Volume 4, Issue 9, September 2014 **ISSN: 2277 128X**

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Defend Against Online Password Guessing Attacks

Shabana T Pirjade
Department of Computer engineering,
Rajarshi Shahu College of Engineering,
Pune, India

Prof. Dr. P. K. Deshmukh
Department of Computer engineering,
Rajarshi Shahu College of Engineering,
Pune. India

Abstract— Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users, enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Brute force and dictionary attacks on password-only remote login services are now well-known and ever growing. In this paper, we discuss the drawbacks of existing protocol and proposed a login protocol designed to address large scale online dictionary attacks. 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, We propose a new PAPP (Prevent Attack Password Protocol), derived upon revisiting prior proposals designed to restrict such attacks. The PAPP keeps track of information about the user account and its activities with the help of some data storage lists. PAPP is a new protocol which uses MAC address of machine each login. If MAC address change then user can detect intrusion in between current & previous login. For the password, the proposed system uses the MD5 encryption and decryption method to provide more security to previous approach. The practical work is done under the real time environment to check the performance of this method.

Keyword— ATTs, Brute force attack , Dictionary attack, Online password guessing attacks, PAPP.

I. INTRODUCTION

Online Password Guessing Attacks are the most wide spread and frightening attacks on every browser login and peer to peer systems. Several online attacks include brute force attacks and dictionary attacks. Brute force attacks are those which are occurred by testing every combination of all the possible passwords. Dictionary attacks are those in which all the likely keyword set is formed as a dictionary and compared with the guessed password. For accessing user account user must enter their password and username while login. Each of these transactions are prone to password guessing attacks initiated by remote login systems or bot logins. Many login protocols has been implemented so far to resist such online password guessing attacks. ATTs (Automated Turing Tests) are the common approach used in these protocols to prevent such attacks. They provide secure authentication of username and password in case of remote intrusions as ATTs are capable of detecting human interactions from automated bot logins. Captchas (Completely Automated Public Turing Tests to tell Computers and Human Apart) are the common example for ATTs.

ATTs are used in the assumption that these kinds of challenges are difficult for the bots and easy for most people. But now days there are human solvers and bots which are successful in breaking Captchas. So Captchas are made more complex which are not easily perceivable by users. Therefore the primary aim is to reduce inconvenience to legal users and prevent attackers from attempting remote logins.

There are various kinds of ATT tests like CAPTCHAs (Completely Automated Public Turing Test to tell Computers and Humans Apart), security questions, mobile code verification etc. among which we are using distorted text captcha.

In this paper we propose PAPP protocol in which server insistently rely on MAC address, supplies 3 attempts for login to every client. If 2 attempts are finished then server side notification will be send to registered user. After 3 attempts, user has to face ATT check which contains one security code which server send to legitimate client email address.

PGRP designed to overcome below two categories of attacks:

1. Brute Force Attack: This is kind of attack which is used for guessing online passwords. In this attack different possible code, password or combination is formed until the correct password found. This is very slower kind of attack due to several possible characters combinations in the password. But this attack is effective; and hence given enough time and processing power, all passwords can eventually be identified

2. Dictionary Attack: Another attack which is frequently used to guess the online passwords using the dictionary of common

words in order to crack the end users password successfully. In this the breaking into password protected server by systematically entering every word in a dictionary as a password

A. Organization

In next section II we are presenting the literature survey. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

© 2014, IJARCSSE All Rights Reserved

II. LITERATURE SURVEY

Although online password guessing attacks have been known from the time of the Internet, there is little scholastic literature on prevention techniques.

- In R. Kirushnaamoni [1] gives defense to online password guessing attacks. It uses PGRP protocol to prevent password from offline or online attacks. In PGRP ,the user when try to login from new machine for very first time will not required to answer ATT test. It means that protocol need very less ATT test. Distorted text based CAPTCHA is used.If ATT test is correctly answered, the user is granted access else the user is denied access.
  Pros-Need very less ATT test
  Cons-Login server will be unable to identify the user in all cases.
- Pinkas and Sander (PS) introduced a protocol that requires answering an ATT challenge first before entering the {username, password} pair. Failing to response the ATT correctly stops the client from proceeding farther. This protocol requires the adversary to overtake an ATT challenge for each password estimating try, in alignment to gain data about correctness of the estimate. While this simple protocol is effective against online dictionary attacks assuming that the utilised ATTs are protected, legitimate users should furthermore overtake an ATT challenge for every login try. Therefore, this protocol affects client convenience considerably, and requires the login server to generate an ATT challenge for every login attempt [2].
  Cons-Inconvenient for user
- Van Oorschot and Stubblebine Protocol is considered to be as an improvement for PS protocol. Only if the clientname, password is incorrect the client is inquired to response an ATT dispute. Else the client is allocated get access to. The number of ATT trials inquired to the client is founded on a threshold value called AskATT(). Sometimes legitimate users may be inquired to answer numerous ATT challenges before being allocated which may annoy the client. Therefore this protocol affects client convenience [3].
- Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot [4]In this paper they stated PGRP password protecting protocol. In PGRP ,the user when try to login from new machine for very first time will not required to answer ATT test. It means that protocol need very less ATT test.The user when attempting from a new machine for the first time is not required to answer an ATT challenge, if the no. of failed login attempts for a specific username is below a threshold. There are two cases where ATTs are not needed at all. When the no. of failed login attempts for a given username is very small, no ATTs are required. When the remote host has successfully logged in using the same username in the past, no ATTs are required.
  Pros-Convenient to user as less ATT test is required.
  Cons-No session protection and no intrusion detection.
- The account locking method is used after a couple of repaired number of failed login attempts, the account of the user is locked for some time. This system assists in preventing some of the most widespread online password estimating attacks by limiting the number of incorrect password estimates. On the other hand this system is vulnerable to Denial of Service (DoS) and circulated Denial of Service (DDos) attacks in which an attacker or a assembly of attackers will randomly estimate passwords in alignment to lock the user's account, thereby stopping the legitimate users from logging into their schemes. Another drawback of the account locking scheme is that occasionally the legitimate users may lock their own accounts by mistake. In that case the client will have to either communicate their service providers in alignment to unlock their account or delay till the account is automatically unlocked. regardless of these drawbacks, account locking is still commonly taken up in numerous systems[5].
- In Resmipriya M G, Sangeetha N et.al [6] gives efficient approach to prevent password attacks. It introduced secure session and password protection protocol which ask machine name along with ATT test. If machine name changes then user can detect whether there is intrusion in between current and previous login. The db keeps track of information about the user account and its activities with the help of some data storage lists.
  Pros- Protects the session information and Tracks down any attempt of unauthorized access
  Cons-Requires more time
- In Delayed Response scheme, the server presents a delayed answer to the client request. This may help in preventing an attacker from ascertaining many passwords in a reasonable time. This design is very effective for localizedizedized appliances in which a client has to login utilising a physically attached keyboard. It is less productive in a mesh natural natural environment as the attacker can carry out DoS or DDoS strike very efficiently [7].
- One productive protecting against against automated online password estimating attacks is to constraint the number of failed trials without ATTs to a very little number (e.g., three), limiting automated programs (or bots) as utilised by attackers to three free password guesses for a targeted account, even if different appliances from a botnet are used. However, this inconveniences the legitimate client who then must response an ATT on the next login attempt [10].

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

Our main security goal is to restrict an attacker who is in control of a large botnet from launching online password dictionary attacks. In terms of usability, we want to reduce the number of ATTs sent to legitimate users as much as possible.

In this paper PAPP (Prevent Attack Password Protocol) is presented. Registration is done for new user and all the data is stored in member table.For existing user,login is done using their registered username and password.Password entered by user during registeration is encypted and stored in datatable named member.The PAPP keeps track of information about the user account and its activities with the help of three data storage lists.

© 2014, IJARCSSE All Rights Reserved

White List (W)

The successful login attempts by the user from the 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 MACaddress and username.

Failed Login Table (FT)

The failed login attempts from any machine for that username is tracked and stored in a datatable 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 datatable named Failed loginTable(FS).

This **Fig 1.** represents the entire system architecture:

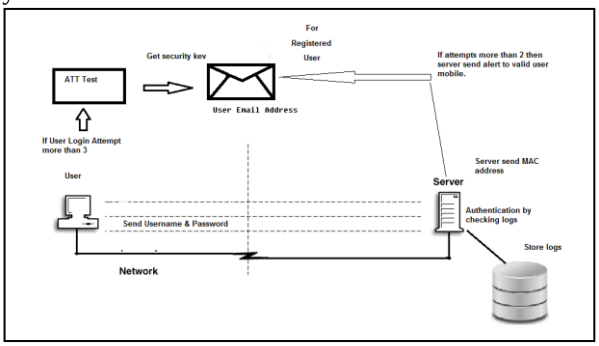

Fig.1 System Architecture

The functional requirements of the system is to defend against the online guessing attacks over the passwords which are been achieved using the PAPP protocol. The requirements are to enter the user name and password for checking authorized user or not. If the user name is correct then the User will be successfully logged in. The Server monitors all details during the communication. If the User misbehaves any Login attempt it will be identified and the misbehaved user will be blocked in the network.

Every user are monitored by the protocol so message transmission will be very clear and very interactive to the Server. If misbehave occur from any user, Server will identify the Misbehaving User or malicious login attempt and avoid that user from the communication progress.

MD5 algorithm is used for encrypting password and storing it in member table. MD5 algorithm is message Digest algorithm. The advantages of this algorithm is that it only encrypt the message it can't decrypt message to original, so chances of getting original data after guessing the keys are equals to "NO.

In previous system instead of MD5 ,AES/DES are used but it has several problem that if hacker got keys and if he attack on data base then they can easily get the password,to overcome this problem we use MD5 algorithm.

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash.

MD5 hash algorithm consist of 5 steps

Step 1. Append Padding Bits
Step 2. Append Length
Step 3. Initialize MD Buffer
Step 4. Process Message in 16-Word Blocks
Step 5. Output

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 i.e. MAC address, browser history, date and time are goes into database and every time it is been checked by database admin.

B. Algorithm

Input Set:

Notations	Description
u	User name
p	password
N(p)	New password
W	White List
Ft	Fail Test
M	Member table
Fs	Fail list
MAC	MAC address
Fc	Fail login count
Δ	Threshold (Δ =3)
M	Member Table

© 2014, IJARCSSE All Rights Reserved

Process

1. If login (u,p) true Then W={MAC,u}
2. If step 1 fails
   Then Ft={Fc, u},
   Fs={MAC,u,Fc}
3. Calculate (Fc, u).
4. If calculate (Fc,u) == Δ true
   Then send N(p) to (u)
5. Go to step(1)
6. If (Fc,u) > Δ true
   Then Go to Step 7.
7. Check credential(u)
8. Pass(u) to ATT Test.
9. If step 8 fails
   Then go to step 10.
10. Block(u).

Functions Details

Calculations of Fc:

If user fails to login then increment Fc by 1 i.e
Fc = Fc+1, where initially Fc =0;
When user successfully login to account then decrement Fc by 1, i.e
Fc= Fc-1.
And update this Fc to Ft and Fs.

Calculation of N(p) :

We have three sets,
Str = { as| as A to Z || as a to z }
Num = {x | 0 x 9 and x is real number}

By combining this two set create new string. For Random selection of Str and Num perform permutation on their respected set. Equation given as follow.

N(p) = $P_{leg}^{Str} + P_{leg}^{Nu}$

where leg = length of password.

***Output Set*:** {Login success, Login Fails, Block account}

In section IV we are presenting the current state of implementation and results achieved.

IV. PRACTICAL RESULTS AND EVIRONMENT

In this section we are presenting practical environment, dataset used, and metrics computed.

A. Input Dataset

For implementation we use database as My SQL.Data sets were collected and the following results were obtained.
Member log files and User log files have been collected as data sets. Log files have been collected from 20 users. Details like each authentication event, including: username, password,Mobile Number,Email Address,date, time, login status (valid or invalid user), MAC address are collected. Users have been classified as valid and invalid users. **Table 1** shows the
Member login files and **Table 2** shows userlog files

TABLE 1 MEMBER

Id	User Name	Password	Mobile Number	Email Address	Registered Date	Time
1	Alice	rewrewt	9923456776	hello@gmail.com	12-02-14	12.20
2	Bob	dsfsdff	9765563483	bob@gmail.com	15-02-14	11.45

TABLE 2 USERLOG

User Name	MAC Address	Attempt Date	Browser History	Login status
Alice	90-E6-BA-CA-4F-8A	12-02-14	Mozilla	valid
Bob	90-E6-BA-DT-8F-3C	16-02-14	IE	valid

TABLE 3 FAIL LIST

User Name	MAC Address	Attempt count	Browser History

© 2014, IJARCSSE All Rights Reserved

Alice	90-E6-BA-CA-4F-8A	0	Mozilla
Tina	90-E6-BA-DT-5F-1C	2	IE

TABLE 4 FAIL TEST

User Name	Attempt count
Alice	0
Tine	2

TABLE 5 WHITE LIST

User Name	MAC Address	Browser History
Alice	90-E6-BA-CA-4F-8A	Mozilla
Bob	90-E6-BA-DT-8F-3C	IE

B. Results of Practical Work

Following figure 2 is showing the performance results for experiment work carried. We have compared proposed approach method against the existing methods. Our proposed method i.e. PAPP is very easy to handle for client. At same time if user faces ATT test is much easier as compared to other protocols. As we use MD5 algorithm for password encryption and virtual keyboard to prevent outside attacks, so ultimately our system is more secure than other system. In figure 2, it is showing that proposed method minimizes the failed login attempts to three only as compared to existing methods given there. Also in figure 2, the total valid uniqueusername entries performances is showing in which with or without performance is varies for methods like VS, PS andPGRP, but for proposed method it doesn't changes and keeping the same level of security.

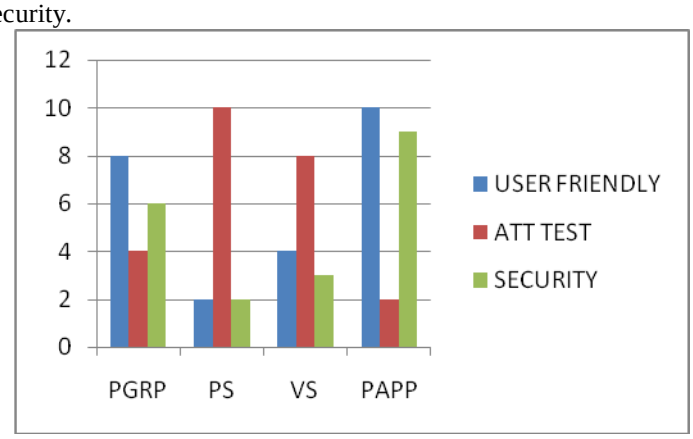

Fig.2: Comparisons between password protection protocols.

V. CONCLUSION

Online password estimating attacks on password-only schemes have been discerned for decades. Present day attackers aiming at such systems are empowered by having command of thousand to million-node botnets. In previous ATT-based login protocols, there lives a security usability trade-off with esteem to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PAPP protocol restricts all internal and outside attacks as we use MD5 encryption algorithm, virtual key board, machines physical address instead of IP address and very ease of use ATT Tests. By considering all this parameters and result we conclude that PAPP gives good security for passwords. In future we further like to extend this method by investigating its performance under real time environment. Scalability investigation is also one promising future direction for this approach.

ACKNOWLEDGEMENT

I thank my project guide and M.E Coordinator Prof.Dr.P.K.Deshmukh M.E (PhD),my H.O.D Prof.Dr.A.B.Bagwan, who are members of faculty with the Department of Computer Engineering, Rajarshi Shahu College of Engineering , without whose guidance, this paper would not have been possible. I also wish to record my thanks for their consistent encouragement and ideas. I would like to express my gratitude to all those who helped me make this paper a reality and gave me the opportunity to publish this paper.

REFERENCES

[1] "Defense to curb online password guessing attacks", R. Kirushnaamoni PG Scholar, Dept. of Computer Science and Engineering, IEEE.

[2] B. Pinkas and T. Sander, "Securing Passwords ag ainst Dictionary Attacks," Proc. ACM Conf. Computer and Comm. Securi ty (CCS '02), pp.161-170, Nov. 2002.

[3] P.C. van Oorschot and S. Stubblebine, "On Count ering OnlineDictionary Attacks with Login Histories and Humans-in-the-Loop," ACM Trans. Information and System Security, vol. 9, no. 3, pp. 235-258, 2006.

© 2014, IJARCSSE All Rights Reserved

[4] Revisiting Defenses against Large-Scale Online Password Guessing Attacks Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE.

[5] E. Bursztein, S. Bethard, J.C. Mitchell, D. Jurafsky, and C. Fabry, "How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation," Proc. IEEE Symp. Security and Privacy, May 2010

[6] "An Efficient approach for preventing online password guessing attacks", Resmipriya M G, Sangeetha N,Vol 2 Issue 3 March2013.International journal of Computer Science and Management Research

[7] 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.

[8] 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.

[9] 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.

[10] Y. He and Z. Han, "User Authentication with Provable Security against Online Dictionary Attacks," J. Networks, vol. 4, no. 3,pp. 200-207, May 2009.

[11] T. Kohno, A. Broido, and K.C. Claffy, "Remote Physical Device Fingerprinting," Proc. IEEE Symp. Security and Privacy, pp. 211-225, 2005.

[12] M. Motoyama, K. Levchenko, C. Kanich, D. Mccoy, G.M. Voelker,and S. Savage, "Re: CAPTCHAs Understanding CAPTCHA Solving Services in an Economic Context," Proc. USENIX Security Symp., Aug. 2010.

[13] 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.

[14] 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.

[15] Nat'l Inst. of Standards and Technology (NIST), Hashbelt. http://www.itl.nist.gov/div897/sqg/dads/HTML/hashbelt.html, Sept.2010.

[16] "The Biggest Cloud on the Planet Is Owned by ... the Crooks," NetworkWorld.com., http://www.networkworld.com/community/node/58829, Mar. 2010.

[17] S.M. Bellovin, "A Technique for Counting Natted Hosts," Proc.ACM SIGCOMM Workshop Internet Measurement, pp. 267-272,2002

© 2014, IJARCSSE All Rights Reserved