International Journal of Advance Foundation and Research in Computer (IJAFRC)
Volume 1, Issue 12, December 2014. ISSN 2348 – 4853

Implementation and Analysis of Password Guessing Resistant Protocol (PGRP): A Literature Survey.

Miss. Vaishali K. Kosamkar*, Prof. V. M. Deshmukh
Prof. Ram Meghe Institute of Technology and Research Badnera(India).

A B S T R A C T

Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. Present day attackers targeting such systems are empowered by having control of thousand to million-node botnets. Account locking is a customary mechanism to prevent an adversary from attempting multiple passwords for a particular username. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. 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. In previous ATT-based login protocols, there exists a security usability trade-off with respect 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, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. In this proposed work we are going to modify PGPRP 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 PGPRP, Stander PGPRP, 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 PGPRP algorithm and original PGPRP algorithm which will be going to our prime targets for comparison.

Index Terms: Online password guessing attacks, Dictionary attacks, brute force attacks, password dictionary, ATTs, Security

I. INTRODUCTION

A common threat Web developers face is a password-guessing attack known as a brute-force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. If your Web site requires user authentication, you are a good target for a brute-force attack. An attacker can always discover a password through a brute-force attack, but the downside is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations. To speed things up a bit, a brute-force attack could start with dictionary words or slightly modified dictionary words because most people will use those rather than a completely random password. These attacks are called dictionary attacks or hybrid brute-force attacks. Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. 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. We discuss the inadequacy of existing and proposed login protocols designed to address large-scale online dictionary attacks. 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. 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. However, online attacks have some inherent disadvantages compared to offline attacks: attacking machines must engage in an interactive protocol, thus allowing easier detection; and in most cases, attackers can try only limited number of guesses from a single machine before being locked out, delayed, or challenged to answer Automated Turing Tests (ATTs, e.g., CAPTCHAs [11]). Consequently, attackers often must employ a large number of machines to avoid detection or lock-out.

The remainder of this paper is organized as follows:

Section 2 gives idea about the previous work done, the Literature Survey. Section 3 briefly provides details about Proposed System Design, which covers protocol goals, Overviews & Algorithm. Section 4 gives concluding remarks.

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 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. The proposed function requires extra server-side storage per username and at least one cryptographic hash operation per login attempt Dinei Flor encio, Cormac Herley[6], shows that it is the combined size of the userID plus password key-space rather than the password key-space alone that protects large institutions against bulk guessing attacks. 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 ,solved a small percentage of ATTs, e.g., through automated programs, brute force mechanisms, and low paid workers. Incidents of attackers using IP addresses of known machines and cookie theft for targeted password guessing are also assumed to be minimal. Traditional password-based authentication is not suitable for any untrusted environment e.g., a key logger may record all keystrokes, including passwords in a system, and forward those to a remote attacker. The data integrity of cookies must be protected e.g., by a MAC using a key known only to the login server.The general idea behind PGRP is that except for the following two cases, all remote hosts must correctly answer an ATT challenge prior to being informed whether access is granted or the login attempt is unsuccessful. When the number of failed login attempts for a given username is very small; and when the remote host has successfully logged in using the same username in the past (however, such a host must pass an ATT challenge if it generates more failed login attempts than a pre specified threshold. In 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. Thomas Wu[8], 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 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. 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. J. Jayavasanthi Mabel, Mr. C. Balakrishnan [10], 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.

III. PROPOSED SYSTEM DESIGN

In this proposed system we are going to implement the PGRP algorithm which is based on the validating authentication. The general idea behind PGRP (Password Guessing Resistant Protocol) is that it checks user id and password if both are current then it will check for presence of cookie in the client system, if it is present then it will grant access to user. If user id and password is incorrect then user has to pass ATT challenges, PGRP will except for the following two cases,

- When the number of failed login attempts for a given username is very small
- When the remote host has successfully logged in using the same username in the past with having cookies or having and IP authorized address

However, such a host must pass an ATT challenge if it generates more failed login attempts than a pre-specified threshold. In contrast to previous protocols, PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated. 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 security usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). Our empirical experiments on operational network environments show that while PGRP is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users even if no cookies are

available and no known IP address is available. In this proposed work we are going to modify PGPRP 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 PGPRP, Stander PGPRP, 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 PGPRP algorithm and original PGPRP algorithm which will be going to our prime targets for comparison

A. Passwords Guessing Resistant Protocol Goal

Our objectives for 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). For example: for legitimate users, any additional steps besides entering login credentials should be minimal. Increasing the security of the protocol must have minimal effect in decreasing the login usability.
3. The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space.

B. Passwords Guessing Resistant Protocol Overview

The general idea behind PGRP is that except for the following two cases, all remote hosts must correctly answer an ATT challenge prior to being informed whether access is granted or the login attempt is unsuccessful:

1. When the number of failed login attempts for a given username is very small; and
2. When the remote host has successfully logged in using the same username in the past (however, such a host must pass an ATT challenge if it generates more failed login attempts than a prespecified threshold). In contrast to previous protocols, PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated.

C. Passwords Guessing Resistant Protocol Algorithm

Input: Username and Password of user

Process:

1. Read credentials (Username and password)
2. If user name and password is correct then
3. Check for the valid cookies If yes then Grant access
4. If cookies are not valid then check for ATT challenges, valid ATT challenges then Grant access else Incorrect ATT Challenge.
5. If Username and password are not correct then Check for the valid user if valid user then count login Attempt and user name and password is correct. If not valid user then check for ATT challenges, valid ATT challenges then user name and password is incorrect. If not then ATT challenge is incorrect and restrict login attempt.

Table 1. Comparison of PGRP, VS, PS Algorithm[1]

Parameter(Usability, Security ,Deployability)	PGRP	VS	PS
Cookies Theft	Yes	Yes	Yes
Failed login attempts to force ATT legitimate User	No	Yes	No
Protocol is suitable for browsers only	No	Yes	Yes
Protocol state grows linearly with number of users	Yes	Yes	No

IV. 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 (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users.

V. 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] 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.

[7] 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.

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

[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] 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.

AUTHORS PROFILE

Miss.Vaishali K.Kosamkar persuing Master of Engineering degree From Sant Gadge Baba Amravati Universuty , India.