Restriction For Online Password Guessing Attacks Using PGRP

Engineering

KEYWORDS:

Josmine mathew

M.Tech Student, Dept of Computer Science and Engineering, Shree Devi Institute Of Technology,Mangalore,Karnataka (India).

ABSTRACT

Now a day's different kind of attacks are increasing. The main types of attacks on password are brute force and dictionary attacks. Prohibiting such type of attacks is a difficult problem. Automated Turing Test (ATT) is efficient technique to reduce such attacks and identify evil logins. But it may disturb the authorized user as the user always go through the ATTs .so preventing this type of inconvenience, it implementing concept PGRP(Password Guessing Resistance Protocol). PGRP reduces the number of login attempt from the unknown remote host. Here It record the ipaddress and no of login attempt, Based on this record PGRP tracking the attacker who is try to access the system. PGRP introducing one more technique is that Question answer challenge.

1. INTRODUCTION

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.PGRP can easily detect brute force attack The brute force attack and dictionary attacks can be prohibited by implementing a blocking mechanism in the system if the number of login attempt goes beyond the limit. But attackers can attempt only limited number of trial from a single machine before being blocked out or challenged to answer Automated Turing Tests (ATTs e.g., CAPTCHAs[1]). 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. However, this is an inconvenient approach to the legitimate user who then has to answer an ATT on the next login attempt. The users generally feel that being an authorized user and putting correct username and password also he/she has to go through the ATTs. Many existing techniques and proposals include the ATT challenge that is difficult for automated programme and easy for human. In PGRP, it limits the legitimate users from a known machine to go through a ATTs while enforces ATTs after some failed login attempts. It helps to avoid the bots by enforcing ATTs to users who try to log in from the unknown users and make multiple failed login attempts. This would be more convenient to the authorized users. PGRP enforces ATTs after a few (e.g., three) failed login attempts are made from machines.. We define known machines as those from which a successful login has occurred within a fixed time period. This can be idenfied by ip address stored on each machine .PGRP to increase the number of ATTs for password guessing attacks and meanwhile to decrease the number of ATTs for legitimate login attempts.

PGRP defines 2 type of systems that are known system and unknown system. It define known machines as those from which a successful login has occurred within a fixed period of time. These are identified by their IP addresses saved on the login server as a white list, or cookies stored on client machines.The authentication procedures do not work well in all systems. so the possibility of account hacking is increases. User should add username and password when the creation of an account. The hacking process will be very easy if the password is not strong. So the user must care about password while the creation time. A brute force attack is a trial method used to obtain information such as password, PIN[3](personal identification no).PGRP concept is used to prevent this type of attacks.

the following measures can be used to defend against brute force attack.
1)Requiring uers to have complex passwords.

2)Limiting the number of times a user can attempt to log in.

3)Temporarily locking out users who exceed the specified maximum number of login attemts.Now a days brute force attack is widespread and ever increasing.Attcks may happen in 2 ways 1)By human 2)By automated machine. The attacker can easily hack account by using automated programme, So that PGRP include ATT challenge(CAPTCHA). PGRP system can analyse the type of attacker based on pass/fail of ATT. The Automated programme cannot pass ATT because human can only read the text shown by the system through capcha. PGRP Providing the security in 2 level. The first one is Question answer challenge and second is OTP challenge. Question answer challenge:The user will add the personal details when the creation of an account eg(pet name,best teacher etc).After the creation of an account user has to login to the system.

if the login of attempt exceed the limit ,then PGRP will ask random question which is entered at the creation time.so here user should enter correct password and answer which is stored before.

if it failed then user account will blocked for certain duration(days or month). so that we can say security level increased by using concept of first level.

OTP Challenge: A one time password is an automatically generated numeric or alphanumeric string of characters that will authenticate the user for a single transaction or session. If the user again try to acess an account which is blocked then PGRP will provide OTP challenge. The valid user can only pass OTP challenge. Because only those people will get the message contain OTP through sms or mail.

Two well-known proposals for limiting online guessing attacks using ATTs are Pinkas and Sander [4] (hereindenoted PS), and van Oorschot and Stubblebine [5] (hereindenoted VS)

II P ASSWORD GUESSING RESISTANT PROTOCOL

This section describe the Objectives, Hypothesis and Features of PGRP[2].

A.Objectives,Hypothesis and features.

- The objectives for PGRP include the following. PGRP protocol should prevent the brute force and dictionary attacks.

- The protocol should limit the number of attempt made from the unknown system.

- The protocol should be easy to implement, deploy and use minimum resources.

- The PGRP should give the notification to the valid user whose system is going to be attack.

- PGRP providing the question and answer challenge when the user tried the password exceed the limit.

1). Hypothesis

Incidents of attackers using IP addresses of known machines and cookie theft for targeted password guessing are also assumed minimum .Authentication on password is not suitable for any untrusted environment (e.g., a keylogger may record all keystrokes, including passwords in a system, and forward those to a remote attacker). We do not prevent existing such attacks in untrusted environments, and thus essentially assume any machines that legitimate users use for login are trustworthy. The data integrity of cookies must be protected (e.g., by a MAC using a key known only to the login server).

2). Features

The proposed protocol minimizes users inconvenience in the login process

- It has a white list of IP addresses.

- If a user sees that someone has tried to log in to his account and have made failed log in attempts then the user can add that IP address to the blacklist. This list may be made only by tracking the log information. This list may consume considerable memory

B. Data Structure and Function Description

1). Data Structures

PGRP contain three data structures:

a). W:This table contain the list of ipaddress and username.

b). FT. This table record the number of failed login attempt from the known system. Here it set as k1.
(example k1=4).

c). FS.This table record the number of failed login attempt from the unknown system. Here it set as k2.In FS table we reduces the failed login attempt than FT.(Example k2=3)

Each entry in W, FT, and FS has a "write-expiry" interval such that the entry is deleted when the given period of time (t1, t2, or t3) has lapsed since the last time the entry was inserted or modified

2). Functions.

PGRP contain following functions.

a).ReadCredential(OUT:usrnme,psswrd,ipaddress). User will enter username and password.

b).LoginCorrect(IN: usrnme,psswrd; OUT: true/false). If the username and password pair is correct then the function return ; otherwise, return false.

c). GrantAccess(IN: un,cookie). The function sends the cookie to the user's browser and then enables access to the specified user account.
d). Message(IN: text). Shows a text message.
e). ATTChallenge(OUT: Pass/Fail). Challenges the user with an ATT and returns "Pass" if the answer is correct; otherwise, it returns "Fail."

f). ValidUsername(IN: un; OUT: true/false). If the username and password.

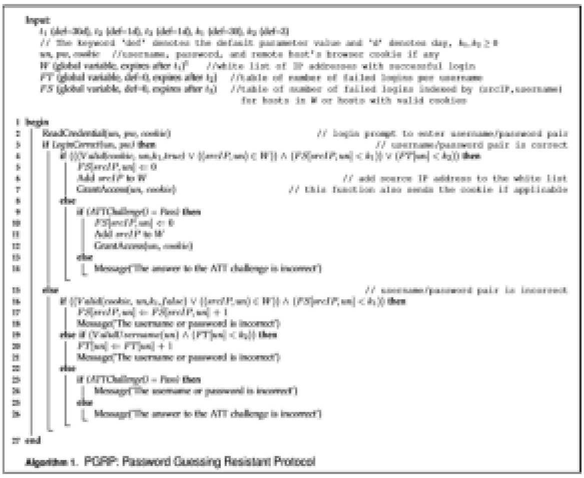
g).Valid(IN:cookie,un,k1,state; OUT: cookie, true/false).

First, the function checks the validity of the cookie (if any) where it is considered invalid in the following cases: the login username does not match the cookie username, the cookie is expired, or the cookie counter is equal to or greater than k1. The function returns true only when a valid cookie is received. If state ¼ true (i.e., the entered user credentials are correct, as in line 4 of Fig. 1), a new cookie is created (if cookies are supported in the login system) including the following information: username, expiry date, and a counter of the number of failed login attempts (since the last successful login; initialized to 0).

Notice that if state ¼ true, the function does not send the created cookie to the user's browser. Rather, the cookie is sent later by the GrantAcces function. If state ¼ false (i.e., the entered user credentials are incorrect, as in line 16 of Fig. and a valid cookie is received, the cookie counter is incremented by one and the cookie is sent back to the user's browser. No action is performed for all the other cases.

3) Purpose

The purpose of doing this project is login protocol should make brute force and dictionary attacks ineffective even for adversaries with access to large botnets (i.e., capable of launching the attack from many remote hosts). The protocol should not have any significant impact on usability (user convenience). For example: for legitimate users, any additional steps besides entering login credentials should be minimal. Increasing the security of the protocol must have minimal effect in decreasing the login usability. The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space.



```
Input:
    $t_1$ (def=30d), $t_2$ (def=1d), $t_3$ (def=1d), $k_1$ (def=30), $k_2$ (def=3)
    // The keyword 'def' denotes the default parameter value and 'd' denotes day, $k_1,k_2 \geq 0$
    un, pw, cookie  //username, password, and remote host's browser cookie if any
    W (global variable, expires after $t_1$)   //white list of IP addresses with successful login
    FT (global variable, def=0, expires after $t_2$)   //table of number of failed logins per username
    FS (global variable, def=0, expires after $t_3$)   //table of number of failed logins indexed by {srcIP,username}
                                                 for hosts in W or hosts with valid cookies

1  begin
2      ReadCredential(un, pw, cookie)                    // login prompt to enter username/password pair
3      if LoginCorrect(un, pw) then                      // username/password pair is correct
4          if ((Valid(cookie, un, $k_1$, true) ∨ ((srcIP, un) ∈ W)) ∧ (FS[srcIP, un] < $k_1$)) ∨ (FT[un] < $k_2$)) then
5              FS[srcIP, un] ← 0
6              Add srcIP to W                            // add source IP address to the white list
7              GrantAccess(un, cookie)                   // this function also sends the cookie if applicable
8          else
9              if (ATTChallenge() = Pass) then
10                 FS[srcIP, un] ← 0
11                 Add srcIP to W
12                 GrantAccess(un, cookie)
13             else
14                 Message('The answer to the ATT challenge is incorrect')
15     else                                              // username/password pair is incorrect
16         if ((Valid(cookie, un, $k_1$, false) ∨ ((srcIP, un) ∈ W)) ∧ (FS[srcIP, un] < $k_1$)) then
17             FS[srcIP, un] ← FS[srcIP, un] + 1
18             Message('The username or password is incorrect')
19         else if (ValidUsername(un) ∧ (FT[un] < $k_2$)) then
20             FT[un] ← FT[un] + 1
21             Message('The username or password is incorrect')
22         else
23             if (ATTChallenge() = Pass) then
24                 Message('The username or password is incorrect')
25             else
26                 Message('The answer to the ATT challenge is incorrect')
27 end
```

Algorithm 1. PGRP: Password Guessing Resistant Protocol

Fig1:Alogorithm for PGRP

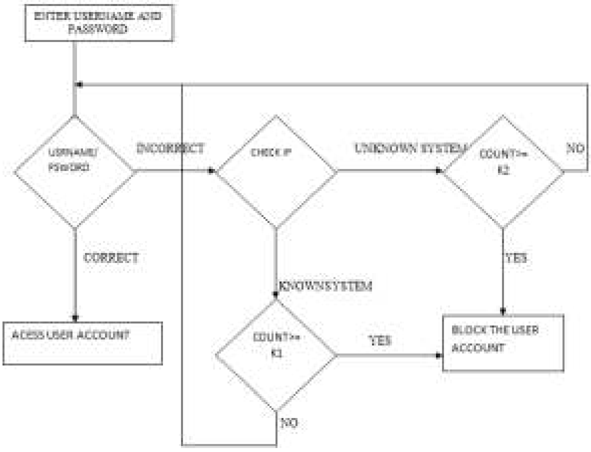


Fig2: Flow chart of PGRP

C)Functional Requirements

- User Registration

In this process user should enter the details such as name, address, phone number, current email address, etc.

- User Login

After the login process the user has to login into their account by using username and password.

- ATT Challenge

ATT is one of the effective defense against automated online password guessing attacks. The users generally feel that being an authorized user and putting correct username and password also he/she has to go through the ATTs. ATT challenge used to identify whether the attack is human or automatic machine.

- Blocking User Account

PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

- Sending OTP

OTP:one time password

It will send the OTP messages to the valid user when the login attempt goes beyond the limit.

- Admin login

Admin login process by using username and password.

- View all Registered user

It will take all datas about user registration id,first name, last name, addresss, email id, password, username, security question, security answer from the database and display to the administrator.

- View all Blocked user

It will take datas about ipaddres,,no of login attempt from known system,no of login attempt from unknown system,date. Then it will display the blocked user.

- Sending Notifications

It will send notification to the blocked user by email or sms.

CONCLUSION

In previous ATT based login protocol, there exist a security usability trade-off with respect to the number of free failed login attempts .PGRP is more restrictive against brute force attack while safely allowing a large number of free failed attempts for legitimate user.

Everywhere we should enter username and password in order to access their account. If the password is not strong then the attacker can easily hack the user account. So the user should care for selecting the password and it should contain keyword like #,.,! etc. In this PGRP completely prevents hacking. It will reduces the number of failed login attempt.PGRP, Temporarly locking out users who exceed the specified maximum number of login attemts.so that security will increase. In order to prevent several kind of attacks it implemented Concept of PGRP.It will limit the total number of failed login attempt and block the user. If he want to acess again then he should pass some challenges(otp,Question answer challenges).

REFERENCE

1.on random field captcha generation micheael a.kouritzin *frasernewton,and bio. | 2 Revisiting Defenses against Large-Scale Online Password Guessing Attacks Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE | 3. B. Pinkas and T. Sander, "Securing Passwords against DictionaryAttacks," Proc. ACM Conf. Computer and Comm. Security (CCS '02), pp. 161-170, Nov. 2002. | 4. P.C. van Oorschot and S. Stubblebine, "On Countering OnlineDictionary Attacks with Login Histories and Humans-in-the-Loop," ACM Trans. Information and System Security, vol. 9, no. 3,pp. 235-258, 2006