Implementation of Password Guessing Resistant Protocol (PGRP) in Improving User Login Security on Academic Information System

by Arkhan Subari

Submission date: 21-Jan-2020 09:16AM (UTC+0700)
Submission ID: 1244240723
File name: arkhan-pgrp-asl.pdf (1.6M)
Word count: 1740
Character count: 9090

RESEARCH ARTICLE

Advanced Science Letters
Vol. 24, 9523–9525, 2018

Implementation of Password Guessing Resistant Protocol (PGRP) in Improving User Login Security on Academic Information System

Arkhan Subari*, Saiful Manan, and Eko Ariyanto

Electrical Engineering of Industrial Technology Department of Vocational School, Diponegoro University, Jl. Prof. Sudharto, SH., Tembalang, Semarang, 50275, Indonesia

One of the most widely methods of authentication is use user-id and password that entered on the login form. Users only need to memorize user-id and password then can login anywhere. But usually, users choose short and weak user-id and password that are easily stolen by brute force techniques. Brute force attacks are one of the most common attacks. The method is entry user-id and password on the login form repeatedly until attacker got a valid password. One alternative to overcome a brute force attack is use Password Guessing Resistant Protocol (PGRP). PGRP limits the number of failed login on login form. If the number of failed login reaches the specified number, then to re-login, user should contact system administrator in order to access login page again. This research is done on academic information system of Diponegoro University that not yet used security system on login form. Login form security is done by logging mechanism of IP Address and 2 level of security. If IP address is not recorded, ATT Challenge will appear, and user must pass this challenge to continue. At the security level, each security level is only allowed for 3 logins. At level 1, if after 3 failed login, user will be suspended for 1 minute. At level 2, if the login still fails then the user will be disabled. To reactivate, the account owner must contact the system administrator.

Keywords: Information System, Brute Force, PGRP, ATT Challenge.

1. INTRODUCTION

Information system is a set of components that interconnect, collect, process, store, and distribute information to support decision making and supervision within an organization.[1] In information system, authentication is used as a means to access a system that is confidential and limited. One of the most widely used methods is to use user-id and password entered on the login form.[1,2] Besides being cheap and does not require any enhancements, user-id and password usage is also convenient. Users only need to memorize user-id and password then can login anywhere.[5]

Nevertheless, use of user-id and password is not without weakness. Users often choose short and weak user-id and password that are easily stolen by brute force techniques. Brute force and dictionary attacks are common attacks observed in web applications.[4,9] In this type of attack, attacker runs an automated program to guess the password. Brute force attacks and dictionary attacks can be avoided by applying a locking mechanism in the system if it exceeds the number of failed login attempts.[4,5] One of those used is Automated Turing Tests (ATT, like CAPTCHA). ATT is one of the most effective defenses against online password guessing attacks.

However, this is an uncomfortable approach for legitimate users who have to answer ATT on every login attempt.[3] Users generally feel that by being an authorized user and placing the correct username and password, he should get immediate access without going through ATT. Users increasingly dislike ATT for claiming this as an unnecessary step. Thus, a new protocol has been introduced that is Password Guessing Resistant Protocol (PGRP).

In PGRP, legitimate users of known machines are restricted to go through ATT while enforcing ATT after several failed login attempts.[6] This is identified by the IP address stored on the login server as a white list, or cookies stored on the client machine. White list IP or cookies will expire after a certain time. It helps to avoid bots by enforcing ATT for users who try to login from unknown users and make some failed login attempts.[7] It will be more convenient for authorized users. The objectives of PGRP are as follows:[8]

1. PGRP protocol should make brute force and dictionary attacks ineffective.

*Author to whom correspondence should be addressed.

2. The protocol does not have to create legitimate users and other additional steps, just enter the login information.
3. The protocol should be easy to manage and scalable, requiring minimum computing resources in terms of memory, processing time, and disk space.

2. EXPERIMENTAL DETAILS

The idea of this research is to improve security system of academic information system of Diponegoro University. The concept of password guessing resistant protocol on information system shown at Figure 1.

When user enters a username and password, it will be checked. If username and password are valid, then the user's IP address will be saved on the white list and user is given a permissions to access information system according to the user group. If username and password are invalid, then it will be checked if user's IP address is listed on the white list.

If IP address is recorded, level 1 security flag will be added. If level 1 safety flag has reached the number 3, then level 2 security flag will be added and user will be given a 1 minute delay to access login form again. If level 2 security flag reaches number 3 then user will be disabled and should contact the administrator for access.

If IP address is not listed on white list, then user will be given an ATT challenge. If ATT challenge is unsuccessful by user, then user will be disabled and should contact the administrator for access again.

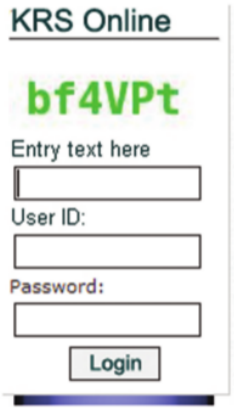

Fig. 2. CAPTCHA form will appear when ip address not in whitelist.

3. RESULTS AND DISCUSSION

ATT Challenge is performed if user's computer ip address is not on the specified list. If login attempt is failed, system will check the list of ip address that stored on the system. If ip address of a user who has failed login is not listed, it will display ATT Challenge (CAPTCHA) form along with system login form. When ATT Challenge is successfully passed (CAPTCHA field valid), user's ip address will be saved in whitelist. In this case, ATT

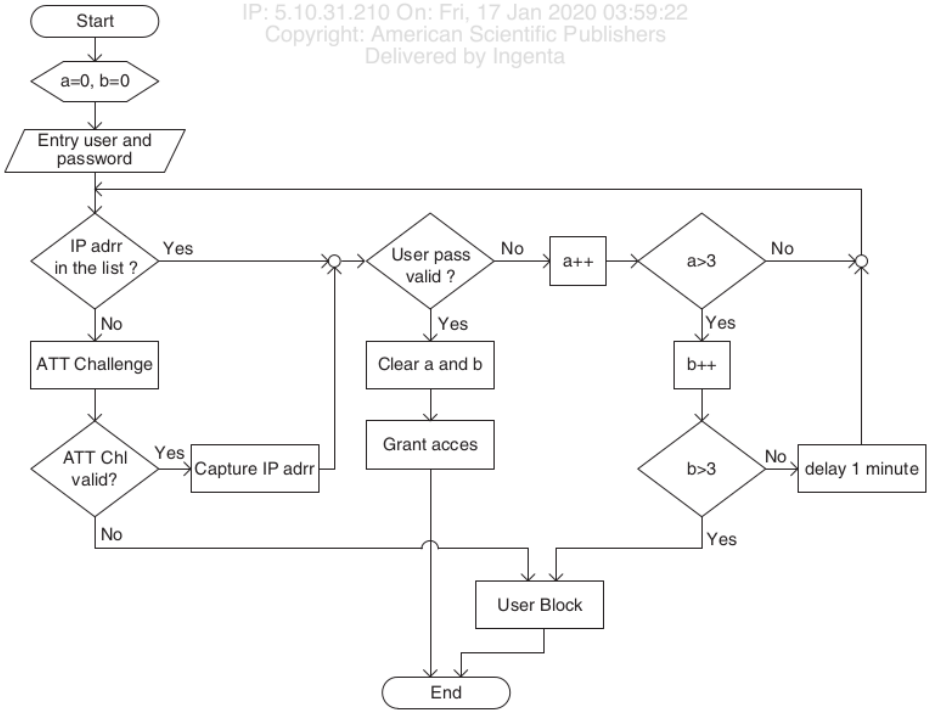

Fig. 1. Concept of password guessing resistant protocol on information system.

Fig. 3. Account will be disable if CAPTCHA is not correct.

Fig. 4. View page of temporary block account.

Challenge is not necessary for next login. But if the ATT Challenge fails, the user account will be disabled.

Figure 2 is an image that will appear when a login fails and user's computer ip address is not in the saved list. If user entry captcha correctly, user's ip address will be added to the saved list. However, if the captcha is not correct, account will be disabled and an error message as in Figure 3 will appear when the user log in.

Every login fail will be registrate security level flags 1 and 2, in accordance with the conditions. In initial conditions, login fail will record on level 1 security flag (field secure 1). It also recording failed login time occurs and stored in field lastattempt. If the contents of secure 1 has reached 3, then level 2 security flag (secure 2) will be added. This addition is continued by resetting secure 1, so next failed login will be recorded on secure 1. If secure 1 value has reached 3, user account will be temporarily disabled for 1 minute. This repeats on secure 2. If the value of secure 2 becomes 3, then account will be permanently disabled and must contact information system manager if it wants to be reactivated. View page of login failed process on academic information system is shown on Figure 4.

4. CONCLUSION

PGRP method is use to improve security system on academic information system of Diponegoro University. ATT Challenge on PGRP method is performed if user's computer ip address is not listed on whitelist. If ATT Challenge is successful, ip address will be added to the address list stored on the system. However, if ATT Challenge fails, account will be disabled and to activate it, user should contact the information system manager. There are added 2 (two) security levels designed using PGRP method in this academic information system that performed if user's ip address listed on whitelist. If first level security system is skipped, the user account will be temporarily disabled for 1 minute. If second level security system is bypassed, the user will be permanently disabled, and to activate it the user should contact the academic information system manager.

Acknowledgments: This work was supported in part by Vocational School of Diponegoro University.

References and Notes

1. Y. Yang, J. Zhou, J. Weng, and F. Bao, A new approach for anonymous password authentication, *2009 Annual Computer Security Applications Conference*, IEEE Computer Society **(2009)**, pp. 199–208.
2. E. Sediyono, K. I. Santoso, and Suhartono, Secure login by using one-time password authentication based on MD5 hash encrypted SMS, *International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013* **(2013)**, pp. 1604–1608.
3. A. Subari and Saiful Manan, Web secure login design with symetric encryption RC-6 algorithm, *The 1st International Conference on Information Systems for Business Competitiveness*, Diponegoro University **(2011)**, pp. 21–28, ISBN: 978-979-097-198-1.
4. Arya Kumar and A. K. Guptas, *Int. J. Eng. Res. Appl.* 656 **(2014)**.
5. Vaishali K. Kosamkar and V. M. Deshmukh, *International Journal of Advance Foundation and Research in Computer (IJAFRC)* 1, 96 (2014).
6. K. Rajakumari, *Middle-East Journal of Scientific Research* 20, 29 **(2014)**.
7. S. Kumar Samudrala, Venkatramulu Sunkari, and C. V. Guru Rao, *International Journal of Advanced Research in Computer Science and Software Engineering* 3, 1274 **(2013)**.
8. J. Mathew, *International Journal of Scientific Research* 4, 12 **(2015)**.
9. J. Jayavasanthi Mabel and C. Balakrishnan, *International Journal of Emerging Technology and Advanced Engineering* 3, 291 **(2013)**.

Received: 1 June 2017. Accepted: 1 August 2017.

Implementation of Password Guessing Resistant Protocol (PGRP) in Improving User Login Security on Academic Information System

ORIGINALITY REPORT

12%	10%	6%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

4%

★ eprints.undip.ac.id

Internet Source

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

Implementation of Password Guessing Resistant Protocol (PGRP) in Improving User Login Security on Academic Information System

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3