Defenses to curb Online Password Guessing Attacks

R. Kirushnaamoni,
PG Scholar, Dept. of Computer Science and Engineering,
Mepco Schlenk Engineering College,
Sivakasi, India.
rkmoni90@hotmail.com

Abstract - Passwords are the most commonly used means of authentication as passwords are very convenient for users, easier to implement and user friendly. Password based systems suffer from two types of attacks: i) offline attacks ii) online attacks. Eavesdropping the communication channel and recording the conversations taking place on the communication channel is an example for offline attack. Brute force and dictionary attacks are the two types of online attacks which are widespread and increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. The proposed protocol called Password Guessing Resistant Protocol (PGRP), helps in preventing such attacks and provides a pleasant login experience for legitimate users. PGRP limits the number of login attempts for unknown users to one, and then challenges the unknown user with an Automated Turing Test (ATT). There are different kinds of ATT tests such as CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart), security questions etc. In this system, a distorted text-based CAPTCHA is used. If the ATT test is correctly answered, the user is granted access else the user is denied access. The proposed algorithm analyzes the efficiency of PGRP based on three conditions: i) number of successful login attempts ii) number of failed login attempts with invalid password iii) number of failed login attempts with invalid password and ATT test. PGRP log files are used as data sets. The analysis helps in determining the efficiency of PGRP protocol.

Keywords-Online password guessing attacks, brute force attacks, password dictionary, ATTs.

I. INTRODUCTION

Passwords are commonly used means for user authentication as they are very convenient for the users, easier to implement and user friendly. There are alternatives to passwords that are more secure, such as hardware tokens that generate time-dependent pass codes or SSL/TLS client certificates or smartcards. None of them have been in widespread use in the consumer market as these alternatives require costly maintenance and infrastructure. The password based system, though very convenient has some drawbacks. Humans have a tendency to choose relatively short and simple passwords that can easily be remembered. Stronger passwords generated by the servers are difficult to remember and are not user friendly [3].

Password based systems mainly suffer from offline and online attacks. In an offline attack, the attacker eavesdrops the network channel and records data. Then the attacker goes offline and tests passwords without contacting the server. In an online attack, the adversary tries the possible passwords by logging into the server online. There are two types of online attacks: Brute force and dictionary attacks. In brute force attack, a program tries all available words it has to gain access to the account. A dictionary attack is a method of breaking into a system or server by entering every word in a dictionary as a password. Offline attacks can be prevented by using public key cryptography. However, no satisfactory measures to curb online dictionary attacks have been suggested so far [3]. There are some methods to deal with them but some of them have security flaws and these methods have been discussed in section 2.

ATT is a type of challenge-response test which is used to differentiate between a human and a bot. It proves the identity of a human. The process involves the computer asking the user to solve a simple test from which the computer differentiates between a human and a bot. These tests are designed to be easy for a computer to generate, but difficult for a computer to solve, so that if a correct solution is received, it can be presumed to have been entered by a human. 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. of these CAPTCHAs are commonly used. A common type of CAPTCHA requires the user to type letters or digits from a distorted image that appears on the screen [5].

PGRP helps in preventing online dictionary attacks. The PGRP protocol has been discussed in the following sections.

A. *Organization*

Section 2 discusses existing systems for prevention of online dictionary attacks. Section 3 presents the PGRP login protocol. Section 4 discusses the results and section 5 concludes and discusses about the future work.

II. EXISTING SYSTEM

Password based systems are vulnerable to online dictionary attacks. These attacks are difficult to curb and hence pose a major problem in the functioning of password based systems. Countermeasures adopted to prevent the online dictionary attacks are many a times expensive and yet not very effective.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.

Some of the measures adopted to prevent this attack (with their drawbacks) are as follows:

A. *Account Locking*

After a few fixed number of unsuccessful login attempts, the account of the user is locked for some time. This system helps in preventing some of the most common online password guessing attacks by limiting the number of wrong password guesses. On the other hand this system is vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDos) attacks in which an attacker or a group of attackers will randomly guess passwords in order to lock the user's account, thereby preventing the legitimate users from logging into their systems. Another drawback of the account locking system is that sometimes the legitimate users may lock their own accounts by mistake. In that case the user will have to either contact their service providers in order to unlock their accounts or wait till the account is automatically unlocked. Despite these drawbacks, account locking is still commonly adopted in many systems [4].

B. *Delayed Response*

In this scheme, the server provides a delayed response to the user request. This may help in preventing an attacker from checking many passwords in a reasonable time. This scheme is very effective for local machines in which a user has to login using a physically attached keyboard. It is less effective in a network environment as the attacker can carry out DoS or DDoS attack very efficiently [3].

C. *Pinkas and Sander Protocol*

Pinkas and Sander (PS) introduced a protocol that requires answering an ATT challenge first before entering the {username, password} pair. Failing to answer the ATT correctly prevents the user from proceeding further. This protocol requires the adversary to pass an ATT challenge for each password guessing attempt, in order to gain information about correctness of the guess. While this simple protocol is effective against online dictionary attacks assuming that the used ATTs are secure, legitimate users must also pass an ATT challenge for every login attempt. Therefore, this protocol affects user convenience substantially, and requires the login server to generate an ATT challenge for every login attempt [2].

D. *Van Oorschot and Stubblebine Protocol*

This protocol is considered to be as an improvement for PS protocol. Only if the username, password is incorrect the user is asked to answer an ATT challenge. Else the user is granted access. The number of ATT challenges asked to the user is based on a threshold value called AskATT(). Sometimes legitimate users may be asked to answer many ATT challenges before being granted which may annoy the user. Therefore this protocol affects user convenience [7].

E. *General Techniques*

One effective defense against automated online password guessing attacks is to restrict the number of failed trials without ATTs to a very small number (e.g., three), limiting automated programs (or bots) as used by attackers to three free password guesses for a targeted account, even if different machines from a botnet are used. However, this inconveniences the legitimate user who then must answer an ATT on the next login attempt [8].

Several other techniques are deployed in practice, including: allowing login attempts without ATTs from a different machine, when a certain number of failed attempts occur from a given machine; allowing more attempts without ATTs after a time-out period; and time-limited account locking. Many existing techniques and proposals involve ATTs, with the underlying assumption that these challenges are sufficiently difficult for bots and easy for most people [1].

III. IMPLEMENTATION OF PGRP

In this section the PGRP protocol is described.

A. *Goals*

Objectives for PGRP include:

1. The login protocol should make brute force and dictionary attacks ineffective.
2. The protocol should not have any significant impact on usability (user convenience).
3. The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space [1].

B. *Methodology*

PGRP builds on the PS and VS proposals. PGRP enforces ATTs after a user enters either the wrong username or password. In this case a strong ATT test should be used. There are many ATT tests of which CAPTCHA is most commonly used. In this case, a distorted text based CAPTCHA is used. The modules of the proposed system are described below:

1) New user registration and login: This is the initial phase in the proposed system. During registration and login, the following steps take place:

1. The new user during registration is asked to fill in details like first name, last name, gender, date of birth, username, password, confirm password are stored.
2. The user can then login with the username and password.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.

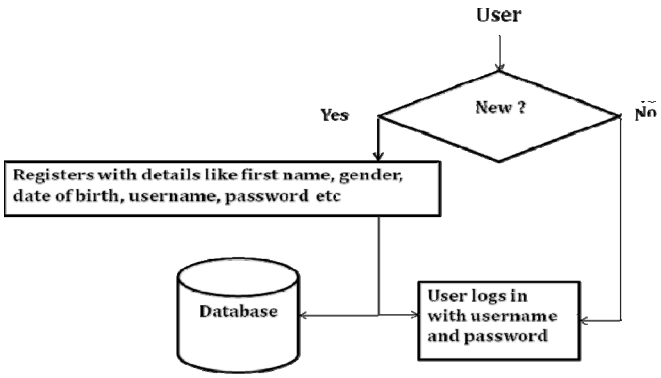

Fig. 3.1 New user registration and login

2) Identifying user: This is the second phase in the proposed system. During user identification, the following steps take place:

1. If the user logs in with the correct username and password, the user is granted access.
2. If the user logs in with either the wrong username or password or both, then the user is challenged with an ATT test.
3. If the ATT test is correctly answered, the user is once again given a chance to enter the correct username and password.
4. If the ATT test is not correctly answered, the user stays in the ATT test page until the ATT test is correctly answered. Maximum of three chances is provided. After that access id denied.

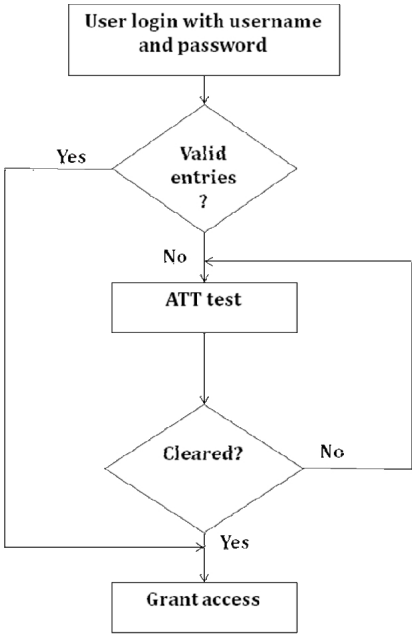

Fig. 3.2 Identifying for valid user

3) Classifying the user: This is the third phase in the proposed system. During user classification, the following steps take place:

1. In general details such as username, password, date and time of login, port, domain, status and ATT test status are collected.
2. When the user logs in with the correct username and password, the status is recorded as 'valid' along w ith the other above mentioned details.
3. When the user logs in with either incorrect username or password or both, the user is challenged with an ATT test. If the ATT test is correctly answered then the status is recorded as 'invalid' and the ATT tes t status is recorded as 'correct' along with the other above mentioned details.
4. If the ATT test is not answered correctly, the status is recorded as 'failed' and the ATT test status is recorded as 'wrong' along with the other above mentioned details.

By collecting such details, the valid and invalid user can easily be identified.

C. Algorithm

```
Input  : Username (un) and Password (pw)
Output : Access is granted if the username and password
         is correct else denied.
Begin
read data (un, pw)
if new user then
        store user details
   else
        login with the un and pw.
end if
if un and pw is correct then
        access is granted to the user
            details such as username, password, date
            and time of login, domain, host, status
            (valid) and CAPTCHA status (-) are
            recorded.
  else
        access is denied to the user. User is challenged
        with ATT test.
            If the ATT test is correctly answered
               Store the above details; status (invalid)
               and CAPTCHA status (correct) are
               recorded.
                    login with the un and pw.
            else
               Store the above details; status (failed)
               and CAPTCHA status (wrong) are
               recorded.
            end if
   end if
```

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.

IV. EXPERIMENTAL RESULTS

This section provides details of the test setup, empirical results and analysis of PGRP on login data sets.

A. Data Sets

Data sets from a college environment were collected and the following results were obtained.

Login Data sets. User log files have been collected as data sets. Log files have been collected from 25 users. Details like each authentication event, including: username, password, date, time, authentication status (success, failed or invalid user), source IP, source port, protocol, domain and CAPTCHA status (correct, wrong) are collected. Users have been classified as valid and invalid users. **Table 1** shows the user login files.

B. Implementation Details

Implementation was carried out using NetBeans 7.2, database used was MySQL 5.5.18 and the language used was Java Server Pages (JSP).

C. Analysis Procedure

When the user logs in, information like username, password, date, time, IP address, protocol, domain, port and path is recorded. By recording these details, information like

a) Number of successful login attempts.
b) Number of failed login attempts with invalid password.
c) Number of failed login attempts with invalid password and ATT test.

are analyzed and the efficiency of PGRP protocol is determined.

1) Number of successful login attempts: When the user logs in with the correct username and password, the status is recorded as 'valid' along with details such as user name, password, IP address, port, host, domain. **Table 2** shows the details of valid users.

2) Number of failed login attempts with invalid password: When the user logs in with either the wrong username or password or both, the user is challenged with an ATT test. If correctly answered, the user is given another chance to login with the correct username and password. The status is recorded as 'invalid' and the CAPTCHA status is rec orded is recorded as 'correct' along with details such as us ername, password, IP address, port, host, domain. **Table 3** shows the details of number of failed login attempts with invalid password

3) Number of failed login attempts with invalid password and ATT test: When the user logs in with either the wrong username or password or both, the user is challenged with an ATT test. If wrongly answered, the user stays in the ATT test until the test is correctly answered. The status is recorded as 'failed' and the CAPTCHA status is recorded is reco rded as 'wrong' along with details such as username, passwo rd, IP address, port, host, domain. **Table 4** shows the details of number of failed login attempts with invalid password and ATT test.

4) Number of valid and invalid users: Based on the acquired details the users are classified as valid and invalid. Out of 120 log files, 54 have been identified as valid users and 46 have been identified as invalid users. **Table 5** shows the details of valid and invalid users.

TABLE 1 USER LOG FILES

Username	Password	Date	Time	IP	Port	Protocol	Domain	Status	CAPTCHA
Agnes	Agnes	12-10-12	12:43	127.0.0.1	8084	http	Localhost	Valid	-
Andal	Andal	12-10-12	13.23	127.0.0.1	8084	http	Localhost	Invalid	Correct
Moni	Mani	13-10-12	09:01	127.0.0.1	8084	http	Localhost	Failed	Wrong
Vani	Moni	13-10-12	11:45	127.0.0.1	8084	http	Localhost	Failed	Wrong
Prabha	Prabha	14-10-12	02:01	127.0.0.1	8084	http	Localhost	Valid	-

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.

TABLE 2 VALID USERS

Username	Password	Date	Time	IP	Port	Protocol	Domain	Status	CAPTCHA
agnes	bharathi	12-10-12	12:43	127.0.0.1	8084	http	Localhost	-	Valid
moni	moni	13-10-12	11:45	127.0.0.1	8084	http	Localhost	-	Valid

TABLE 3 NUMBER OF FAILED LOGIN ATTEMPTS WITH INVALID PASSWORD

Username	Password	Date	Time	IP	Port	Protocol	Domain	Status	CAPTCHA
moni	mani	13-10-12	09:01	127.0.0.1	8084	http	Localhost	-	-
moni	moni	13-10-12	11:45	127.0.0.1	8084	http	Localhost	Invalid	Correct
pinky	prinky	14-10-12	02:01	127.0.0.1	8084	http	Localhost	-	-
pinky	prinky	15-10-12	04:00	127.0.0.1	8084	http	Localhost	Invalid	Correct

TABLE 4 FAILED LOGIN ATTEMPTS WITH INVALID PASSWORD AND ATT TEST

Username	Password	Date	Time	IP	Port	Protocol	Domain	Status	CAPTCHA
vani	mani	13-10-12	04:08	127.0.0.1	8084	http	Localhost	Failed	Wrong
andal	priya	15-10-12	02:10	127.0.0.1	8084	http	Localhost	Failed	Wrong

TABLE 5 NUMBER OF VALID AND INVALID USERS

Valid users	Invalid users	
	Invalid password attempts	Invalid password and ATT test attempts
54	20	26

V. CONCLUSION AND FUTURE WORKS

The existing systems provide more login chances to both legitimate and unknown users which make it a drawback and increase a chance for Brute force and Dictionary attacks. Sometimes it becomes difficult to distinguish between a legitimate and unknown user. The developed system is more restrictive against Brute force and Dictionary attacks while on the other hand limits the total number of login attempts from unknown hosts. The experimental results gathered from operational network environments shows that while PGRP is apparently more effective in preventing password guessing attacks, it also offers more convenient login experience, e.g. fewer ATT challenges for legitimate users. The log files reveal who the legitimate users are and who the unknown users are which helps in easily preventing the attacks carried by the unknown users.

Future work includes in further improving the ATT tests. In the tests carried out, only certain category of users

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.

has been used. The protocol can be further tested with different kinds of users of various categories. Instead of using ATT tests to differentiate between the valid and invalid users, IP addresses can be used. The IP address from an adversary can be blocked by comparing with the IP addresses already stored in the database.

REFERENCES

[1] Alsaleh, M.; Mannan, M.; van Oorschot, P.C. Van Oorschot, "Revisiting Defenses against Large-Scale Online Password Guessing Attacks ," IEEE Transactions on Dependable and secure computing, Vol. 9 , no. 1, pp. 128 - 141, Jan/Feb. 2012.

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

[4] 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.

[5] J. Yan and A.S.E. Ahmad, "Usability of CAPTCHAs or Usability Issues in CAPTCHA Design," Proc. Symp. Usable Privacy and Security (SOUPS '08), pp. 44-52, July 2008 .

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

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

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

Authorized licensed use limited to: Auckland University of Technology. Downloaded on May 27,2025 at 10:21:36 UTC from IEEE Xplore. Restrictions apply.