International Journal of Advanced Technology in Engineering and Science
Vol. No. 06, Issue No. 02, February 2018
www.ijates.com
ijates
ISSN 2348 - 7550

Defences against Password Guessing Attacks in Online System

Japneet Kaur
[1,2]*Guru Kashi University, Talwandi Sabo*

ABSTRACT

Authentication is an important aspect of any application implementation. Because hackers have been attempting to get secret information or private data by stealing passwords in recent years. By continuously monitoring the system or guessing passwords, they are able to obtain secret passwords or authentication keys extremely simply. The network application that uses a login service for authentication requires stronger security to protect the information contained within the application. Because the login screen is the first thing you see when you open any application. If the intruder has access to the login credentials, obtaining all of the data in the system is simple. In the actual world, the number of internet users is quickly increasing. The issue is how safe we are with our personal information, which includes passwords. The major purpose of this project is to prevent password guessing attacks by encouraging users to use better passwords that are harder for unauthenticated users to guess. Automated Turing Tests remained a helpful, easy-to-implement method for detecting automated fraudulent login attempts at a fair cost of difficulty to users. In this study, we argue that existing and planned login methods for dealing with large-scale online dictionary assaults are insufficient. Proposes the Password Guessing Resistant Protocol (PGRP), which was developed after studying previous suggestions aimed at preventing password guessing attacks.

Keywords: ***Password Guessing Attacks, Dictionary Attacks, Brute Force Attacks, Password Guessing Resistance Protocol.***

I. INTRODUCTION

Maintaining privacy data and preserving them with a password has gotten more challenging as the number of internet users in the real world grows. Now we're working on a secure application that uses the Password Guessing Resistant Protocol to protect our personal information (PGRP).

Password Guessing Attacks can be divided into two types

- Brute force attack
- Dictionary attack

1.1 Brute Force Attack

Brute Force is a time-consuming assault in which the attacker attempts every possible combination of upper and lower case characters, numbers, and symbols. During this time, the user is unable to locate any attackers. It's a form of password guessing attack that involves attempting every possible code, combination, or password until the one that works is discovered. As may be seen in Fig. 1.

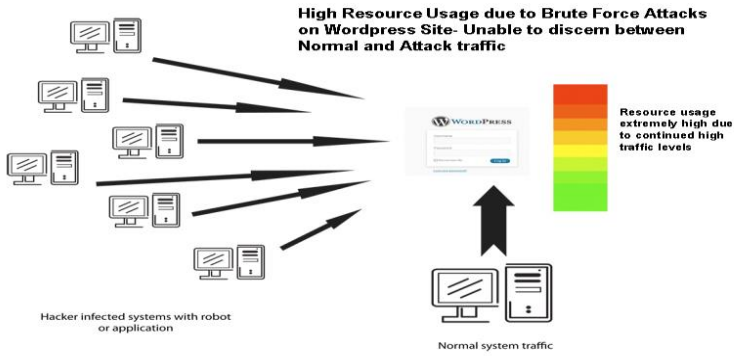

Fig.1 Example for Brute Force Attacks On Wordpress Website

Because of the many potential permutations of characters in the password, a brute force assault is an extremely sluggish sort of attack. Nevertheless, brute force is successful; given enough time and computing capacity, all passwords may be found eventually.

1.2 Dictionary Attack

A dictionary attack is a sort of password guessing attack that identifies user passwords by using a dictionary of common terms. A dictionary attack is a way of getting into a password-protected site by inputting each word in a dictionary as a password one by one.

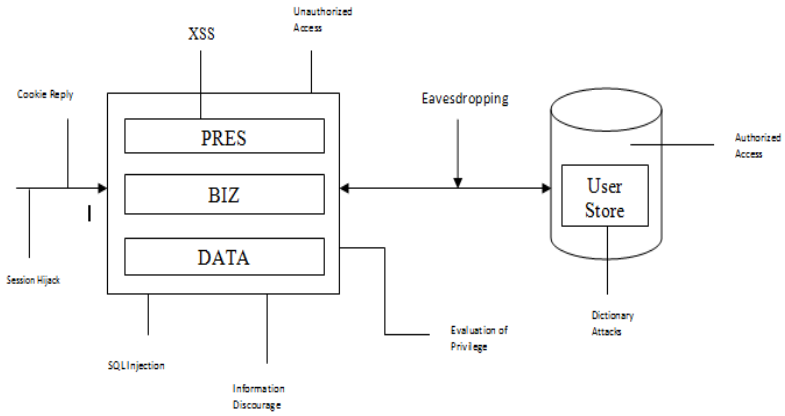

Fig. 2 Example for Dictionary Attack

II. RELATED WORK

Passwords are vitally important in computer security, but they may be easily guessed by automated algorithms, and some hackers have built tools that execute dictionary assaults. In the current system, an automated test is used that people can readily comprehend and pass, but computer programmes are unable to do so. Any software that does well in these tests can be used to guess passwords, posing a security concern. A 'captcha' is an example of such a test. A captcha is a test used in computers to guarantee that the response is created by a human rather than a machine. Captchas are employed in an attempt to prevent automated software from doing activities that damage a system's quality of service. Before being locked, attackers can only try a certain number of guesses from a single machine. Humans, on the other hand, can only be limited by current systems. Captcha can be readily broken by a computer with a high computing competence. A computer will normally require a user to

perform a basic test in order to assure a successful login. These tests are meant to be simple for a computer to create but difficult for a machine to complete, so that if a valid solution is found, it may be presumed that it was submitted by a person. A captcha example is shown in the following image (Fig.3).

Fig. 3 An Example Of Captcha

III. PROPOSED METHODOLOGIES

In the proposed approach, the user is recognised by their IP address, which is recorded on the server as a White list OR in cookies. The Password Guessing Resistance Protocol (PGRP) tracks users via cookies or IP addresses. PGRP (Password Guessing Resistant Protocol) restricts the total number of login attempts (assume three) from unknown remote hosts to only one. The owner and user with administrative privileges are referred to as administrators in our technique of security against online password guessing attacks and related denial of service assaults. The owner just registers with the application provider, and administrators establish user accounts using a web interface. A unique user identifier that is only known by the user and administrators.

The suggested approach is more convenient than the current system since it just requires a few steps for a genuine user to log in:

The major steps concerned in this process are:

- If a trustworthy system fails the initial login attempt, it will be granted two further attempts (totally three chances). If the user fails to log in for the third time, the user will be notified.
- If an unknown system fails the first time it tries to log in, it will be denied further opportunities and notification.

After their password has been reset, a person who has been locked out is able to login again. When a user changes his or her password, he or she is not permitted to choose a new password that has already been used on his or her user account as a permanent or temporary password. This strategy protects against online guessing attacks and related denial-of-service assaults, as well as attacks by unauthorised users or ex-users, as well as providing additional security benefits.

3.1 Password Guessing Resistant Protocol (PGRP)

PGRP Objectives include the following:

- ✓ Even for adversaries with access to massive botnets capable of launching assaults from numerous distant hosts, the Login method should render brute-force and dictionary attacks ineffectual.

- ✓ The protocol should have no discernible effect on usability (user convenience). For example, any additional steps beyond inputting login credentials should be minimal for legitimate users. Increasing the protocol's security must have a negligible impact on login usability.

The protocol should be simple to set up and scale, needing the least amount of computing resources in terms of memory, processing time, and disc space.

The general design behind PGRP is that user does not have to face an ATT challenge for the following two conditions.

- ➢ While the number of failed login attempts for a given username is very.
- ➢ When the remote host has successfully signed in before the maximum number of unsuccessful login attempts has been reached. PGRP, unlike prior protocols, employs IP addresses or cookie identifiers to identify systems from which users have been properly authenticated.
- ➢ The user is not forced to answer an ATT challenge if the number of unsuccessful login attempts for a specific username is below a threshold, even if the login attempt is from a fresh computer for the first time.

3.2 Algorithm Implementation

3.2.1 Input

T1 (DEF=30D), T2 ((DEF=1D), T3 (DEF=1D), K1 (DEF=30), K2 (DEF=3)

Here DEF refers to default parameter value and D refers Day count and K1, K2 ≥ 0

un, pw, cookie // username, password, host browser cookie

W // white list of IP with successful login

FT // table of no. of failed logins per username

FS // table of no. of failed logins by srcIP, username

Begin

Read Credential (un, pw, cookie)

If Login Correct (un, pw) **Then**

If (((Valid (cookie, un,k1,true) ∨ ((srcIP, un) ∈ W)) ∧ (FS [srcIP, un] < k1)) ∨(FT[un]<k2)) **then**

FS [srcIP, un]← 0

ADD srcIP to W

Grant Access (un, cookie)

Else

If (Captchavalue=Pass) **then**

FS [srcIP, un]← 0

ADD srcIP to W

Grant Access (un, cookie)

Else

Display Message (“Please enter valid Captcha Value”)

Else

If ((Valid (cookie, un, k1, false) ∨ ((srcIP, un) W)) ∧ (FS [srcIP, un] < k1)) **then**

FS [srcIP, un]← FS [srcIP, un]+1

Display Message ("Please enter valid Login credentials")

Else If (Valid Username (un) ∧ (FT [un]<K2)) **then**

FT [un]← FT [un]+1

Display Message ("Please enter valid Login credentials")

Else

If (Captchavalue=Pass) **then**

Display Message ("Please enter valid Login credentials")

Else

Display Message ("Please enter valid Captcha Value")

End

The recommended approach of defence against online password guessing attacks and related denial of service attacks is to refer to the owner and users who have been granted administrative access as administrators. The owner just registers with the programme provider, and administrators establish user accounts using a Web interface.

This algorithm can be explained by with the help of flow chart of the algorithm of the discussed protocol is shown below. Character based. It t will be given

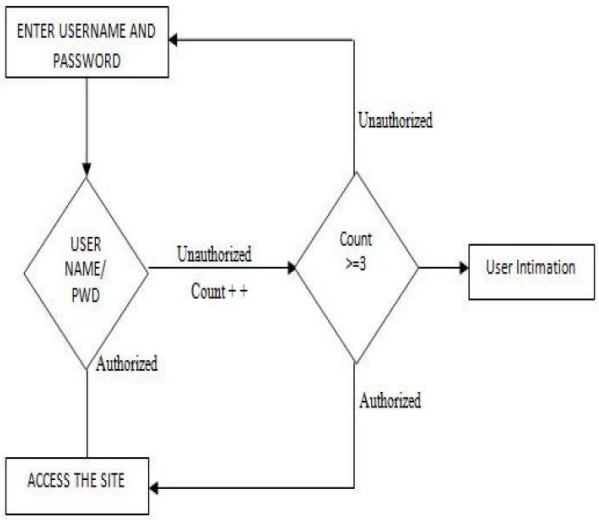

Fig. 4 Flow Chart of PGRP Algorithm

Every user logs in with three identifications rather than the usual two:

- The application instance name is considered as a secret shared by the users of the application instance.
- A user ID is known only to the user and the administrators.
- The user ID is chosen by the administrator who creates the user account, and can be changed by an administrator (by any administrator if the user has no administrative privileges, by the owner if the user is himself an administrator). A password, known only to the user.

A user is barred after a specified number of failed password tries in a row. If there is no successful completed login to the user's account between invalid tries guesses, they are deemed consecutive. Everyone of the subsequent poor guesses must be against the same password; if the password is changed, the counting starts

anew. After her password has been reset, the person who has been locked out is able to log in again. While changing her password, the user is not permitted to use a password that has previously been used as a permanent or temporary password on her user account as the new password. This strategy provides protection against online guessing attacks and related denial of service assaults, as well as other security benefits, such as attacks by unauthorised users.

IV. CONCLUSIONS

Password guessing attacks are becoming more common. We utilise PGRP to put an end to this. It will limit the amount of attempts made by a system or computer and give the genuine user complete access to their account information in a safe manner. PGRP looks to be appropriate for both small and big enterprises with a significant number of user accounts and data. Because PGRP can prevent brute force and dictionary attacks, it improves the security of a user's account.

REFERENCES

[1] Mansour Alsaleh, Mohammad Mannan, P.C. van Oorschot “Revisiting Defenses against Large-Scale Online Password Guessing Attacks”.

[2] Nitin Garg, Raghav Kukreja, Pitambar Sharma “Revisiting Defenses against Large-Scale Online Password Guessing Attacks” on International Journal of Scientific and Research Publications.

[3] Arya Kumar, A. K. Gupta “Password Guessing Resistant Protocol” on Int. Journal of Engineering Research and Applications.

[4] E. Bursztein, S. Bethard, J. C. Mitchell, D. Jurafsky, and C. Fabry. How good are humans at solving CAPTCHAs? A large scale evaluation. In IEEE Symposium on Security and Privacy.

[5] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In USENIX Security Symposium.