International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 7, July-2014, pp: (228-231), Impact Factor: 1.252, Available online at: www.erpublications.com

A method of password protection using Your Advance Security Hood (YASH)

Saurabh Verma[1], Akhilesh Yadav[2]
[1,2]Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India

Abstract: Human-memorable passwords are a mainstay of computer security. To decrease vulnerability of passwords to brute-force dictionary attacks, many organizations enforce complicated password-creation rules and require that passwords include numerals and special characters. With the many ways we use the Internet; it's easy to consider some passwords less important than others. However, all passwords are important because wrongdoers can piece together the information you store online and use it for their benefit [9]. "A perfect password does not exist; a hacker can crack any password if he has enough time and right "dictionary" or "brute force tools". It is typical task to protect password via brute force attacks, but either they are typical to perform or have number of drawbacks. Protection using Your Advance Security Hood (YASH) was a software based approach to protect password and provide lest option in front of hackers. It can be programmed as an application easily and provide its best results too. This approach was different to all the approaches applied till date [1].

Keywords: Brute-force attacks, Social engineering, Shoulder surfing, guessing, the hoax.

1. Introduction

The complex methods that attackers can use to gain access to your personal information are becoming more easily accessible to wrongdoers and are increasingly effective. It is important to avoid the common mistakes that give these individuals the opportunity to exploit your personal data [10]. In cryptanalysis and computer security, password cracking is the process of recovering password from data that have been stored in or transmitted by a computer system. Cryptanalysis (from the Greek crypto's, "hidden", and analyzing, "to loosen" or "to untie") is the study of analyzing information systems in order to study the hidden aspects of the systems. Breaking is sometimes used interchangeably with weakening. This refers to finding a property (fault) in the design or implementation of the cipher that reduces the number of keys required in a brute force attack (that is, simply trying every possible key until the correct one is found). On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted [7]. The generic name for the collection of tools designed to protect data and password to fraud is security [5]. There are so many approaches used in previous work related to security issues. Some important approaches are mentioned below:

1.1 Gmail security model:

To protect Gmail account by brute force attack, users are asked to provide a recovery email address to allow them to reset their password if they have forgotten it, or if their account is hacked. Google offers a 2-step verification option for security against hacking—that requests a validation code when user accesses their Google account. The code is either generated by an application ("Google Authenticator") or received from Google as an SMS text message, a voice message, or an email to another account.

1.2 Locking Accounts :

To block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. . Account lockout is not the best solution, because someone could easily abuse the security measure. paper is intended for a conference, please observe the conference page limits.

YASH - A software based Approach

YASH was a software based approach to provide better security by giving much facility to user and least options to hackers to crack passwords. It can be programmed as an application easily and provide its best results too. YASH together can fight form password cracking and that's why it is named as Yours Advanced Security Hood (YASH)[1].

In this method user has a mobile phone with a facility of UAC, by which he can activate VMC application that will not allow the hacker to attack and user also has a facility to deactivate this application any time. This process provides fully protection of your password as well as your data. This process also provides the facility to user by any unauthorized person to access your database. This method work as a barrier in front of unauthorized person to locking your data and system. The user CAN PROTECT his ACCOUNT EVEN IF HACKER SOMEDAY GOT users MOBILE PHONE and deactivate his VMC, by simply deactivating users SIM card, this was not possible in dual security where 2nd level of security password is provided by mobile phone as once hacker gives his identification as a valid user there is no way to stop him from using Brute Force attack. However the user may himself forget the passwords which he should be able to recover.

In brute force attack the attackers make repetitive attempts to crack your password. There may be hundreds of attempts per minute to break the password. These types of attacks are done using software tools called “Brute Force dictionaries”[2].

Brute force dictionaries start with first alphabet in the English language with simple letters “a” ,”a” and so on, and then eventually moves to words like apple, airplane etc. this brute force dictionaries tries every possible combination to break the password, given enough time it can break any password. This theory can work more than a lot, your consciousness regarding to password security and YASH together can fight form password cracking and that’s why it is named as Yours Advanced Security Hood (YASH) [1].

We are not using mobile phone to again provide a password (as in Gmail dual security); because once it gets hacked there is no way to stop hacker. We are not locking any account, where user will face numerous problems. But in here we are providing a method that is simple to program, easy to use and strong enough to stop hackers from doing password cracking of any online account through brute force and dictionary attacks, which is one of the greatest problems of the time.

The Working Model explanation with an Example:

This method work on following two methods:

1. In this proposed method we will describe each aspect. We have a device that store unsuccessful attempts to access the data called teller device. We create a function that store the unsuccessful attempts which is enter by any person. This indicates that the value of final counter (FC) gives value of each error in writing incorrect writing password. Let’s take that maximum value of FC to be as x, and a history counter (HC) that will increment only when a wrong password is inserted. Then if number of counts in HC>x then the person is unauthorized one and we will move to second step. If number of counts in HC<x then the person has still chances to prove himself as correct and can get access to the data.

2. To protect your password from hackers we go to second method called VIRTUAL MACHINE CROSSCHECKING (VMC). After entering password, if password value is incorrect than HC value, than the VMC activated and we get a automatic generated UMC code to my mobile phone. By this method we find fraud person. If person is detected as a fraud he will be never allowed to even reach to actual database carrying the correct password, rather a function will initiated that never matches the password provided by the fraud to the actual password located in database.
Example:

Let’s take Actual password as country and FC=3, HC=3. After entering another password the value of HC=4 hence HC>FC, then VMC will be activated. When VMC activated the UMC code will be send to your mobile phone. Brute force dictionary giving password one by one (BFP) Here until VMC is activated all the given passwords are crosschecked directly to the password written in the actual database holding the correct account and their passwords. Now suppose for the fourth time BFP gives correct password that is Hero, but as VMC is activated following thing happens.

The answer of it is the mobile phone that user is carrying will provide an authorized user a facility; we call it UNAUTHORISED ACCESS CONTROL (UAC). UAC is different than the facility provided by the Gmail though the basic concern is same, in both manners we are trying to get the actual user but here method is more secure than that of Gmail.

2. Proposed Method

Though the YASH model was very secure but there are certain limitations of the model**.** First problem is that in this proposed method if fraud person enter consecutively same password, means system allow the fraud person to access account. This problem remove in the “A method to protect password using YASH”. Second problem is that only initial password which enters by user store in database. If second password is incorrect than this password not be store in database. Hence it is easily crack by fraud person by any technique. Here certain amendments have been suggested in the YASH Process in order to overcome the above problems: The following steps will be followed in the proposed method:

1. Design a login form which will take username and password from user.

2. In the database three attributes for all user will be FC, HC and VMC. FC and HC are counter values. FC- maximum final counter and HC- history counter value.

VMC- it is a flag, as it is set then afterword no password checking is done against original password.

3. The data from login form will be passed to another which will perform certain action on it.

4. If this user's try is unsuccessful then it will increase HC values by one in database and if it is correct it will reset HC as zero.

5. After increasing the HC it exceed thr FC then we will set VMC flag.

6. We store this information that VMC is set, in cookies and send a message to user that VMC is set and he should take appropriate action.

7. Our process check cookies for VMC flag information it is not there than it perform according to 4-6. But if is present than it will not go to database and check password against previously written password.

8. A real user can reset the VMC through UAC.

9. We can check the performance of YASH through a brute force attacking tool which attacks the server with dictionary attack.

3. Methodology

This project need php java-script and a brute force attack tool.

1. first of all we design a login form in php which will take username and password from user.

2. in our database we have three attributes for all user they are FC,HC and VMC. FC and HC are counter values. FC- maximum final counter and HC- history counter value. VMC- it is a flag, as it is set then afterword no password checking is done against original password.

3. the data from login form is passed to another php file (say process.php) which will perform certain action on it.

4. if this user's try is unsuccessful then it will increase HC values by one in database and if it is correct it will reset HC as zero.

5. after increasing the HC it exceed the FC then we will set VMC flag.

6. We store this information that VMC is set, in cookies and send a message to user that VMC is set and he should take appropriate action.

7. our process.php , check cookies for VMC flag information it is not there than it perform according to 4-6. but if is present than it will not go to database and check password against previously written password (this thing can be done by java-script).

4. Conclusion

Using a weak password. Selecting a weak password is like closing your front door but not locking it. A password is weak if it can be guessed easily. The YASH process was depends totally upon VIRTUALISM. It was a software based approach to provide the better security by giving much facility to user and least options to hackers to crack the passwords. But here we feel that the user may himself forget the passwords which he should not find any difficulty to recover. but by this improve method we can easily catch initial password by using UMC code. After VMC deactivation we enter new password. The advantage of this will be clearly enhanced security and it will also be helpful to recover the passwords by using VMC technique by the users.

References

[1]. Yashasvini Sharma1 1(Student of 7th semester, Computer science, Gyan Ganga Institute of Technology and Sciences /RGPV Bhopal, INDIA)

[2]. Y. He and Z. Han, “User Authentication with Provable Security against Online Dictionary Attacks,” J. Networks, vol. 4, no. 3, May 2009.

[3]. N. Bohm, I. Brown, B. Gladman, Electronic Commerce: Who Carries the Risk of Fraud? 2000(3) The Journal of Information, Law and Technology.

[4]. International Journal of Network Security, Vol.8, Authentication against Guessing Attacks in Ad. Hoc Networks.

[5]. Hacking Exposed: Network Security Secrets &Solutions, 5th Edi-tion by Stuart McClure, Joel Scambray and George Kurtz.

[6]. Improving Web Application Security: Threats and Counter-measures**,**Mark Curphey.

[7]. Password cracking - Wikipedia, the free encyclopaedia.

[8]. Brute force attack http://www.mandylionlabs.com/ PRCCalc/

[9]. BruteForceCalc.htm (Accessed date:28-Aug-2012) Fast Dictionary Attacks on Passwords Using Time Space Trade-off. Password Security, Protection, and Management.