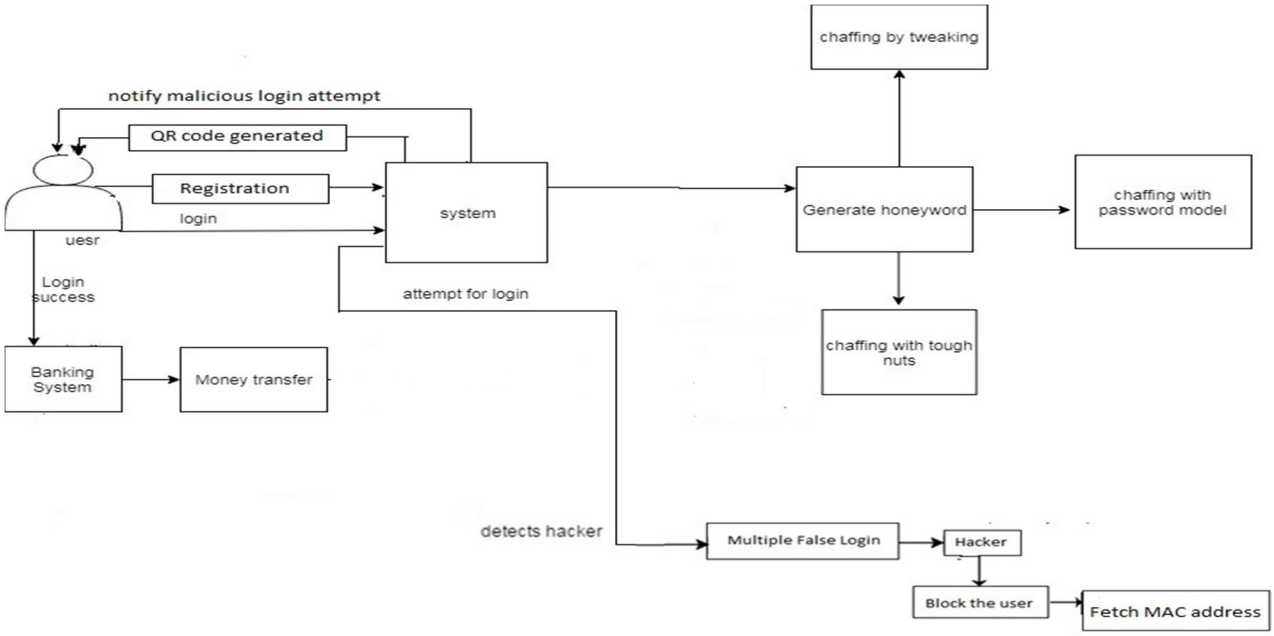

Fig.1. System Architecture

IV. IMPLEMENTATION

In this paper, the implementation is based on password protection for any online transaction systems. The transactions are securely done with the help of honeyword. In this paper, while doing the registration the system will ask for three honeywords which user has to provide. After getting the honeyword, the system automatically develops more honeywords using the user's password and honeyword. The main use of honeyword is that they confuse the hacker and protect the password from being decoyed. And if a hacker is trying to get access, then the user gets an E-mail with the information of IP address and MAC address of the system from which hacker is trying to hack the password.

A. Algorithm

1) Step 1: User registers with username and password.
2) Step2: Original password is assigned a random position.
3) Step3: The last 3 digits of the password are replaced those are the number of characters to be tweaked.
4) Step4
a) A random number between 33 to 126 is assigned to the last character of the password.
b) The original character is been replaced by the ASCII value of the randomly generated number.
5) Step5: Repeat step 4(a) and (b) for the last three characters of the password.
6) Step6: Repeat steps 3 to5 for n number of Honeyword.

B. Mathematical Model

Let S be the system S= { ss | I,O,F }
I:- Input for the system
O:- Output from the system
F:- Function of the system
I= { i E I | set of characters and numbers}
O= { o E o | Output of system function}
F= { f E f | H ,L, Otp, Ft, Bc }
H :- Honeywords
L :- Login System
Otp :- otp generation

Ft :- Function for transaction
H- { h E h | List function to check the passwords in honeypot}
L – { l E l | function to login}
Otp – { otp E otp | function to generate and send otp}
Ft – { ft E ft | Function to make transaction securely}

V. RESULT

Fig.2. Home Page

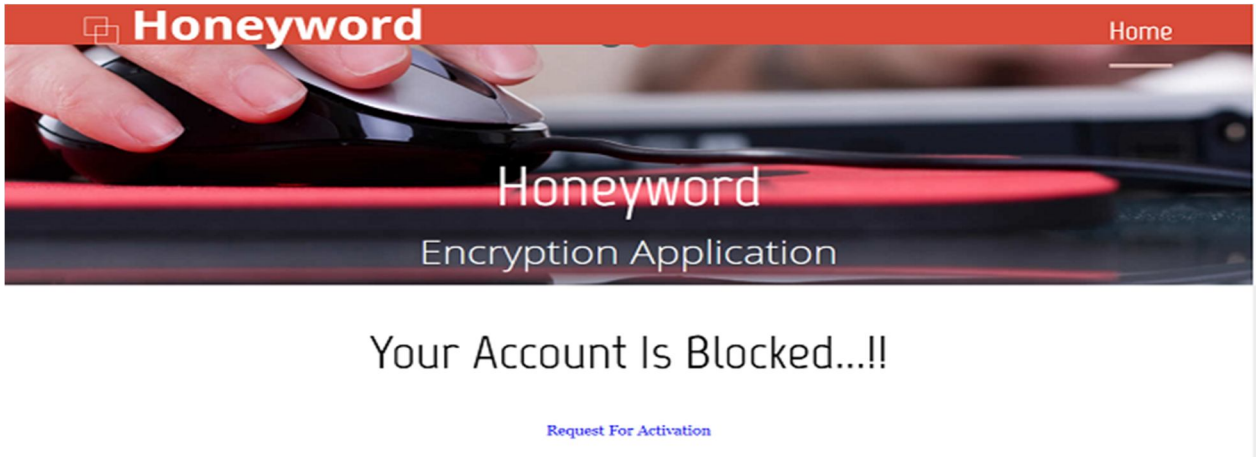

Fig.3. Notification of Blocked Account

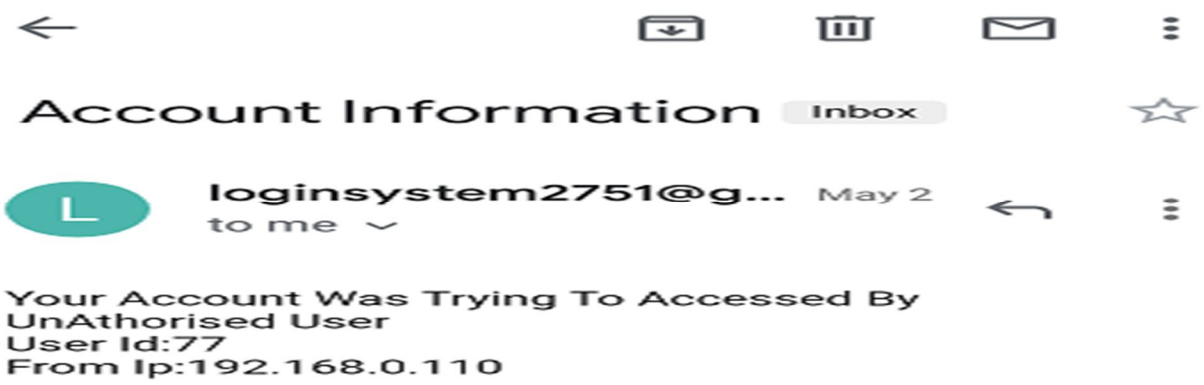

Fig.4. Gmail alert after wrong password

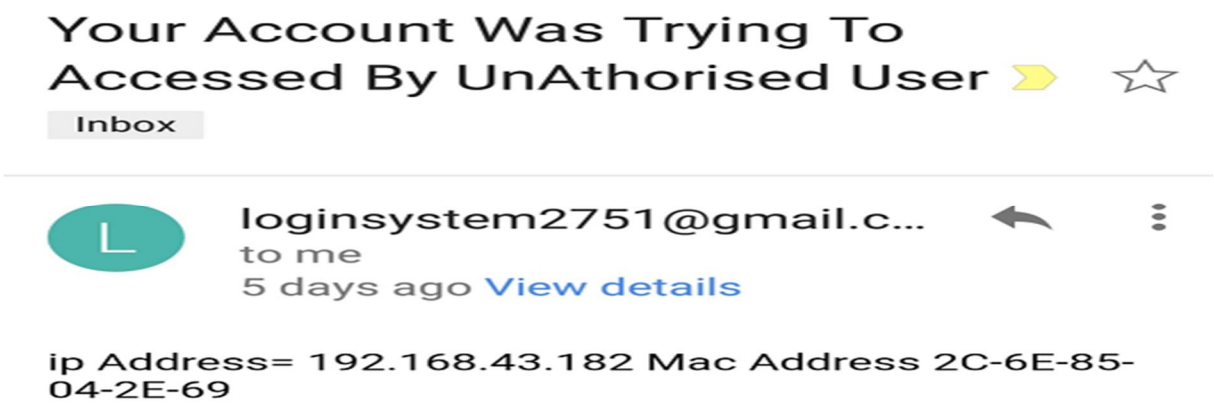

Fig.5. Gmail before hacking system

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we provide security for online transactions using honeywords for password security. The new concept of QR code instead of OTP is been provided in this study. If any mishap happens the user will get the IP address of the hacker and also the live location.

QR code is generated for user while registration. Admin uses QR code to check whether the person who has sent the request for activation is authorized or not.

REFERANCES

[1] Mirante and C. Justin, "Understanding password database compromise," Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, New York, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.
[2] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 145–160
[3] C. Biever, "Project honeypot to trap spammers," New Sci., no. 2485, p. 26, 2005.
[4] Z. A. Genc, S. Kardas, and M. S. Kiraz, "Examination of a new defense mechanism: Honeywords," IACR Cryptology ePrint Archive, Report 2013/696, 2013.
[5] K.Palanivel," A Survey on Password Stealing Attacks and Its Protecting Mechanism", International Journal of Engineering Trends and Technology (IJETT) – Volume 19 Number 4 ,Jan 2015 [4] Ari Juels,Ronald L. Rivest "Honeywords:Making Password-Cracking Detectable"; International Conference on Science and Technology 2015, RMUTT, ACM SIGSAC Conf. Comput.Commun. Security, 2013
[6] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 2, MARCH/APRIL 2016
[7] Kelly Brown," The Dangers of Weak Hashes", SANS InstituteInfoSec Reading Room
[8] Joseph Jaeger, Thomas Ristenpartz ,Qiang Tax," Honey Encryption Beyond Message Recovery Security", February 23, 2016
[9] Juels, A.; Ristenpart, T., "Honey Encryption: Encryption beyond the Brute-Force Barrier," Security Privacy, IEEE , vol.12, no.4, pp.59,62, July-Aug.2014
[10] P. Srisuresh, K. Egevang: "Traditional IP Network Address Translator (Traditional NAT)," RFC3022, 2001.
[11] Ugen J. S. Antsilevich, Poul-Henning Kamp, Alex Nash, Archie Cobbs, Luigi Rizzo: "IP firewall and traffic shaper control program," FreeBSD System Manager's Manual, 2007.