International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 5, Issue 11, November 2016 **ISSN 2319 - 4847**

Review of Defense Mechanisms for Online Password Guessing Attacks

Sarita T. Sawale[*1], Pooja K. Khatri[*2]

[*1] Asst. Professor of IT Department, Anuradha Engineering College, Chikhali

[*2]Student of CSE Department, Anuradha Engineering College ,Chikhali

ABSTRACT

With the increasing vulnerability of private and confidential information because of illegitimate access , preventing password guessing attacks is a must. Various protocols have been proposed till date for this purpose. ATT based protocols are used to identify automated malicious attempts but they cause a reasonable amount of inconvenience to the user . In these there exists a security usability trade-off with respect to the number of free failed login attempts..This paper presents a brief view of the existing protocols like PS, VS , PGRP and PAPP and also discusses their inadequacy and drawbacks . The PGRP protocol is very stringent for attackers but it is very user friendly for legitimate users. PAPP protocol uses MAC address of each machine login. If MAC address changes then user can identify intrusion.

KEYWORDS: Brute force attack, dictionary attacks, ATT, PGRP, PAPP.

1.INTRODUCTION

Number . of online users is increasing in the real world. All government, private business organizations are spending lots of money on security of data .i.e maintaining privacy of information is the need of the hour. The most common threat here is that of password guessing attack as password be used as a means of authentication in most web applications.

Password guessing attacks are of two types. Offline and Online password guessing attacks.

Online password guessing attacks are of two types

i) Brute force attack- It is a trial and error method used for guessing online passwords. Here different possible code, combination or password is generated by using automated software until the correct one is found. Many combinations of various upper and lower case letters, special characters and numbers made .It is a very slow but effective type of attack. This type of attack can be easily detected.

ii) Dictionary attack- This attack uses a dictionary of scommon words to detect a user password to defeat an authentication mechanism. It causes a breach of a password protected server by entering each and every word in a dictionary as a password.[1][2] .

2.LITERATURE SURVEY

Below are two common countermeasures against online dictionary attacks.

- Account locking: It is a customary mechanism which prevents the opponent or challenger from trying multiple passwords for a username.. Here when a number of unsuccessful login attempts are made the account gets locked temporarily.
- Delayed response: After receiving the user credentials the server provides a slightly delayed yes/no answer. Thus the attacker will not be able to check sufficiently many passwords in a reasonable amount of time.

These counter measures when used in a single computer environment can be quite useful. But they prove to be inadequate in a network environment. ATT challenges are used in some login protocols to prevent automated programs from brute force and dictionary attacks.[3]

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

A. PINKAS and SANDER (PS) PROTOCOL

Here any user (legal or illegal) first need to clear the ATT before proceeding further. It means if the answer to the ATT test is correct, then the user is allowed to enter the username and password. The improved version of PS stores browser cookies. 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.

DISADVANTAGES of PS PROTOCOL:

- Valid users must also overtake an ATT challenge for every login attempt.
- . Inconvenience for the user.

B. VAN OORSCHOT STUBBLEBINE (VS) PROTOCOL

VS proposed modification to previous protocol .It keeps a track of failed login attempts and maintains a threshold for it. Once the number of failed login attempts exceeds a threshold, ATTs are required. Other modifications were introduced to reduce the effects of cookie theft..

DISADVANTAGES of VS PROTOCOL:

- The valid user has to face an ATT challenge once the threshold is exceeded .
- Does not restrict the number of failed login attempts for attackers. [2][10]

C. PASSWORD GUESSING RESISTANT (PGRP) PROTOCOL

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 max1and 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.[2]

D. PREVENT ATTACK PASSWORD (PAPP) PROTOCOL

Any new user must first do registration and a member table is used to store all data. If a user already exists then he/she has to login using his/her username and password. This entered password is encrypted and stored in data table named member. The PAPP tracks the user account and its activities information with the help of three storage lists.

White List(W)

The successful login attempts by the user from a particular MAC address for that username is tracked and stored in a data table named White List(W). This storage list includes fields like source MAC address and username.

Failed Login Table(FT)

The failed login attempts from any machine for that username is tracked and stored in a data table named Failed Login Table(FT). This list includes username and failed login attempts for that particular username.

Failed Login Table(FS)

The failed login attempts for that username from a particular MAC address is tracked and stored as {username, MAC} pair in a data table named Failed Login Table(FS).

It uses MD5 algorithm for encrypting password and storing it in member table. For better security purpose we are using virtual keyboard to prevent attacks from viruses, Trojan and malware. The programs that might be present in the computer that logs every keystroke from the physical keyboard (keylogger). When user enters username and password at every time, there machine information ie. MAC address, browser history, date and time goes into database and every time it is been checked by database admin. [10]

I. **Comparison of PAPP, PGRP, PS and VS PROTOCOL[2]**

Sr.no	Properties	PAPP	PGRP	PS	VS
1.	Limit the number of login attempts	Yes	Yes	No	No
2.	Make brute force and dictionary attacks ineffective for large botnets	Yes	yes	No	No
3.	Impact on legitimate user convenience	Very less, as ATT test is much easier	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	yes	No	No
7.	Issues related to cookie theft	No. As MAC address is used	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.

3.CONCLUSION

Earlier ATT based login protocols had a security-usability trade-off with respect to the number of free failed login attempts .In spite of the efficiency of ATT based technique for dealing with brute force and dictionary attacks, PGRP proves to be more effective and more restrictive against them. It allows a large number of free failed attempts for legitimate users.. On the other hand PAPP protocol restricts all internal and outside attacks as we use MD5 encryption algorithm. PAPP gives good security for passwords.

REFERENCES

[1] Poonam M. Khairnar,Kirti K. A. Nagare, Ritika V. Agrawal , Ashwini U. Mahale, "Securing password against online password guessing attacks using graphical password",Imperial Journal of Interdisciplinary Research(IJIR) Vol-2, Issue -3 ,2016, ISSN 2454-1362 .

[2] Jesna George Pokkathayil, Tanaya Rajmane,Rupali Mhatre, Devyani Gawad, Smita Patil "Defences to Curb Online Password Guessing Atatcks",International Journal of Advanced Research in Computer and Communication Engineering , Volume 4, Issue 2, ISSN 2278-1021 , February 2015

[3] Nitin Garg, Raghav Kukreja, Pitambar Sharma, "Revisiting Defences against Large-Scale Online Password Guessing Attacks", International Journal of Scientific and Research Publications , Volume 3, Issue 4, ISSN 2250-3153, April 2013 .

[4] 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.

[5] K. Rajakumari, "The Large-Scale Onlinme Password Guessing Attacks with Revisiting DefensesRevisiting Defenses ", Middle East Journal of Scientific Research 20(1): 29-33,2014, ISSN 1990-9233 ,IDOSI Publications,2014.

[6] Benny Pinkas, Tomas Sander, "Securing Passwords Against Dictionary Attacks

[7] Vaishali K. Kosamkar, Prof . V. M .Deshmukh, "Implementation and Analysis of Password Guessing Resistant Protocol(PGRP): A Literature Survey",International Journal of Advance Foundation and Research in Computer(IJAFRC), Volume 1, Issue 12, ISSN 2348-4853 Decmber 2014

[8] Arya Kumar, A. K. Gupta, " Password Guessing Resistant Protocol", International Journal of Engineering Research and Applications, Volume 4, Issue 2(Version 1), ISSN 2248-9622 ,February 2014

[9] Nikitha Basu,Raju. K. Gopal , "Enhanced Security Solution to Prevent Online Password Guessing Attacks ", SSRG-International Journal of Computer Science and Engineering(SSRG-IJCSE), Volume 1, Issue 6 August 2014
[10] Shabana T Pirjade, Prof .Dr.P. K .Deshmukh, "Defend Against Online Password Guessing Atatcks",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, ISSN 2277-128X , September 2014