IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 1 (Jul. - Aug. 2013), PP 83-89
www.iosrjournals.org

Yours Advance Security Hood (Yash)

Yashasvini Sharma[1]

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

***Abstract**: Hacking of any online account is a practice done by an unauthorized person to get an access in an account of some other person. People says that usually person get hacked because of his own mistake of opening the password before the hackers, some of them are Social engineering, Shoulder surfing, Guessing, The hoax, Accessing your email account from cyber cafes (key logger).*

All the above mentioned topics occur because of either lack of awareness or due to a type of fraud. So people should be very careful all about it. But again there are techniques called as Dictionary attacks and Brute-fore attacks that are done by hackers directly and it is difficult to escape from it. It is clearly mentioned that-

A perfect password does not exist; a hacker can crack any password if he has enough time and right "dictionary" or "brute force tools".

The present work is somewhat different to all the approaches applied till date. Number of Research papers, books etc are containing lots of stuffs to stop cracking of passwords via brute force attacks, but either they are typical to perform or have number of drawbacks. But YASH is totally software based approach and can be programmed as an application easily and provide its best results too. This work is more than a barrier before a hacker; it contains simple logic to prevent not your data only but your password as well. This process provides its user a facility of "my key in my hands".

The work is an approach that uses a type of special mechanism containing both the goodwill of 2-level security used by Gmail and locking sites virtually that can clearly stop this type of hacking (99.9% sure) and can provide a better security by giving much facility to user and least options to hackers to crack passwords anyhow.

***KEYWORDS-** Brute-fore attacks, Social engineering, Shoulder surfing, guessing, the hoax*

I. INTRODUCTION

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". English dictionary words are recombined with thousands of recombination of spellings to form a password by trial and error basis. This kind of attack is best shown in the Hollywood flick National Treasure, were hero tries to break one of the security locks.

Brute force dictionaries start with first alphabet in the English language with simple letters "a" ,"aa" 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.

The biggest question is even the password is strong it is not guaranteed that it cannot be cracked. Means even users are going on with strong password they are not safe. This theory is pretty different and can change trend of security concern regarding to account.

It does not only provide a better way but it is easy to apply, simply saying actually it is a way of providing key directly to the user and nobody can use that key without user's permission . Until and unless user wants nobody can get access to his account. This was difficult to achieve earlier as a big concept of VIRTUALISM is neglected that can be used. 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).

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.

II. Literature Review

2.1 Terminology

Following are the terms used in hacking

Social engineering is the name given to the art of attacking the person, rather than the computer or system. The basic principle is that many people can be talked into giving someone else their id and password if they think it is someone that they can trust.

Shoulder surfing it is exactly what it sounds like. The hacker would simply attempt to look over your shoulder as you type in your password. The hacker may also watch weather you glance around your desk, looking for a written reminder or the written password itself

Guessing -If you use a weak password, a hacker could simple guess it by using the information he knows about you. Some examples of these are: date of birth, phone number, favorite pet, and other simple things.

The hoax - Let's dispose of one technique that is absolutely a HOAX (meaning a fraud: something intended to deceive; deliberate trickery intended to gain an advantage.)

Accessing your email account from cyber cafes-In fact many people loose their email account in cyber cafes. For the owner of the cyber cafe it's just a cakewalk to steal your password. For this he just needs to install a key logger on his computers.

Phishing- The other most commonly used trick for hacking email is by using Fake Login Pages, known as phishing, which is something like the hoax method, the user is asked to enter his login id and password into a fake site.

Dictionary attacks - is when a text file full of commonly used passwords, or a list of every work from the dictionary is used against a password database. However, the strong passwords usually aren't vulnerable to this kind of attack.

Brute-fore attacks - by using this method, a brute fore tool will try every possible combination of letters, number and special characters until the right password is found.

2.2 Goals

The basic goal of password was to prevent data; means if you get password you can access data. There was no option to check whether the person is actual user or a fraud. The goal of YASH is to protect password rather than data, means again it is true that if you get password you can access data, but we are preventing a fraud to get a true password and thus preventing our data.

It is simple to explain. This is a well known story ALIBABA and CHALIS CHOR (40 thieves). Alibaba has a secret treasure assume your valuable data. This was secretly placed inside a cave (account). The cave doors only open when Alibaba enchants a correct password KHUL JA SIM SIM, and correlate it to your password- A correct password provides access to the data. But in this whole story we are facing a problem and that was the door of cave opens even when somebody else enchants the same password and that's how Alibaba can loose all his treasure.

Our goal is to make any misuse of correct password must be ceased.

2.3 Previous Works

1. Gmail security model

To restrict the brute Force by creating a Gmail account, 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. In some countries, such as the United States, the United Kingdom and India, Google may also require one-time use of a mobile phone number to send an account validation code by SMS text messaging or voice message when creating a new account. This requirement to associate a unique recovery email and/or phone number with an account makes it difficult for would-be spammers to set up multiple accounts.

Google also offers a 2-step verification option—for extra security against hacking—that requests a validation code each time the user logs in to 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.

2. Locking Accounts

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. However, account lockout is not always the best solution, because someone could easily abuse the security measure and lock out hundreds of user accounts. In fact, some Web sites experience so many attacks that they are unable to enforce a lockout policy because they would constantly be unlocking customer accounts.

The problems with account lockouts are:

- You cannot lock out an account that does not exist, only valid account names will lock. An attacker could use this fact to harvest usernames from the site, depending on the error responses.
- An attacker can cause a diversion by locking out many accounts and flooding the help desk with support calls. An attacker can continuously lock out the same account, even seconds after an administrator unlocks it, effectively disabling the account.
- Account lockout is ineffective against slow attacks that try only a few passwords every hour.
- Account lockout is ineffective against attacks that try one password against a large list of usernames.
- Account lockout is ineffective if the attacker is using a username/password combo list and guesses correctly on the first couple of attempts.
- Powerful accounts such as administrator accounts often bypass lockout policy, but these are the most desirable accounts to attack. Some systems lock out administrator accounts only on network-based logins.
- Even once you lock out an account, the attack may continue, consuming valuable human and computer resources.

III. The Proposed Method

3.1 Assumptions

After discussing the issues on which we have to work, the first challenge is to detect a fraud person. This is simple to assume that we have a secret room and room is filled with valuable things, we protect its illegal access by providing a lock to a gate. The fraud or unauthorized person surely will not have the idea of correct key. But he has a bunch of keys carrying all types of keys for all types of locks. He will crosscheck the key with lock in trial and error method and this is the approach of brute force attack.

1. So we must have a history teller device that can store number of unsuccessful attempts to access the data, the given number of such attempts give us information that the one who wants to access data is unauthorized.

   So now we have a method to detect the fraud person, the second step will be prohibiting his access to the data, this is difficult to do means when we are working on network it is not possible to shut down system again and again as in computer password or the other is to block the account as a whole. So what to do? We cannot remove the particular account or email-id from the database neither it something like that to prevent anybody from getting access to the site. So means a simple method will not work here. The way we mentioned here is VIRTUAL MACHINE CROSSCHECKING (VMC).
2. To prevent hacker from getting correct password we will go for a new method (VMC).

   Now finally a question arises how the system will detect actual user. 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.
3. Finally the system will detect his correct user by the facility called UAC.

The Working Model explanation with an Example

Now we will describe each thing by elaborating each aspect.

1. We must have a history teller device that can store number of unsuccessful attempts to access the data, the given number of such attempts give us information that the one who wants to access data is unauthorized.

This means that, each account user will be provided with a maximum Final Counter (FC) that contains value of the maximum number of error in writing the correct password that is bearable. 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.

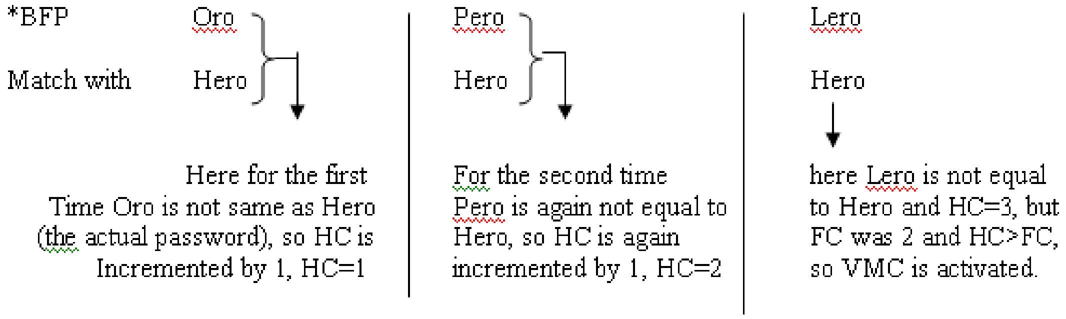
2. To prevent hacker from getting correct password we will go for a new method VIRTUAL MACHINE CROSSCHECKING (VMC).

This is the second rule and will occur if the person trying to get access to the data is detected as invalid one. Here following rules will occur and collectively termed as VIRTUAL MACHINE CROSSCHECKING.

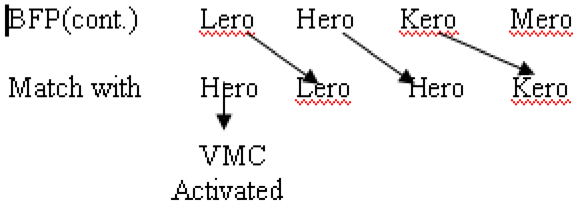
If person is detected as a fraud he will be never allowed to even reach to actual database carrying the correct password, rather a function will initiated that never matches the password provided by the fraud to the actual password located in database.

In the Virtual machine crosschecking the next password after the 1st condition that proves person as invalidate will crosscheck the current typed password to the password he wrote before. Person has no right to write a password twice consecutively. This means none of the passwords is correct for the fraud and the correct password though he typed it somewhere is also not detected. Means we saved our password from getting detected.

Example-
Let's take
Actual password as Hero
And FC=2
If HC>FC, then VMC will be activated
And initially HC=0



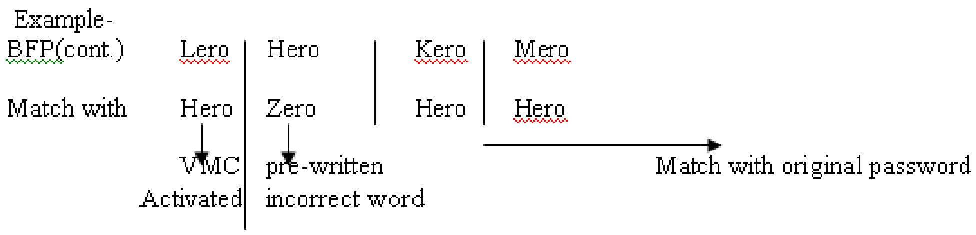
*Brute force dictionary giving password one by one (BFP)
Here until VMC is activated all the given passwords are crosschecked directly to the password written in the actual database holding the correct account and their passwords.
Now suppose for the fourth time BFP gives correct password that is Hero, but as VMC is activated following thing happens.



It is cleared by above example that no 2 passwords can be same (means Hero does not match to Lero, Kero does not match to Hero, Mero does not match to Kero and so on), moreover it is explained previously that PERSON HAS NO RIGHT TO WRITE A PASSWORD TWICE CONSECUTIVELY. Also none of the password provided by the BFP is matched with the actual password located in actual database; it is just like a loop running at some other place.

Now a question may arise that if we are finally misguiding the hacker so instead of going on such a large process why don't we simply do one thing, that is as person is detected as unauthorized instead of matching each word with its previous one, why don't we simply match the correct password to a pre-written incorrect one?

Example:-
Let's take
Actual password as Hero
And FC=2
If HC>FC, then VMC will be activated
And now HC=3, means VMC is activated



For the fourth time if the brute force technique gives the correct password that is Hero, in response to our quest above VMC will compare Hero to a wrong pre-written password say Zero and hacker will be misguided.

But this approach has a serious drawback that every time if the written password is wrong it is matched with the correct password in database. There is only one time when the written password is not matched with the correct one in database that is when the written password is correct, this may give a clue to hacker to crack it easily by some networking techniques.

So that's why VMC process is used.

Now a question arises who will initiate this process? The first answer is valid user himself; he can stop this process too. The second is, it will be initiated automatically if HC>x and gives an information to the correct user in his mobile that VMC has been activated.

The next question arises how user can initiate this process, this is simple an authorized user has one thing that is sure shot with him that is his mobile. He has power to initiate UAC a simple signal that activates above process (VMC), means now no HC will be checked. This process is all about that a valid user is saying that "whatever, but I am not using or even trying to access my account" so it means in other way everybody who is trying to access the account is an unauthorized one. So in one line UAC is all about that user is not accessing his account by this time. When the valid user wants to access his account then via UAC he will deactivate VMC and do the norms.

The above gives answer that how system will recognize his master. So the third rule is verified.

3. Finally the system will detect his correct user by the one and only facility called UAC.

This can be explained by an example-

Let the value of x=3, that is almost 3 trials are provided to access the account.(as HC is 0 initially so we are considering FC=2)

Suppose an authorized person came and mistakenly commits a mistake while writing password for the first time. Still he 2 more chances to write a correct password he does the same and get access to his account.

This time our user does not activated UAC and an unauthorized person somewhere else start a brute force, our user's password is pretty strong so just 3 random or sequential guesses can't produce the desire result and VMC gets activated by itself giving information to valid user in his mobile for the fourth time and now it is clear until valid user himself will not deactivate it via UAC there is no power in Brute force or dictionary checking to crack the password.

Let's say the password is pinky*1984@bugati

Yes enough strong!!

Now the UAC is not active by this time means no VMC is running.

A hacker somewhere writes the email-id of account and start a brute force in random manner

1st he wrote rancho

2nd he wrote cute78

3rd he wrote giraf^78

All the three are wrong the History Teller Machine is counting the number of times when entered password is incorrect and compare it with HC. Here HC=3 and VMC will be activated if the number of times the entered password is incorrect>FC (2).

So VMC activates over here.

In VMC the entered wrong password earlier was giraf^78 for the forth time the brute force technique wrote password blinda54. Now by this time blinda54 will be crosschecked to giraf^78 which obviously is not equal and he can't get access to the account.

Let's say for the 5th time the BF wrote pinky*1984@bugati (which is correct) but the VMC will equate this password to the blinda54 and again the results are not equal.

This was the thing we actually want the password is hidden from hacker, though he had typed it.

Now until user deactivates VMC via UAC there is no way to any user, hacker, and person to get access to account at any time, in any system.

Now the valid user wants to access the account, he knows he has not activated UAC so he simply go to the login page enter his correct id and password but he founds that the system is not accepting his password. He will check UAC by his phone and found that VMC is active; by this time he concluded that somebody was trying to hack my account. Well he is 99.9%secure that no brute force can hack me, if he wants to access the account he will simply deactivate it and can proceed then.

Thereafter he himself activate the UAC , and by now if any unauthorized person wants to access the account even three trials are not provided to him to crosscheck the correct password. The password will remain disguised to him. No correct password means, no access to account.

The example above was taking just one password, while actual YASH works on 2 levels of passwords each of which follows the same rule described above.

Now a question arises that why 2 levels of password are provided. Means a valid user has to type 2 correct passwords to get access to his account. The reason behind this is to increase the complexity. The question arises that why we are concerning about complexity?

The answer is hidden in much powerful security concern.

Suppose that someday somehow our valid user lost his mobile and now it's in the hand of hacker!!! If we were using Gmail security plans we certainly have a chance to get hacked.

Hacker will verify himself as a valid user and startup with brute force or vice-versa. If he got sufficient time for sure you will be hacked moreover once he verified himself as valid user you have no choice to protect your data or account from get hacked, the only thing one can do is transferring all his valuable data to some other account. Not a flexible and easy approach!

Here in YASH concept the hacker can just deactivate the UAC only for HC times. If he press wrong password for more than x times then VMC will activated by itself. He will again have to do same process. Here complexity helps to prevent hacking at least until the valid user deactivate his SIM card and buy a new one (It is a good approach to change password by now).Once you deactivate your SIM card there is again no risk and you are on safer zone. Now because after every 3 wrong attempts hacker has to deactivate the UAC, after deactivating SIM card, he has no right of deactivating UAC and again he is in same condition in which he was earlier.

3.3 RESULTS

1. The history teller device will judge that whether the user is a valid or invalid one with the help of a number called history counter (HC).

2. (I) If the user is valid one he can access the account by writing the correct password in any turn where turn<=x.

2. (II) If the user is invalid one then following 2 conditions can happen

a. If UAC is not activated by then user will be provided x number of turns to write a correct password if he fails to do so, that is he is unable to provide a correct password within x approaches then UAC will be activated by its own.

b. If UAC is activated by the valid user, the invalid one is unable to get access to account.

In both of the cases a Virtual Machine Crosschecking will be activated that hides the actual password and thus hides the data, which is the theme of the application YASH.

3. If the UAC is activated by any of means described above the valid user first of all have to deactivate it to get access to desired account for writing correct passwords.

3.4 The Mathematical Model

When VMC is activated then there is no chance of hacking by either brute force technique or by dictionary hacking. But if the mobile of any valid user goes in the hand of any unauthorized person or hacker then there must be some way to protect data until the valid user invalidate the SIM card, for this 2 passwords are provided with increased complexity, if the passwords are strong and powerful then they will come out as a challenge before hacking more over after x entry of wrong passwords the VMC will be activated. To deactivate it again and again is sure shot time consuming along with finding the correct strong password which will sufficient time to valid user to deactivate the stolen SIM card and preventing his account from getting hacked.

According to following information, for hacking a password

No. of Characters	**Possible Combinations**	**Human Hacker**	**Computer Hacker**
1	36	3 minutes	0.000018 seconds
2	1, 300	2 hours	0.00065 seconds
3	47, 000	3 days	0.02 seconds
4	1, 700, 000	3 months	1 second
5	60, 000, 000	10 years	30 seconds
10	**3, 700, 000, 000, 000, 000**	**580 million years**	**59 years**

Let's assume that our both passwords are of 10 characters and are pretty strong then for sure to crack one password if hacker takes 'a' amount of time, then to crack both the passwords correctly he will take a to the power 2, means square of cracking just one password. This will give more than sufficient time to valid user to deactivate his SIM card and again make his account safe.

IV. Conclusions

4.1 Conclsion

The whole process depends upon VIRTUALISM. Here virtual means once VMC is activated hacker will see as if he is matching his entered passwords to the one written in the database but in actual practice no entered password is matched with the correct one there in database but a virtual loop will run that will show that all the passwords entered by hacker are wrong even correct one is wrong, means YOU HAVE SAVED YOUR PASSWORD.

It is more beneficial than just this, as someday you mistakenly opened your ATM account password before a hacker (via. phishing), then earlier you have no chance to save your money, but here is CHANCE TO SAVE YOUR MONEY, if you have activated your UAC from the starting (because of security concern) no one can get access to your account, even if they are typing correct password. In this period you can transfer your money to some other account or can take other protective measures, once you realized that you are trapped in phishing.

In YASH 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 AVOIDS US FROM LOCKING ANY PARTICULAR ACCOUNT FROM DATABASE.

You CAN PROTECT YOUR ACCOUNT EVEN IF HACKER SOMEDAY GOT YOUR MOBILE PHONE and deactivate your VMC, by simply deactivating your 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.

Moreover here number of problems in locking account also eliminated. Not only this, Virtualism has shown its effect in various fields so why security concern remains untouched?

References

Journal Papers

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

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

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

Books:

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

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

Conference Proceedings

[1] A. Narayanan and V. Shmatikov, "Fast Dictionary Attacks on Human-Memorable Passwords Using Time-Space Tradeoff," Proc.ACM Computer and Comm. Security (CCS '05).

[2] B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks," Proc. ACM Conf. Computer and Comm. Security (CCS '02).

Generic Website

[1] Password cracking - Wikipedia, the free encyclopedia

[2] Brute force attack http://www.mandylionlabs.com/ PRCCalc/ BruteForceCalc.htm (Accessed date:28-Aug-2012)

[3] Dictionary attacks http://www.cryptosmith.com/node/231 (Ac-cessed date: 02-sep-2012)

[4] http://www.dummies.com/how-to/content/a-case-study-in-how-hackers-use-windows-password-v.html
www.iosrjournals.org