International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 1; Issue: 4; August –2013

Secured Protocol to Differentiate Known and Unknown Users for Preventing Password Attacks

D.Saranya[*1]
Department of MCA
Adhiyamaan College of Engg
Hosur.
[*1]saranyabca2@gmail.com

G. Nagajothi[2]
Department of MCA
Adhiyamaan College of Engg
Hosur.
[2]nagajothig9@gmail.com

V.Saravanan[3]
Department of IT
P.S.V College of Engg & Tech
Krishnagiri.
[3]v_saravanan18@yahoo.co.in

Abstract- **Password hacking is increased to more percentage when compared to earlier days. Since the users are creating the passwords which is more easy to remember. So this makes the advantage for password hackers to try multiple combinations of words and numerals to hack the password. As well as hackers are trying through dictionary attacks via hundreds of thousands of Nodes. Hence we propose the secured protocol to differentiate known and unknown users in order to prevent dictionary attacks.**

Keywords— *Security, dictionary attacks, captcha, IP address, Cookie*

1. INTRODUCTION

Dictionary attacks on passwords are now widespread and ever increasing. More secured applications like banking application needs to be prevented from such attacks. As on now, when a user types his passwords wrongly for three times his account will be locked temporarily. But this is an inconvenient to a legitimate user once the user forgets his passwords. In order to avoid the inconvenience to the user the server should be able to recognize the known and unknown user. So that whenever a known user types wrong password the server will have to give more number of attempts to the known user. Where as if a unknown user types a wrong password the server has to restrict him with limited number of access.

2. REASONS BEHIND THE WEAK PASSWORDS

Users usually prefer their passwords should be simple and easy to remember. But this is not the suggested way in order to prevent the passwords from hackers. Since hackers are smart enough to guess and use all combination of alphabets and numerals to form a word and try hacking the passwords. So in order to avoid this risks password managers are introduced. A password manager is software that helps a user organize passwords and PIN codes. Passwords are commonly reused by a user across accounts; thus a password used for a low-security site, easily compromised by an attacker, may allow access to a higher-security site . In one of the survey it is found that 96% of the users reuse their passwords across multiple accounts. This is one of the major reasons for password theft.

Few years back password managers were introduced in order to prevent password theft. But there were so many difficulties for a real time user to use this tool. Since this needs to be installed into the client machine in order to use it. But most of the internet users are not preferred to install as because of multiple instruction behind the installation steps. So this not the feasible solutions to prevent the password attack. Single account attack is the concept in which specific account is targeted where as multi account attack is the concept in which attempt to break into multiple accounts. This is the current trend of dictionary attacks.

3. TO PREVENT DICTIONARY ATTACKS USING TEXT GRAPHICS

In earlier days only user id and passwords are used to identify the users. But hackers also trying to login to other account by guessing the user id and password. Similarly hackers were trying dictionary attacks i.e hundreds of thousands of attacks from different nodes. In dictionary attacks there is a more chance that id and passwords can be hacked. In order to prevent this Text graphics

concept is introduced. Where this is also used as one of the identification mechanism. This method differentiates the users from machines. Whereas alphabets and numerals were given in the form of image with distracted shape. In this scenario user has to manually identify the text graphics and enter the word in order to pass the authentication levels. Whereas by dictionary attacks this will lead to failure. TGC (Text graphics character) is the concept used here where humans achieve 95% success in this authentication level where as machines achieve less than 35%.

1. COMMONLY USED USER NAME AND PASSWORDS

Botnets attack is one of the biggest security threat where different type of criminal activities like spamming, identity theft, click fraud, traffic sniffing, key loggings are done by the hackers. Spreading different types of virus and worms are also causing inconvenience to the common users. There are commonly used user name and passwords around the globe. Hence because of this hackers has more chance of attacking other user id and passwords.

"Top 10" usernames observed in SSH attacks		**Top 10" passwords observed in SSH attacks**	
Username	% Used	Password	% Used
root	25.7	%*username*%	56.9
admin	2.1	123456	3.6
test	1.6	password	1.4
a	0.9	tes	0.8
guest	0.9	12345	0.6
user	0.6	test123	0.5
oracle	0.4	123	0.5
postgres	0.4	1234	0.5
webmaster	0.3	passwd	0.4
mysql	0.3	admin	0.4

2. KNOWN AND UNKNOWN MACHINES

Automated Turing Test is the concept in which once the user types the wrong password for more than 3 times, and then it will lead to the lock out. Since this will avoid the password hacking. To control the large botnet attacks the protocol should enforce ATT after three failed login attempts from unknown machines. Simultaneously the protocol should allow high number failed login attempts from known machines. In order to differentiate the known and unknown machines IP address and client cookie concept is used. Whereas known machines are the one in which successful login has occurred within fixed period of time. The protocol should use either cookie or IP address or both to identify the known users. Recently users logging into their online accounts by multiple personal devices like PCs, Smart phones, laptops. When a user uses it from home environment it will have a single IP address which makes IP based tracking more user friendly than cookies. If the number of failed login attempts is less than the threshold then the user should not be asked for the ATT questions. The decision to require an ATT challenge depends upon cookie and IP address.

3. DATASTRUCTURE TO IDENTIFY KNOWN MACHINES

IP address and usernames pairs are stored as List for successful logins IP address and usernames pairs are stored as List for failed logins. Numbers of failed login attempts for a username are stored in a table.

In order to identify the number of failed or successful login attempts, timestamps are also entered along with the each login attempts. When a failed login attempt cross the threshold then it will mandate for ATT. In Client server interaction, browser cookie is used to identify the clients. The server sends the cookie to the user after successful login attempts. For the further interaction between client and server this cookie is used for the server to recognise the particular client. But cookie cannot be always used for server to identify the client since the user may use multiple browsers or multiple operating systems. Sometimes cookie may also be deleted by the user. Source IP address can be used to identify the user machine. Sometimes relying on source IP address is also incorrect since same machine may be assigned with different IP address over different times. Hence it is better to use both browser cookies and Source IP address or only one of them if other is not available is the best way.

There are certain basic questions in which server will verify before ATT questions are challenged to the user, that is if the cookie is valid from the user and the number of unsuccessful login attempts from the user machine IP address for that user name is less than the threshold over a period of time then ATT challenge will not be asked. If the source machine IP address is in the server white list and the number of unsuccessful login attempts from the user machine IP address for that user name is less than the threshold over a period of time then ATT challenge will not be asked. Similarly if the number of failed login attempts from a user name is less than the threshold over a period of time then ATT challenge will not be asked for the user.

4. BLACK LISTING OF UNKNOWN IP ADDRESS OR NOT

It is decided that not to create black list for unknown IP address for the following reasons:

1. The black list may consume considerable amount of memory in the server.
2. Known users from the black list may also be blocked
3. Hosts using dynamic IP address will be more affected when compared to host using static IP address.

8. SECURE PROTOCOL

The following algorithm is the example for secure protocol but it is more inconvenient to the users. Since in the beginning itself the user has to answer the ATT challenged question in order to go the next level of authentication.

1. Begin
2. If ATTChallenge()=Pass then
3. ReadCredential(un,pw)
4. If LoginCorrect(un,pw) then
5. Access is granted to the account
6. Else
7. Message("The username or password is incorrect")
8. Else
9. Message("ATT answer is incorrect")
10. End
11.

Whereas the below protocol is more convenient the end user when compared to the above mentioned protocol. In this protocol username, password and cookie are taken into account for login authentication, if all the three are correct then server will grant access to the application. Where as if any one of the thing is incorrect then it will ask for the ATT challenged questions.

1. Begin
2. ReadCredential(un,pw, cookie)
3. If LoginCorrect(un,pwd) then
4. If Valid(Cookie,un) then
5. GrantAccess(un)
6. Else
7. If ATTChallenge()=Pass then GrantAccess(un)
8. Else Message("Login fails")
9. Else
10. If AskATT(un,pw)=True then
11. If ATTChallenge()=Pass then Message("Login fails")
12. Else Message("Login fails")
13. Else
14. Message("Login fails")
15. end

8. CONCLUSION

In this paper we have discussed about various types of password attacks and its prevention methods. We have analysed the commonly used usernames and passwords which is the main cause for password attacks. Secured and convenient protocol for the user is explored. We have proposed the identification of known user by IP address and cookie. In future the proposed idea has to be updated for more secured protocol.

REFERENCES

[1]. C. Namprempre and M.N. Dailey, "Mitigating Dictionary Attacks with Text-Graphics Character Captchas," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E90-A, no. 1, pp. 179-186, 2007.

[2]. S. Chiasson, P.C. van Oorschot, and R. Biddle, "A Usability Study and Critique of Two Password Managers," Proc. USENIX Security Symp., pp. 1-16, 2006.

[3]. A. Narayanan and V. Shmatikov, "Fast Dictionary Attacks on Human-Memorable Passwords Using Time-Space Tradeoff," Proc. ACM Computer and Comm. Security (CCS '05), pp. 364-372, Nov. 2005.

[4]. M. Casado and M.J. Freedman, "Peering through the Shroud: The Effect of Edge Opacity on Ip- Based Client Identification," Proc. Fourth USENIX Symp. Networked Systems Design and Implementation (NDSS '07), 2007.

[5]. D. Florencio, C. Herley, and B. Coskun, "Do Strong Web Passwords Accomplish Anything?," Proc. USENIX Workshop Hot Topics in Security (HotSec '07), pp. 1-6, 2007.

[6]. K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and Don'ts of Client Authentication on the Web," Proc. USENIX Security Symp., pp. 251-268, 2001.