INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AN OPTIMAL SOLUTION OVER LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS

MOHAMMAD MUDASSAR, PROF. BRAVIM JOREWAR

Department Of Computer Science & Engg. Rajarshi Shahu College of Engineering, Buldhana.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: 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. From a user's perspective user friendliness is a key requirement. 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 online attacks is a major concern in security systems. 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 this paper a novel authentication scheme that preserves the advantages of conventional password authentication is proposed, while simultaneously raising the costs of online dictionary attacks by orders of magnitude. The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods for improving the security of user authentication schemes. The key idea is to efficiently combine traditional password authentication with a challenge that is very easy to answer by human users, but is infeasible for automated programs attempting to run dictionary attacks. This is done without affecting the usability of the system. A new Password Guessing Resistant Protocol (PGRP) is proposed, 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.

Keywords: Mudassar, Captcha, Password Guessing Resistant Protocol, Password Attacks, Network Security, ATT.

Corresponding Author: MR. MOHAMMAD MUDASSAR

Access Online On:

www.ijpret.com

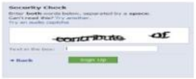
How to Cite This Article:

Mohammad Mudassar, IJPRET, 2015; Volume 3 (9): 65-70

PAPER-QR CODE

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:



Security Check

Enter both words below, separated by a space.
Can't read this? Try another.
Try an audio captcha

contribute of

Text in the box:

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.

MATERIALS & METHODS

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 An example of the captcha.

RESULTS & DISCUSSIONS

Proposed System

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.

Steps Involved In PGRP

1. Tracking Hacker: When there is more of failed login attempts for a particular account than that user is been traced using the IP address. This method find the user’s IP instead of the user browser’s cookie since cookie can be easily modified and deleted.

2. Generate CAPTCHA: CAPTCHA is the completely Automated Public Turing Test to tell Computers and Humans Apart. When the number of attempts made to login increases beyond three limits a CAPTCHA will be generated. The user must undergo this ATT challenge. This is used as a validation method to verify whether the user is a valid user based on the time taken to complete the challenge. In this protocol the CAPTCHA generated are the ATTs which will be generated when the user has failed 3 login attempts.

3. Forward New Password & Block Suspicious IP: Once the captcha has been entered a new password will be generated which will be forwarded to the valid users mobile. The password generated will be dynamic for each time it’s been generated. If the number of failed login attempts made is more the particular IP will be traced and blocked for that particular user name pair.

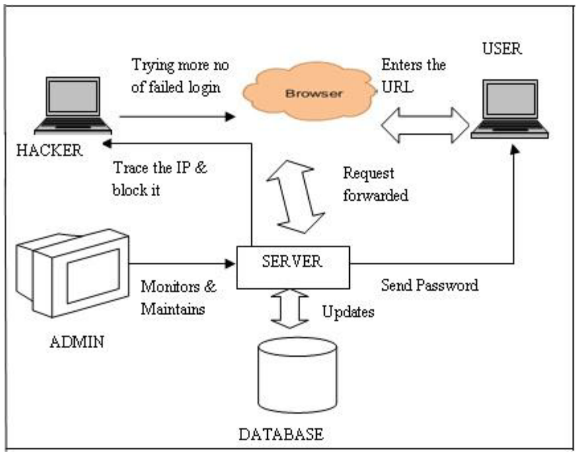


Fig 2. System Architecture.

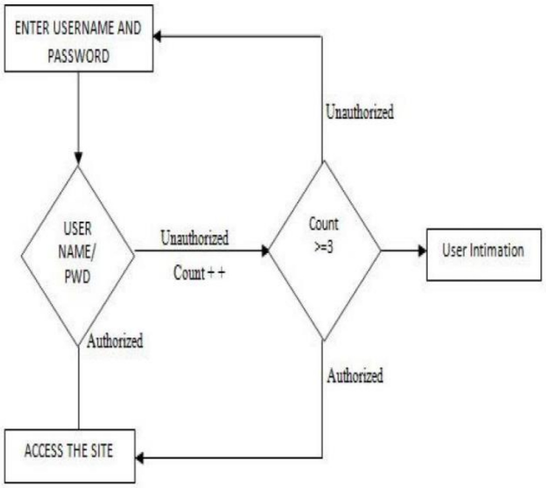


Fig 3. Flowchart of PGRP.

The functional requirements of the system is to resist the online guessing attacks over the passwords which are been achieved using the password guessing resistant 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.

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. The work shows 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. However, no user-testing of PGRP has been conducted so far. PGRP appears suitable for organizations of both small and large number of user accounts. The required system resources (e.g., memory space) are linearly proportional to the number of users in a system. PGRP can also be used with remote login services where cookies are not applicable.

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 Memory Stick Authentication Against Dictionary Attacks Yongge Wan, March 3, 2012.

4. Y. He and Z. Han, “User Authentication with Provable Security against Online Dictionary Attacks,” J. Networks, vol. 4, no. 3, May 2009.

5. J. Jayavasanthi Mabel, Mr. C. Balakrishnan, “Resisting Password Based Systems from Online Guessing Attacks” International Journal of Emerging Technology & Advanced Engineering Volume 3, Issue 1, January 2013.

6. Chippy. T, R. Nagendran,” Defenses against Large Scale Online Password Guessing Attacks by Using Persuasive Click Points” International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012.

7. Hacking Exposed: Network Security Secrets &Solutions, 5th Edition by Stuart McClure, Joel Scambray and George Kurtz.

8. Communication Networks by S. Hekmat.

9. Improving Web Application Security: Threats and Counter-measures**,** Mark Curphey.