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

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

Implementation and Comparative Study of PGRP,PS,VS,Modified PGRP

Miss. Vaishali k. Kosamkar [1], Prof. V. M. Deshmukh [2]

Student of Post Graduation, Department Of Information Technology, P. R. M. I. T. and R., Badnera, India[1]

Head of Department, Information Technology, P. R. M. I. T. and R., Badnera, India[2]

Abstract: Authentication to users account to access web services online is achieved using passwords. These passwords are prone to guessing attacks namely brute force and dictionary attacks. Password guessing attack is a method of gaining unauthorized access to one's computer system. Online guessing of passwords is commonly observed in web based applications where users login a number of time to access the details. The guessing attacks on passwords over online are widely spread which reduces the convenience to the legitimate users. Different types of Turing tests are used to prevent legitimate users from such attacks with certain inconvenience to the valid users. On the other hand users also generally prefer common and easy passwords which are weak and make online guessing attacks much easier. The modified password guessing resistant protocol overcomes these online guessing attacks mainly brute force and dictionary attacks. This is achieved by limiting the number of attempts made during login. Aim of this paper is to provide convenient and secured login to the legitimate users which is by blocking the IP address from which there are more number of failed login attempts.

Keywords: Online Password Guessing Attacks, Brute Force Attacks, Dictionary Attack, PGRP, ATTs.

I. INTRODUCTION

Passwords have become the dominant means of access control to online services. The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Even though they remain the most widely used authentication method despite their well-known security weaknesses. Online password guessing attacks on websites is a top cyber security risk. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective user-friendliness is a key requirement. A password guessing attack is a method of gaining unauthorized access to a computer system by using computers and large word lists to try a large number of likely passwords. An on-line attack is an attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.

Various Turing tests are used to prevent password guessing attacks. One effective defence 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. 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 timeout 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. However, users increasingly dislike ATTs as these are perceived as an unnecessary step.

Online guessing attacks on password-based systems are inevitable and commonly observed against web applications.

II. LITERATURE REVIEW

Although online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. Account locking is a customary mechanism to prevent an adversary from attempting multiple passwords for a particular username. Although locking is generally temporary, the adversary can mount a DoS attack by making enough failed login attempts to lock a particular account. Delaying server response after receiving user credentials, whether the password is correct or incorrect, prevents the adversary from attempting a large number of passwords in a reasonable amount of time for a particular username. Although locking is generally temporary, the adversary can mount a DoS attack by making enough failed login attempts to lock a particular account. Delaying server response after receiving user credentials, whether the password is correct or incorrect, prevents the adversary from attempting a large number of passwords in a reasonable amount of time for a particular username. However, for adversaries with access to a large number of

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

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

machines (e.g., a botnet), this mechanism is ineffective. Similarly, prevention techniques that rely on requesting the user machine to perform extra nontrivial computation prior to replying to the entered credentials are not effective with such adversaries. To provide designers and implementers with a clear framework, Kevin Fu[2], have given a description of the limitations, requirements, and security models specific to Web client authentication. They presented a set of hints on how to design a secure client authentication scheme, based on experience gained from their informal survey of commercial schemes. ATT challenges are used in some login protocols to prevent automated programs from brute force and dictionary attacks. Pinkas and Sander [3] presented a login protocol (PS protocol) based on ATTs to protect against online password guessing attacks. It reduces the number of ATTs that legitimate users must correctly answer so that a user with a valid browser cookie (indicating that the user has previously logged in successfully) will rarely be prompted to answer an ATT. A deterministic function (AskATT()) of the entered user credentials is used to decide whether to ask the user an ATT. To improve the security of the PS protocol, van Oorschot and Stubblebine [4] suggested a modified protocol in which ATTs are always required once the number of failed login attempts for a particular username exceeds a threshold; other modifications were introduced to reduce the effects of cookie theft. For both PS and VS protocols, the decision function AskATT() requires careful design.

He and Han [5] pointed out that a poor design of this function may make the login protocol vulnerable to attacks such as the "known function attack" (e.g., if a simple cryptographic hash function of the username and the password is used as AskATT()) and "changed password attack" (i.e., an adversary mounts a dictionary attack before and after a password change event initiated by a valid user). The authors proposed a secure nondeterministic keyed hash function as AskATT() so that each username is associated with one key that should be changed whenever the corresponding password is changed. J. Yan and A.S.E. Ahmad, Usability of CAPTCHAs or Usability Issues in CAPTCHA Design [6], 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. C. Namprempre and M. N. Dailey [7], Proposed a new construct, the Text-Graphics Character (TGC) CAPTCHA, for preventing dictionary attacks against password authentication systems allowing remote access via dumb terminals. They talk about the inadequacy of existing along with proposed login protocols made to address significant scale online dictionary attacks, from some sort of botnet of tens of thousands of nodes. They proposed a brand new Password Estimating Resistant Method (PGRP), derived on revisiting earlier proposals made to restrict this kind of attacks. While PGRP limits the total number of login tries from unfamiliar remote hosts to as low as a solitary attempt for each username, legitimate users in most cases e. grams., when attempts are made of known, frequently-used machines can make several unsuccessful login tries before becoming challenged by having an ATT. L. von Ahn, M. Blum, N. Hopper, and J. Langford[8], introduced captcha, an automated test that humans can pass, but current computer programs can't pass: any program that has high success over a captcha can be used to solve an unsolved Artificial Intelligence (AI) problem.

They provided several novel constructions of captchas. Since captchas have many applications in practical security, There approach is to introduces a new class of hard problems that can be exploited for security purposes. K.Hari Krishna [9], The major goal is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software's are available in the market. There for, their paper worked on merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method. The major goal is to guessing attacks as well as encouraging user to select more random, and difficult password to guess. In their paper they proposed a click-based graphical password system.

During password creation, there is a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. M. Weir, S. Aggarwal, M. Collins, and H. Stern[10], focused on actual attack methodologies and real user passwords quite possibly makes this one of the largest studies on password security to date. In addition they examine what these results mean for standard password creation policies, such as minimum password length, and character set requirements. Thomas Wu[11], proposed a new password authentication and key exchange protocol suitable for authenticating user and exchanging a keys over a untrusted network. Their paper presented a new password

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

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

authentication and key-exchange protocol suitable for authenticating users and exchanging keys over an untrusted network. The new protocol resists dictionary attacks mounted by either passive or active network intruders, allowing, in principle, even weak passphrases to be used safely. It also offers perfect forward secrecy, which protects past sessions and passwords against future compromises. Finally, user passwords are stored in a form that is not plaintext-equivalent to the password itself, so an attacker who captures the password database cannot use it directly to compromise security and gain immediate access to the host. This new protocol combines techniques of zero-knowledge proofs with asymmetric key exchange protocols and offers significantly improved performance over comparably strong extended methods that resist stolen-verifies attacks. J. Jayavasanthi Mabel, Mr. C. Balakrishnan [12], provided convenient and secured login to the legitimate users which is by blocking the IP address from which there are more number of failed login attempts.

Authentication to users account to access web services online is achieved using passwords. These passwords are prone to guessing attacks namely brute force and dictionary attacks. Password guessing attack is a method of gaining unauthorized access to one's computer system. The password guessing resistant protocol overcomes these online guessing attacks mainly brute force and dictionary attacks. This is achieved by limiting the number of attempts made during login. The goal is to provide convenient and secured login to the legitimate users which is by blocking the IP address from which there are more number of failed login attempts.The proposed function requires extra server-side storage per username and at least one cryptographic hash operation per login attempt.

III. EXISTING SYSTEM

The PS(Pinkas and Sander) and VS (Van Oorschot and Stubblebine)are the existing protocols based on ATT. PS protocol asks the users (legal/attackers) to challenge ATT first and allows them to enter the username and password if the answer made is correct. The improved version of PS sends browser cookies to the login server when the user requests the login server. If the cookie is valid then the user is allowed to enter {username, password} pair. If the pair and received cookie are valid then the user is authenticated otherwise the user is asked to challenge ATT. The VS protocol makes some modifications to PS. The VS protocol traces the number of failed login attempts for a particular username. If the traced value exceeds some threshold value the users are asked challenge ATT for every next attempt.

A. Issues in Existing system

PS: Since the legal users must also pass an ATT challenge for every login attempt, the PS protocol affects user convenience substantially, and requires the login server to generate an ATT challenge for every login attempt. VS: the legal user always faces an ATT challenge once the threshold is exceeded. This feature enables adversaries to affect user login convenience, by initiating failed login attempts greater than the threshold for each targeted username, forcing ATT challenges for the subsequent login attempts.

PGRP: Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While 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 (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

B. PS Protocol

PS protocol referred to as Pinkas and Sander 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.

Initialization-Once the user has successfully logged into an account, the server places in the user's computer a cookie that contains an authenticated record of the username and possibly an expiration data.

Login procedures
If ATT Challenge Pass then
Read Userid and Password
If the Userid/password pair is correct, then
The user is granted access
If the Userid/password pair is incorrect, then
Message Userid & Password is Incorrect
If ATT Challenge Fail then
Message ATT answer wrong.

C. VS Protocol

VS protocol referred to as Van Oorschot and Stubblebine protocol proposed modifications to the previous protocol which track failed logins per username to impose ATT challenges after exceeding a configurable threshold of failures. In addition, upon entering correct credentials in the absence of a valid cookie, the user is asked whether the machine in use is trustworthy and if the user uses it regularly.

The cookie is stored in the user's machine only if the user responds yes to the question.

Login procedures
If Userid and password is correct
The user is granted access
User logins with wrong Userid OR password
Message Fail Login
If Fail login Attempts is greater than threshold value
Generate ATT Challenge
If answer to ATT challenge is correct & password is correct then login successful otherwise again generate ATT.

DOI 10.17148/IJARCCE.2015.4451

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

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

If answer to ATT challenge is incorrect it will display message answer to ATT incorrect.

These protocols involve large number of Turing test which an valid user also must undergo which reduces the convenience of the user.

D. PGRP Protocol

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

The proposal called Password Guessing Resistant Protocol (PGRP), significantly improves the security-usability trade-off, and can be more generally deployed beyond browser based authentication. PGRP builds on these two previous proposals. 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.

We define known machines as those from which a successful login has occurred within a fixed period of time. These are identified by their IP addresses saved on the login server as a white-list, or cookies stored on client machines. A white-listed IP address and/or client cookie expires after a certain time.

PGRP include the following:

1) The login protocol should make brute-force and dictionary attacks ineffective even for adversaries with access to large botnets (i.e., capable of launching the attack from many remote hosts).
2) The protocol should not have any significant impact on usability (user convenience).
3) The protocol should be easy to deploy and scalable.

- Login procedures

```
begin
ReadCredential(unme, pw, cookie)
if LoginCorrect(unme, pw) then
if (((Valid(cookie, un,k1,true) _ ((srcIP; unme) ) then
FS[srcIP; unme]
Add srcIP to W
GrantAccess(unme, cookie)
else
if (ATTChallenge() = Pass) then
FS[srcIP; unme] ( 0)
Add srcIP to W
GrantAccess(unme, cookie)
else
Message(The answer of ATT is incorrect)
else // username/password pair is not correct
 if ((Valid(cookie, un,k1,false) _ ((srcIP; unme)))
Message(The username or password is not correct)
else if (ValidUsername(unme) ^ (FT[unme] < k2)) then
FT[unme] ( FT[unme] + 1
Message(The username or password is incorrect)
else
if (ATTChallenge() = Pass) then
Message(The username or password is not correct)
else
Message(The answer to the ATT is not correct)
End
```

IV. IMPLEMENTATION

Here we are going to implement new algorithm called Modified PGRP(MPGRP) which is based on the validating authentication. The general idea behind MPGRP (Modified Password Guessing Resistant Protocol) is that it checks user id and password & IP if all are correct then it will grant access to user.

If user id and password is incorrect then user has to pass ATT challenges. If fail attempt is greater than three then user has to pass ATT challenge & if fail attempt is greater than six then user id blocked for that day simultaneously master count is also calculated for each fail attempts, if master count is greater than eighteen IP address for that user is blocked permanently.

In this proposed work we are going to implement new algorithm MPGRP i.e. Modified PGRP algorithm which increases security level at good extend which can be used to apply at any application which is going to require high level of authentication. Here we are also going to compare Modified PGRP, Stander PGRP, VS(van Oorschot and Stubblebine) and PS(Pinkas and Sander) algorithm in terms of time taken by that algorithm to get successful access.

Here we mainly going to focus on modified PGRP algorithm and original PGRP algorithm which will be going to our prime targets for comparison.

We proposed a new Password Guessing Resistant Protocol (MPGRP), derived upon revisiting prior proposals designed to restrict such attacks. While MPGRP 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 (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. that makes it convenient to the legitimate users and stop the hackers from guess the passwords of the user. This makes the user's Password additional secured from the unauthorized users access.

- MPGRP Protocol: Login Procedures

```
Input:  K1 = default 3(expires in 1 day), K2 = def 18  FC= Fail Count, MFC= Master Fail Count
begin
 ReadCredential (unme, pw, IP)
 if LoginCorrect(unme, pw) then
 Set MFC & MC to 0
 GrantAccess
```

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

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

Else
If(MFC>K2)
if(FC>K1) then
if (ATTChallenge() = Pass) then
Message("The username or password is not correct")
else
Message("The answer to the ATT is not correct")
else
Message("user is blocked for 1day")
else
Message("your IP is blocked permanently")
End

V. ANALYSIS AND RESULTS

The concept of this paper is implemented and different results are shown below, The proposed paper is implemented in .NET technology on a Pentium-IV PC with minimum 80 GB hard-disk and 1GB RAM.

The propose paper's concepts shows efficient results and has been efficiently tested on different userid & Password. The proposed approach has been validated by experiments with PGRP, Modified PGRP,VS, PS algorithm with Time required in milliseconds. Successful Login Attempts with Time Required in Milliseconds (ms) is shown in fig. 1

TABLE 1

Algorithm	PGRP	Modified PGRP	PS	VS
Time In ms	884	39	9567	1865
	1799	161	29252	1260

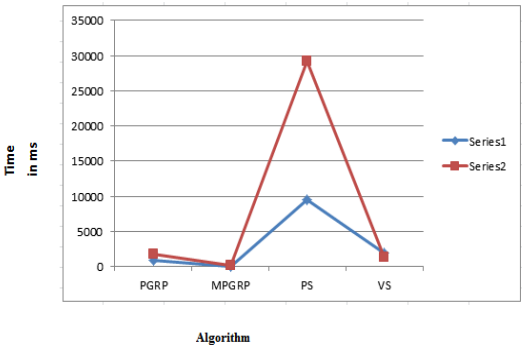

Fig. 1 Time taken for Successful Login Attempts

Fail Login Attempts with Time Required in Milliseconds (ms) is shown in fig. 2

TABLE 2

Algorithm	PGRP	Modified PGRP	PS	VS
Time In ms	2978	193	1252	34963
	10520	305	27552	7168

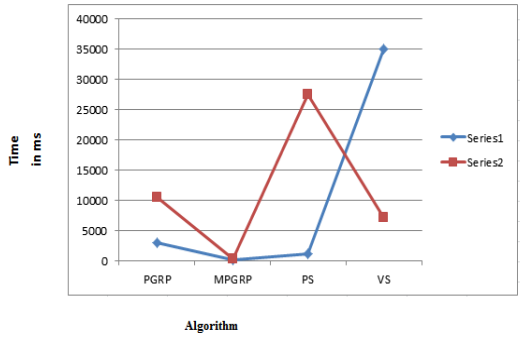

Fig. 2 Time taken for Fail Login Attempts

VI. CONCLUSION

Online password guessing attacks on password-only systems have been observed for decades. Present day attackers targeting such systems are empowered by having control of thousand to million-node botnets. In previous ATT-based login protocols, there exists a security usability trade-off with respect to the number of free failed login attempts versus user login convenience. In this paper we have Compared Modified PGRP, Standard PGRP, VS (van Oorschot and Stubblebine) and PS (Pinkas and Sander) algorithm in terms of time taken by that algorithm to get successful access.

The time taken by modified PGRP algorithm is less as compared to other three algorithm. MPGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. The goal is to provide convenient and secured login to the legitimate users which is by blocking the IP address from which there are more number of failed login attempts.

ACKNOWLEDGMENT

I would like to wish to the Head of the Department of Information Technology & my guide Prof. **V. M. Deshmukh** madam for the encouragement & support, which lead to enhancement of the paper work.

REFERENCES

[1]. Mansour Alsaleh, Mohammad Mannan, and P.C. van 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]. 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.
[3]. B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks", Proc. ACM Conf. Computer and Comm. Security (CCS '02), pp. 161-170, Nov. 2002
[4]. P.C. van Oorschot and S. Stubblebine, "On Countering 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.
[5]. 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.
[6]. 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.
[7]. C. Nampremre and M. N. Dailey, "Mitigating Dictionary Attacks with Text-Graphics Character Captchas", IEICE Trans.

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

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

Fundamentals of Electronics, Comm. and Computer Sciences, vol. E90-A, no. 1, pp. 179-186, 2007.

[8]. L. von Ahn, M. Blum, N. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," Proc. Eurocrypt, pp. 294-311, May 2003.

[9]. K.Hari Krishna, "Persuasive Click Points Based Large-Scale Online Password Guessing Attacks", Publication of problems and application in engineering research- Paper,Vol. 04 Special Issue01; CSEA2012, ISSN: 2230-8547; e-ISSN: 2230-8555,2013.

[10]. M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 162-175, 2010.

[11]. T. Wu, "The Secure Remote Password Protocol", Proc.Network and Distributed System Security (NDSS), The Internet Soc., pp. 97-111, 1998.

[12]. J. Jayavasanthi Mabel, Mr. C. Balakrishnan, "Resisting Password Based Systems from online Guessing Attacks" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, ISSN 2250-2459,An ISO 9001:2008 Certified Journal, January 2013.

BIOGRAPHIES

Miss. Vaishali Kosamkar Persuing Master of Engineering degree in Information Technology from PRMIT&R Badnera, Sant Gadge Baba Amravati University (2013-2015).