ISSN 2250-3153

Revisiting Defences against Large Scale Online Password Guessing Attacks

Nitin Garg, Raghav Kukreja, Pitambar Sharma

Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India

Abstract- Brute force and dictionary attacks on password protected remote login services are increasing rapidly. Letting legitimate user's login conveniently while preventing such attacks is difficult. Automated Turing Tests (ATTs) are effective and easy to implement but cause reasonable amount of inconvenience to the user. We discuss the existing and proposed login protocols designed to prevent large scale online dictionary attacks. We propose Password Guessing Resistant Protocol (PGRP), which is derived upon revisiting prior proposals designed to restrict such attacks. PGRP reduces the total number of login attempts from unknown remote host while trusted or legitimate users can make several failed login attempts before being challenged by ATT.

I. INTRODUCTION

With increasing number of online users in the real world, maintaining privacy details and protecting them with a password also becomes difficult. Here we involve developing a secure application to prevent our privacy information by using Password Guessing Resistant Protocol (PGRP). Password guessing attacks can be classified into two:

1. Brute Force Attack: A Brute Force attack is a type of password guessing attack which consists of trying every possible code, combination, or password until the correct one is found. A brute force attack is a very slow type of attack because of the many possible combinations of characters in the password. However, brute force is effective; given enough time and processing power, all passwords can eventually be identified.

2. Dictionary Attack: A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password.A dictionary attack is a method of breaking into a password protected server by systematically entering every word in a dictionary as a password.

Existing System: The use of passwords is a necessity in computer security but passwords are often easy to guess by automated programs or tools running dictionary attacks. In the existing system, an automated test is implemented that humans can pass, but current computer programs can't pass. Any program that has high success over these tests can be used to guess passwords cause security risks. An example of such a test is a 'captcha'. A captcha is a test used in computing which ensures that the response is generated by a person and not by a tool. The process usually involves a computer asking a user to complete a simple test which can ensure a successful login. 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. Following figure (Fig.1) is an example of the captcha.

Proposed System: Password Guessing Resistant Protocol (PGRP), which is our proposed system, enforces ATTs after a few failed login attempts are made from unknown systems. We define trusted or known systems 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. PGRP accommodates both graphical user interfaces and character interfaces, while the previous protocols deal exclusively with the former. PGRP uses IP addresses for tracking legitimate users. The proposed system is more sensitive against brute force and dictionary attacks while also allows a number of failed login attempts for legitimate users.

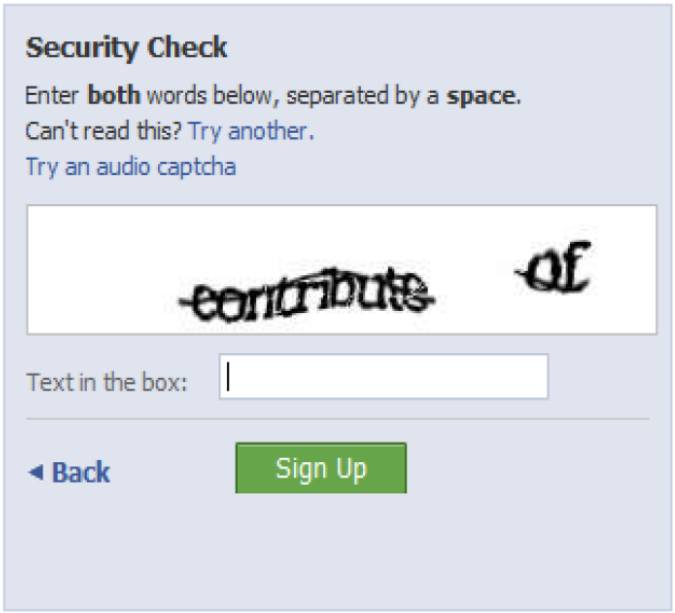

Fig.1: An example of the captcha

The proposed system is much more convenient than the existing system and consists of minimal steps for legitimate user to login.

Two processes involved in this:

1) If a trusted system fails the first login attempt then it is given two more chances (totally three chances). If the user fails in the third attempt to login then the intimation will be given.

2) If an unknown system fails in the first login attempt then it will not be given any more chances and intimation A flowchart

of the algorithm of the discussed protocol is shown below. character-based er. It t will be given.

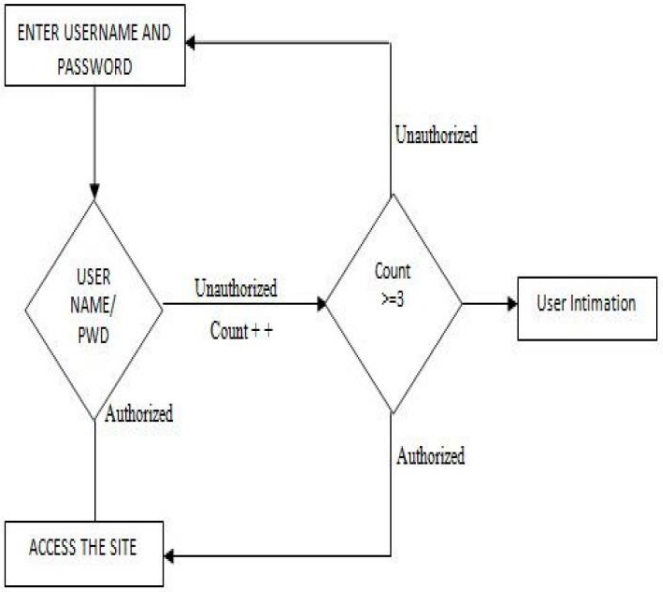

Fig.2: flowchart of proposed system

II. OVERVIEW

The general idea behind PGRP is that user does not have to face an ATT challenge for the following two conditions

1) When the number of failed login attempts for a given username is very

2) When the remote host has successfully logged before reaching the threshold limit of failed login attempts. In contrast to previous protocols, PGRP uses either IP addresses, cooki identify systems from which users have been successfully authenticated. 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.

III. CONCLUSION

Password guessing attacks have been increasing rapidly. To put an end to this we use PGRP. PGRP will restrict the number of attempt made by a system or a machine and allow the legitimate user to have a full secured access over their account. PGRP appears suitable for organizations of both small and large number of user accounts. PGRP can restrict brute force attack and dictionary attack, so it enhances the security of user's account.

REFERENCES

[1] 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.

[2] Usability of CAPTCHAs Or usability issues in CAPTCHA design Jeff Yan, Ahmad Salah El Ahmad July 2008

[3] Password Protected Smart Card and MemoryStick Authentication Against Dictionary Attacks Yongge Wan, March 3, 2012.

AUTHORS

First Author – Nitin Garg, Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India

Second Author – Raghav Kukreja, Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India

Third Author – Pitambar Sharma, Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India