Password Guessing Resistant Protocol for Securing System from Bots and Illegal Access

Arya Kumar[1], Prof. A.K.Gupta[2],
[1]*Student, M.E. Computer Engineering, Jayawantrao Sawant College of Engineering, Pune*
[2]*Professor, M.E. Computer Engineering, Jayawantrao Sawant College of Engineering, Pune*

***Abstract*—Attacks on passwords are increasing day by day. Brute force attack and dictionary attacks are the well known attacks. Automated Turing Test (ATT) is effective approach to minimize such attacks and identify malicious logins. But sometimes it may create inconvenience to the authorized user as the user always has to cross or go through the ATTs. So to avoid such inconvenience, a new technique called Password Guessing Resistant Protocol (PGRP) is introduced. It overcomes the drawbacks of existing protocols. By using PGRP authorised users, who are logging from the known system doesn't have to undergo ATTs. The users who attempt to login from unknown system will have to pass through ATTs after three failed login attempts. This could make the password guessing more difficult by the automated programs as well as illegal access can be restricted to a great extend. ATTs, security questions and verification codes are used to increase security**.

***Index Terms*—ATTs, Dictionary Attacks, Online password guessing attack, Brute force attack.**

I. INTRODUCTION

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization. The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator.

There are three types of authentication

- **The Knowledge Factors**: Something the user **knows** (e.g., a password, or personal identification number (PIN), challenge response (the user must answer a question, or pattern), Security question.
- The **Ownership Factors**: Something the user **has** (e.g., ID card, security token, smart cards or access cards)
- The **Inherence Factors**: Something the user **is** or **does** (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier).

Among these authentication techniques for logging into web it is preferable to use something you know method. But alone this method is inefficient as it may result it brute force and dictionary kind of attacks. So this method should be clubbed with ATTs so as to avoid bots and unauthorized users from accessing the account. Although it requires an extra step when logging into an account, the simple practice of entering a randomly generated security code along with a user name and password goes a very long way toward protecting your account and consequently its assets. This is also known as two factor authentication as in this two techniques are clubbed to form a single security system.

A. Background

Online password guessing attacks are common against web applications. The brute force and dictionary attacks are commonly observed attacks in web applications. In these kinds of attack, attackers run automated password guessing programs. For web login servers an attacker generally does not have an offline attack on a particular account. That is, if the attacker wishes to gain access to the account user ID at the login server he must attempt login. Brute-force attacks are very easily detected. For instance, many web sites institute a three strikes rule where three

unsuccessful login attempts will cause access to the account to be locked (at least for some period of time). More sophisticated rules can be applied to detect less obvious attacks, e.g. if the ratio of unsuccessful to successful login attempts exceeds a threshold then particular action to be set up and so on. The brute force attack and dictionary attacks can be avoided by implementing a locking mechanism in the system if it exceeds a number of failed login attempts. But attackers can try only limited number of guesses from a single machine before being locked out, delayed, or challenged to answer Automated Turing Tests (ATTs e.g., CAPTCHAs). ATT is one of the effective defense against automated online password guessing attacks. It restricts the number of failed trials without ATTs to a very small number (e.g. three); this limits automated programs that are used by attackers to three free password guesses for a targeted account.

B. Motivation

Attacks such as brute force and dictionary are commonly known attacks. Such attacks can be avoided to a great extent by using ATTs i.e. Automated Turing Test. But these ATTs are disliked by authorized users as they consider it as an unwanted step. Moreover, by these ATTs only the brute force and dictionary attacks can be avoided. It does not help in securing account from human attacks, i.e. it doesn't secure account from illegal human access. The actual user authentication is not checked.

In the existing system, it uses IP address of the system to make sure whether the system is known system or unknown system. The system is considered as known from which the user makes multiple successful login attempts. The system monitors IP addresses, when the user makes multiple login attempts from the same system that system's IP is stored in known IP list and the new system or the system from which failed login attempts have been made is stored unknown IP list. The failed login attempts are more from the systems of known IP than unknown IP. The drawback of this is attack can be done from the known system as it has more failed login attempts. A human attack is also possible in such cases because of the more failed login attempts permitted. Most cases of stolen information occur by the hacker guessing the victim's password which is known as brute force attack and dictionary based attacks. Software programs can file through dictionaries and word banks to figure out your password, so avoid using words found in dictionaries, even if you can't speak that language. If an identity thief gets to access your password, he instantly gains access to your information. These thieves can not only clear out your savings, they can run up charges in your name under credit cards they opened with your information. So there should be some mechanism which can protect your account from bots and also from illegal access of the account. And even if such access is done then the legitimate user much understand and should be able to prevent his/her account.

C. Drawback of existing system:

Following are the drawbacks of existing system:-

1. This system is giving 30 failed login attempts from the known system that means if attack is happening from an authorized system then the attacker will also be beneficial by getting more failed login attempts.
2. The system itself is setting the IP as known after some successful login attempts. If the user is using a public system, and due to repeated successful login attempts that system's IP will be stored in known IP list. By this if an attack is made from that system then the user will get more failed login attempts.
3. This system is giving protection only from bots and it only helps to avoid brute force attack and dictionary attacks.

II. SYSTEM ARCHITECTURE

The new approach which is being designed helps in user authentication as well as it helps from bots. Here when the user registers to form a new account, a mail is sent to his mail id through the web server. The user needs to verify his account by inserting verification code sent to his mail. Once this is done that means the user is authenticated user. That user's information is being saved to the database. When the user successfully logs in to the system for the next time then he access his account, check log information, upload documents etc. The users IP address is used and saved in the system so as to show the user about the log information. This IP address is also used to

set the IP as known IP and unknown IP. The benefit of this is that, when the systems IP is set as known IP then in this case the user will get failed login attempts only two times, after this the user has to go through ATT test for logging in. If the user inserts correct ATT then the again two failed login attempts is given to the user. In the account the user can change this IP address from unknown IP to known IP, the benefit of this is that the authorized users need not to go through ATTs. This is done because the authorized users dislike ATTs so more attempts are given to them. By default the users IP address is always set as unknown IP. When the user clicks on IP access list to change the IP address to known or unknown, an email is sent to the users email address. That mail contains authentication key. This key and the account password is required for changing the type of IP i.e. known or unknown.

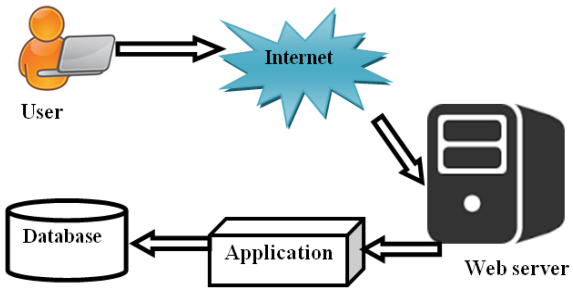

Fig. 1 System Architecture

III. ALGORITHMIC STRATEGY

A. For new user:

1. New user when enters he/she has to fill registration form. This form includes personal details.
2. After finishing with a registration process an email will be send to his/her registered mail id. The user can only login to the account after he/she verifies the account with the code that is sent to his mail.

B. For Existing user tries to log in from the unknown system:

1. The existing user can login in with his/her valid username and password.
2. The existing who logs from an unknown system can make two failed login attempts, after that he/she has to undergo CAPTCHA, then after clearing CAPTCHA. These CAPTCHA will be in the form of random characters. After this the user will be grant access to the account.
3. From the account user can upload and store files of all types.
4. It can also access log information such as IP address of system from which log in attempts are made, status of log in that is in first attempt or number of failed attempts made etc.
5. The user can also set the IP address as known IP or Unknown IP.
6. Repeatedly if user makes two failed login attempts then an email is sent to the registered mail id for verification. After verification two more failed login attempts are permitted then after that if again log in fails then account will be blocked for a particular time.

C. For Existing user tries to log in from the Known system:

1. The existing user can login in with his/her valid username and password.
2. The existing who logs from a known system can make after 3 unsuccessful login attempts. If the user continues to make failed login attempts then a verification email will be send to his/her registered mail id. The user has to verify his/her account. After verifying the account, only 2 attempts will be given, still if it gives wrong credentials then that account will be blocked for a particular time.
3. From the account user can upload and store files of all types.
4. It can also access log information such as IP address of system from which log in attempts are made, status of log in that is in first attempt or number of failed attempts made etc.
5. The user can also set the IP address from known IP to Unknown IP.

D. To access IP list:

1. The existing user can access IP list only after login in with his IP access login details.
2. If the credentials are correct then the users can grant access and change the IP to known or unknown IP.

E. Security at forgot passwords:

1. When the user clicks on forgot password tab then that request is also mailed to his/her registered account.
2. The reset of password can be done only after 24hrs of the request placed.

IV. RESULT

Figure 2 shows a comparison of the previous system and the new developed system on the basis of Security Level, User friendliness, number of ATTs and sending of verification mails. The level of security is high as number of failed login attempts is less. The verification of user through mails make the system more strong. The verification code is send to the user's registered mail id. To protect the system from back doors, the security level has been implemented at the Forgot password attempts also. If the user needs to reset password by clicking on forgot password then the user has to wait for a day to reset the password, meanwhile a mail will be send to the user informing about the request received regarding reset of password.

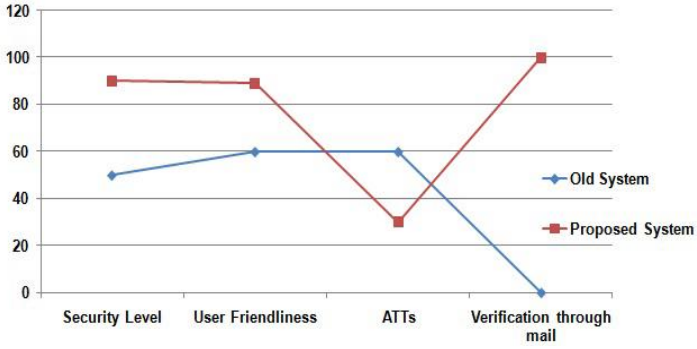

Fig.2 Comparison Result

V. CONCLUSION

ATT based technique is efficient in dealing with brute force and dictionary based attacks. So the new form of PGRP protocol enhances the efficiency of the technique and makes the system more restrictive against the attacks. It helps in a convenient login process for the authorized users as authorized users need not to go through the ATTs from a known machine which increases the usability. The verification code helps in identifying the authorized users. Due to the use of multiple ATTs the systems security is increased. The log information provided to the legitimate users helps to give all the log successful as well as unsuccessful log information so that the user can protect his account by changing the password if some illegal access is made. It can be used in small as well as large organizations. The performance of the system is proved to be efficient. The system provides flexibility for incorporating new features, which may be useful in future enhancement of this work. In this proposed system, only the security mechanism has been shown, so in future these security mechanisms can be used in different websites. In future to give more security more parameters like biometrics, SMS alerts, Email alerts can also be incorporated.

ACKNOWLEDGMENT

We thank anonymous referees whose comments improved this paper.

REFERENCES

[1] Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster,Dos and Donts of Client Authentication on the Web,MIT Laboratory for Computer Science,USENIX Security Symposium,2001

[2] Benny Pinkas and Tomas Sander, Securing Passwords against Dictionary Attacks, Proc. ACM Conf. Computer and Comm. Security (CCS 02), pp. 161-170, Nov. 2002.

[3] Dinei Florencio, Cormac Herley,Baris Coskun, Do Strong Web Passwords Accomplish Anything?, Proc. HotSec,2007.

[4] Yongzhong He and Zhen. Han, User Authentication with Provable Security against Online Dictionary Attacks, Journal of Networks, vol. 4, no. 3,pp. 200-207/May 2009.

[5] Elie Bursztein, Steven Bethard, Celine Fabry, John C. Mitchell, Dan Jurafsky, How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation, Proc. IEEE Symp. Security and Privacy,May 2010.

[6] Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker and Stefan Savage, Re: CAPTCHAs Understanding CAPTCHA- Solving Services in an Economic Context, Proc. USENIX Security Symp.,Aug. 2010.

[7]Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE, Revisiting Defenses against Large-Scale Online Password Guessing Attacks, Published by the IEEE Computer Society/ January/Febbruary 2012.