ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Defences to Curb Online Password Guessing Attacks

Jesna George Pokkathayil[1], Tanaya Rajmane[2], Rupali Mhatre[3], Devyani Gawad[4], Smita Patil[5]

B.E. Student, Department of Information Technology, Atharva College of Engineering, Mumbai, India[1,2,3,4]

Professor, Department of Information Technology, Atharva College of Engineering, Mumbai, India[5]

Abstract: In this digital world, where huge amount of information is available online, illegitimate access to sensitive information is on the increase. This information is accessed using online password guessing attacks like brute force and dictionary attacks. In this paper we depict the inadequacy of existing protocols and we propose the Password Guessing Resistant Protocol (PGRP) which can effectively prevent these attacks. The system is very stringent for attackers and at the same time is very user friendly for legitimate users. The system prevents cookie theft related issues as it uses IP addresses to track known and unknown machines. It also makes use of ATTs to conquer the guessing attacks

Keywords: Online password guessing attacks, brute force attacks, dictionary attacks, ATT, CAPTCHA

I. INTRODUCTION

The number of online users in real world has increased. Protecting confidential information using password based authentication system has thus become the need of the hour. Password is used as a means for authentication because it is easy for legitimate user to remember.

But, online guessing attacks on password based systems like brute force attacks and dictionary attacks are increasing nowadays .If these password guessing attacks succeed, confidential information stored on password based authentication system become vulnerable to illegitimate access. [1][2]The two most common online password guessing attacks are Brute Force attacks and Dictionary attacks.

A. *Brute force attacks or Exhaustive key search*

It is a trial and error method used to obtain information such as user password. In this attacks automated software is used to generate a large number of consecutive guesses using combination of various upper and lower case letters, special characters, numbers

B. *Dictionary Attacks*

A Dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary of likely passwords.

Both these attacks succeed because most of the users use simple passwords that can be easily guessed. Thus increase in usability has negative impact on security. Thus it is important to prevent online password guessing attacks .In this paper we present a password guessing resistant protocol (PGRP) which provides a security- usability balance which means that, it provides security without hampering usability of the user. PGRP builds on two previous proposals Pinkas and Sander (often called PS) and Van Oorschot and Stubblebine (often called VS). PGRP uses IP addresses to track known and unknown machines. In particular, to limit attackers in control of a large botnet, PGRP enforces ATTs after a few failed login attempts are made from unknown machines .On the other hand, PGRP allows a high number of failed attempts from known machines without answering any ATTs.

Also in case where legitimate user fails to provide correct password, the system provides new password after the legitimate user passes few ATT challenges, this new password is send to legitimate user. This paper thus describes PGRP based system that would prevent online password guessing attacks by using ATTs, tracing IP address and is also user friendly.

It also tries to provide new password safely to the legitimate user in case if the legitimate user fails to provide the right password. The system thus treats known and unknown machine differently thus increasing security as well as user friendliness at the same time which at present most password based authentication systems fail to provide

II. EXISTING SYSTEM

There exist two login protocols that prevent online password guessing attacks These protocols can be explained as under:

A. PINKAS and SANDER(PS) PROTOCOL

This protocol asks the users both legal as well as attackers to pass the ATT first and allows them to enter the username and password if the answer made is correct.[4] The improved version of PS stores browser cookies i.e. the information about the machine of users who had previously login successfully .The cookie is related to username of the last successful login attempts. Once the user requests the login server URL, user's browser sends the cookie back to server .

DOI 10.17148/IJARCCE.2015.4240

The protocol then requests the user to enter a username, password pair. If the pair is correct and a valid cookie is received from browser then user is granted access. If the pair is correct but no valid cookie is received then an ATT challenge must be answered before account access is granted.

1) *DISADVANTAGES of PS PROTOCOL:*

- valid users must also pass an ATT challenge for every login attempt thus affecting user convenience.
- . Performance issues exist as the login server has to generate an ATT challenge for every login attempt.

B. VAN OORSCHOT STUBBLEBINE (VS) PROTOCOL

VS proposed modification to previous protocol [4][3].It tracks failed login per username to impose ATT challenges. The protocol maintains a threshold for failed login attempts. Thus the ATT challenge would be given for incorrect pair depending upon this threshold value.

In addition to it , if credentials entered by the user is correct but the cookie is not valid then the user is asked whether the machine in use is trustworthy and if user uses it regularly. The cookie is stored in user's machine only if user responds yes to the question .This approach helps to reduce password guessing due to cookie theft

1) *DISADVANTAGES of VS PROTOCOL:*

- The legal user always face an ATT challenge once the threshold is exceeded .This feature enables attackers to cause a DOS attack by initiating failed login attempts greater than threshold for each targeted username ,forcing ATT challenges for subsequent login attempts
- Does not restrict the number of failed login attempts for attackers.

III. PROPOSED SYSTEM

The proposed system named PGRP is built upon the existing PS and VS protocols.

A. WORKING

PGRP maintains a white list (W) to distinguish between known and unknown machine .White list maintains a list of pair of source IP address and user name. Known machines are the ones for which a successful login attempt was initiated using a valid username password pair from source IP address .

The rest are treated as unknown machines. PGRP maintains a list called FU which records the number of failed login attempts per username. PGRP maintains a list called FP which records the number of failed login attempts per source IP , username pair. Where source IP address is the valid IP address in the White list or a host with valid cookie and username is valid username attempted from source IP address. Each entry in white list, FU, FP is valid for time interval t1, t2, t3 respectively. This can be implemented using time stamp.
The system also maintains two variables max1, max2 which decides the maximum number of login attempts for known machine and unknown machine respectively.max1 is always greater than max2 because legitimate users must be given more number of trial attempts .If the number of failed login attempts exceeds the threshold values max1 and max2 for known and unknown machines respectively then an Automated Turing Test(ATT) is flashed.
Use of ATTs helps prevent most of online guessing password attacks since these tests are generated by the computer but cannot be solved by it. Mostly CAPTCHAs are used as ATTs .If the answer to the ATT is correct user is granted access.
Except for one case wherein the username is valid but no valid cookie is received or host does not belong to white list. In that case the user is denied access even if answer to ATT is correct.

This feature prevent attacker from initiating brute force attack by restricting the attacker from knowing valid usernames. But if answer to ATT is incorrect then access is denied.
The proposed system distinguishes among the known and unknown machine and thus allows more privileges (More no. of trial attempts) to the known machine. It's a legitimate user friendly system. Figure.1 shows diagrammatic representation of the proposed PGRP system.

The general idea behind PGRP is that except for the following two cases, all remote hosts must correctly answer an ATT challenge prior to being informed whether access is granted or the login attempt is unsuccessful:

1) when the number of failed login attempts for a given username is very small; and

2) when the remote host has successfully logged in using the same username in the past (however, such a host must pass an ATT challenge if it generates more failed login attempts than a pre-specified threshold). In contrast to previous protocols, PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated.

The decision to require an ATT challenge upon receiving incorrect credentials is based on the received cookie (if any) and/or the remote host's IP address. In addition, if the number of failed login attempts for a specific username is below a threshold, the user is not required to answer an ATT challenge even if the login attempt is from a new machine for the first time. Also after passing an ATT challenge a new password is generated for the username and this new password is being forwarded to the user's mobile

DOI 10.17148/IJARCCE.2015.4240

B. PROPOSED SYSTEM DIAGRAM

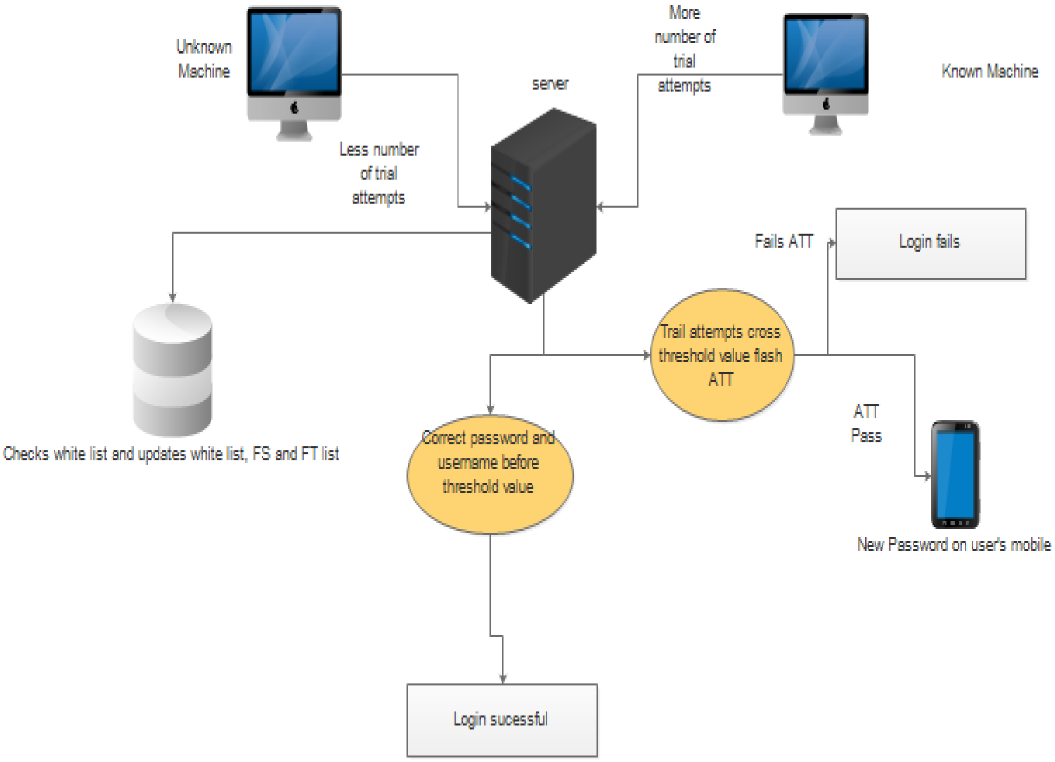
Unknown Machine
server
More number of trial attempts
Known Machine
Less number of trial attempts
Fails ATT
Login fails
Trail attempts cross threshold value flash ATT
ATT Pass
Checks white list and updates white list, FS and FT list
Correct password and username before threshold value
New Password on user's mobile
Login sucessful

Fig. 1 Authentication system based on PGRP protocol

IV. METHODOLOGY

```
Input:
t1,t2,t3//time interval  with default value t1=30 days,t2=1day,t3=1day
w//whitelist  which   expires after time t1
FU//number of failed login attempts per username
FP//number of failed login attempts per username ,souce IP pair
max1//threshold value for known machine
max2//threshold value for  unknown machine.
u//username
p//password

ReadInput(u,p,cookie)
If LoginValid(u,p) then
        If(((valid(cookie,u,max1,true) or ((IP,u)belong to W))and(FP[IP,u]<max1))v(Fu[u]<max2)) then
                Fp[IP,u]=0
                Add IP to W
                GrantAccess(u, Cookie) and reset the password
        Else If ((Valid(cookie,u,max1,false) or ((IP,u) belongs to w)) and  (FP[IP,u]<max1)) then
                        FP[IP,u]=FP[IP,u]+1
                        Alert("The username or  password is  incorrect")
        Else If(ATT()=Pass) then
                        Alert(" username or password is incorrect")
        Else if(ValidUsername9u0and FU[u]<max2)) then
                        FU=FU+1
                        Alert("username or password is incorrect")
        Else
                        Alert(" The answer to ATT is incorrect")
```

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Each entry in W, FU, and FP 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. There are different ways to implement write-expiry intervals.

A simple approach is to store a timestamp of the insertion time with each entry such that the timestamp is updated whenever the entry is modified. At anytime the entry is accessed, if the delta between the access time and the entry timestamp is greater than the data structure write-expiry interval (i.e., t1, t2, or t3), the entry

D.ACTIVITY DIAGRAM

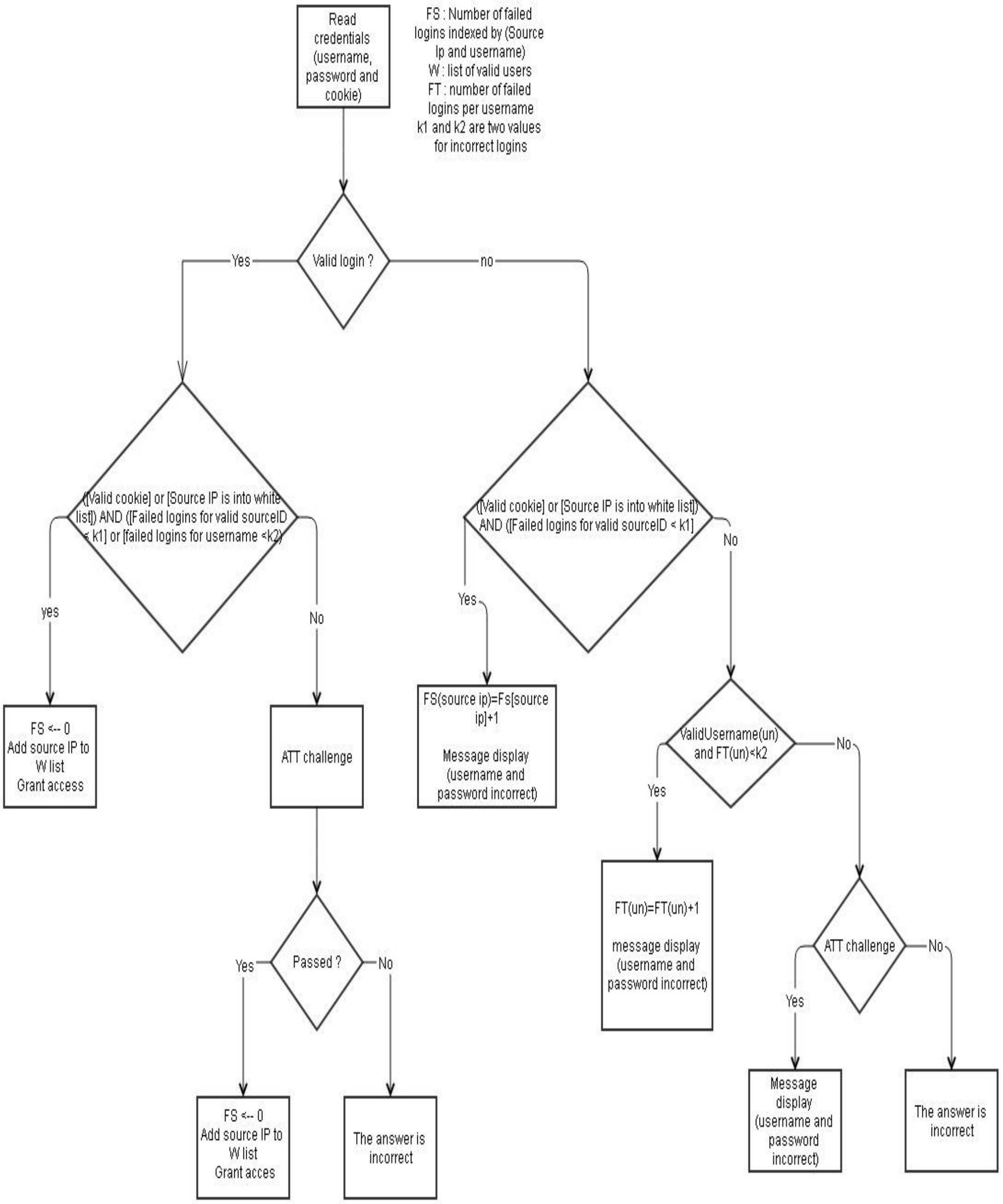
Read credentials (username, password and cookie)
FS : Number of failed logins indexed by (Source Ip and username)
W : list of valid users
FT : number of failed logins per username
k1 and k2 are two values for incorrect logins
Valid login ?
Yes
no
([Valid cookie] or [Source IP is into white list]) AND ([Failed logins for valid sourceID < k1] or [failed logins for username <k2)
yes
No
([Valid cookie] or [Source IP is into white list]) AND ([Failed logins for valid sourceID < k1]
Yes
No
FS <-- 0
Add source IP to W list
Grant access
ATT challenge
FS(source ip)=Fs[source ip]+1
Message display (username and password incorrect)
ValidUsername(un) and FT(un)<k2
Yes
No
Passed ?
Yes
No
FT(un)=FT(un)+1
message display (username and password incorrect)
ATT challenge
Yes
No
FS <-- 0
Add source IP to W list
Grant acces
The answer is incorrect
Message display (username and password incorrect)
The answer is incorrect

Fig. 2 Activity diagram of PGRP based system

DOI 10.17148/IJARCCE.2015.4240

IV. COMPARISON of PGRP with EXISTING PROTOCOL

TABLE 1

Sr no	**Properties**	**PGRP**	**PS**	**VS**
1	Limit the number of login attempts	Yes	No	No
2	Make brute force and dictionary attacks ineffective for large botnets .	yes	no	No
3	Impact on legitimate user convenience.	Less. As legitimate users are given more number of login attempts	Most. As legitimate users as well as attackers need to pass the ATT	More. As legitimate users undergo ATT only if threshold of failed login attempts is reached
4	Distinguish between known and unknown machine	yes	no	no
5	Graphical user interface supported	yes	yes	yes
6	Character user interface supported	yes	no	no
7	Issues related to cookie theft	No .As IP address is used	Yes. As cookies are used, it can be modified or deleted	Yes. As cookies are used it can be modified or deleted

The PGRP can be used in password based authentication system so as to prevent online password guessing attacks.[6]Modifications can be made to the proposed system to enhance its use in the future .In case of account locking the new password can be sent to legitimate users phone or email.

In addition an activity log may be displayed to every legitimate user on login. This feature would alert the legitimate user in case of attacks caused by attacker by logging in correctly from known machine .

Honeypots can be used capture information about the attacker. PGRP system provides stringent security against attackers but at the same time it is very user friendly for legitimate users.

It is better than the existing protocols as it provides good security without affecting user convenience .It can work on any operating system i.e. it is scalable .It is easy to implement i.e. it is deployable .

Online guessing attacks must be prevented because confidential information is always vulnerable to illegitimate access. PGRP is an excellent system that can prevent such attacks

ACKNOWLEDGEMENT

We wish to express our immense gratitude to the range of people who provided invaluable support in the completion of this project. Their guidance and encouragement has helped in making this project a great success. We express our gratitude to our project guide Prof Smita Patil, who provided us with all the guidance and encouragement and making the lab available to us at any time. We are eager and glad to express our gratitude to the Head of the Information Technology Dept. Prof Neelima Pathak, and Dr.Shrikant Kallurkar, Principal for their approval of this project. We are also thankful to her for providing us the needed assistance, detailed suggestions and also encouragement to do the project. We also would like to deeply express our sincere gratitude to Project coordinators.

REFERENCES

[1] M. Alsaleh, M. Mannan and P. C. Oorschot, " Revisiting Defenses against Large-Scale Online Password Guessing Attacks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012.

[2] J. Mabel, C. Balakrishnan, "RESISTING PASSWORD BASED SYSTEMS FROM ONLINE GUESSING ATTACKS ", ISSN :2250-2459 ,IJETAE, Volume 3, Special Issue 1, January 2013.

[3] G. Nitin, K. Raghav, S. Pitambar," Revisiting Defenses against Large Scale Online Password Guessing Attacks ",IJSRP, ISSN :2250-3153,Volume 3,Issue 4,April2013.

[4] Naga Geethika , T. Prem Jacob,"A Efficient Approach For Password Attacks", IJETT, ISSN:2231-5381,Volume 9,Mar 2014.

[5] V. Anusha, T. Lakshmi Priya," FORTIFICATION AGAINST PASSWORD GUESSING ATTACKS IN ONLINE SYSTEM",IJATES,ISSN:2348-7550,Volume 2,Issue 12,Dec 2014.

[6] Arya Kumar, A. K. Gupta," Password guessing Resistant Protocol",IJERA,ISSN:2248-9622,Volume 4,Issue 2,Feb

DOI 10.17148/IJARCCE.2015.4240