IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

# Blacklisted Password Authentication System

**Payal[1*], Suman Sangwan[2], Arun Malik[3]**

[1,2,3] Department of CSE, DCRUST, Murthal, India

[*]*Corresponding Author: payal.2112sangwan@gmail.com , Tel.: +91 7206302513*

DOI: https://doi.org/10.26438/ijcse/v7i6.633635 | Available online at: www.ijcseonline.org

Accepted: 25/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Passwords have always been one of the simplest security methods, weak passwords, default passwords can easily be cracked using brute force attack and dictionary attack which is very dangerous for security of systems across the globe. Security and privacy issues are the challenges faced in many systems. Blacklisted Password Authentication System is an attempt to decrease the efficiency of Dictionary, Brute force Attack which can be implemented in any authentication system without any significant changes.

***Keywords*—**Brute force Attack, Dictionary Attack, Authentication, Blacklisted Password

## I. INTRODUCTION

The rapid development of information and network technologies motivates the development of various new computing models. This also allow more network organisations to provide different services at the same time. To make sure that these services can only be accessed easily by authorized users, many password authentication schemes have been proposed. Password-based authentication scheme is specifically appealing due to its unique features that the password is easy to remember and the scheme is easily be deployed [1]. Basically, Authentication is the process of recognizing a user's identity. Digital world authenticators lack intelligence, they can only detect anomalies to a certain extent. This lack of intelligence makes them vulnerable to even basic attacks.

Traditional passwords are the most common and appropriate authentication scheme because they are familiar to all the users and easy to remember. However, this also makes the scheme vulnerable to offline password attack brute force attack. Blacklisted Password Authentication System is an attempt to decrease the efficiency of Dictionary attacks, Brute force Attack which can be implemented in any authentication system without any significant changes.

Section I contains the brief introduction, Section II contain the related work and problem description, Section III contain the methodology, Section IV contain the algorithm, Section V describes the efficiency of the system and Section VI concludes the research work with conclusion and future scope.

## II. RELATED WORK

Kolias, Constantinos, et al. [2] discusses the self propagating infectious nature of botnets. After only two months of source code deliverance, the number of bot instances occurred more than twice and a vast range of Mirai variants become apparent. Even today nearly a year after Mirai emerged bots continuing the exploiting of same weak security systems in the similar types of IoT devices.

Antonakakis, Manos, et al. [3] describes infection mechanism of Mirai botnet. If Mirai recognises a probable victim, it gain access in brute force login stage in that it attempt to establish a Telnet connection using different usernames and passwords choosed randomly from a pre-set list of 62 credentials. Problem of default password is depicted here.

Ari Juels, Ronald L. Rivest [4] proposes a easy and simple technique to enhance the security of hashed passwords: preservation of additional honeywords related with each user's account. Good technique for password management, Not a wholly satisfactory approach for user authentication.
Vasundhara R.Pagar, Rohini G.Pise [5] uses the concept of Honeyword technique to alert user of leaked passwords. The user is alerted whenever a Honeyword is used as a password. Honeywords mislead the attacker to guess correct password. Discusses various applications where Honeyword technique can be used.

Sohaib Khan, Fawad Khan [6] proposes a solution to use Attempt Based Password to make servers more secure. There will be three passwords for the first three attempts and then

 

repetition occurs. Unlike multiple passwords approach there will be only one password to remember i.e. the password for the third attempt. The other two passwords for the first and the second attempt are just the fragments of the password for the third attempt. Effort to break Attempt based passwords will be three times as compared to simple passwords. As only the password set for first attempt will be accepted on first attempt while the other two will be accepted at their respective attempts.

C.E. Shannon [7] introduces term entropy as to estimate the problems in terms of communication theory. Entropy is used as password strength measure across many password cracking methods. It is explained as a measure of "uncertainty" or "randomness" of random situation.

Taha, Mariam M., et al. [8] discusses the algorithm that examine the password robustness in terms of three estimates: password entropy, password quality indicator, and dictionary attacks. Describes features of passwords on behalf of these three measures.

Wantong Zheng, Chunfu Jia [9] uses the method that enhance the text passwords by inserting separators in between keystrokes. Using the blank space as the separators of passwords strengthen the website authentication against different attacks such as brute force attack.

Aakansha Gokhale et al. [10] studies the different password authentication techniques. The traditional method used for authentication is textual password which has digits and string of letters. Another technique for authentication is graphical passwords. After graphical password another security technique for authentication is captcha.

## III. METHODOLOGY

To make system more secure against bruteforce attack, we propose a new solution that will decrease efficiency of brute-force attack. A separate list of blacklisted passwords will be additionally maintained. Blacklisted passwords are here defined as passwords which if entered by a user, will send the login system into denial mode. Whenever user sets a password on the system, the user will also be asked to set a list of blacklisted passwords.

Further a threshold also needs to be set after which blacklisted passwords will be evaluated. If a malicious user (attacker) will try to brute-force the login process after threshold attempts, and uses one of the blacklisted password in the attempt, the device will enter into a denial mode in which device will deny every password even if attacker later tries a correct password.

In Bruteforce attack, attacker does not tries an already tested incorrect password. After system enters into denial mode, attacker even if tries correct password, he will have a reason to believe that this password is incorrect and won't try that password in future attempts, thus making system safe.
Blacklisted password usage attempt will be logged and will inform its usage when the legitimate user will login to the device.

## IV. ALGORITHM

0. Set FLAG=0
1. Set Threshold
2. Begin
3. Enter password
4. If attempts < Threshold
    a. If password = Correct
        i. Welcome
        ii. EXIT
    b. ELSE
        i. GOTO 2
5. Else
    a. If FLAG = 0
    b. If password = Correct
        i. Welcome
        ii. EXIT
6. If password exist in BLACKLISTED_PASSWORD
7. FLAG=1
8. GOTO 2

Where threshold is the number of attempts, a user is allowed to try any password before system starts Blacklisted Password Authentication method. Threshold is customizable to provide a balance of security and convenience.

## V. RESULT AND DISCUSSION

A system is simulated based on above algorithm on Java. A sample dictionary containing 3105 passwords [11] was tested against the system, with 1000 iterations with passwords at different positions in dictionary (for example correct password in 3rd attempt, 4th attempt and so on).
Efficiency here is defined as the number of times dictionary attack was defeated by the proposed system.

The result of different "Threshold" values on efficiency is visualised in graphs and tables. Based on the security requirement of system and user's convenience threshold can be adjusted.

 

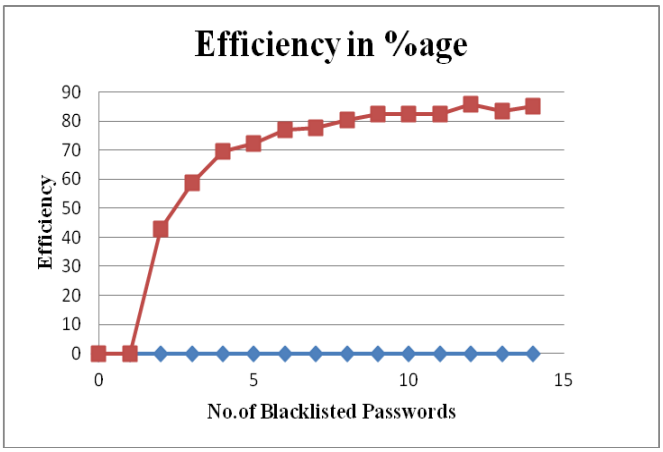


Figure 1 Efficiency of Blacklisted Authentication System when THRESHOLD = 5

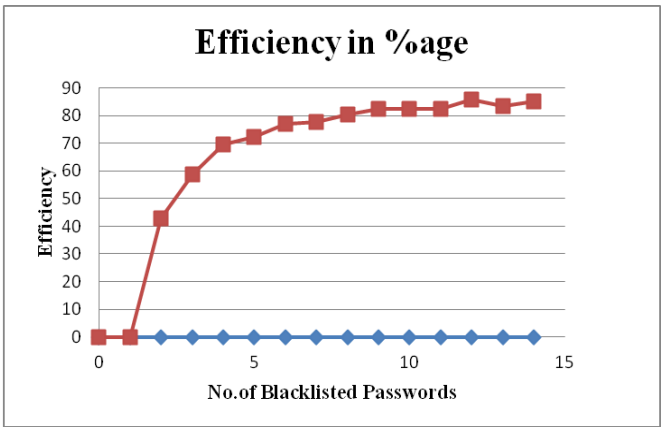


Figure 2 Efficiency of Blacklisted Authentication System when THRESHOLD = 10

## VI. CONCLUSION AND FUTURE SCOPE

By changing the THRESHOLD the efficiency of this Blacklisted password authentication system can be varied. The system is adequately secured from brute force and dictionary attacks when correct password is not tried in initial attempts. This system can be smoothly implemented in any existing authentication system with minor changes.

## REFERENCES

[1] Yan Zhao, Shiming Li, et al. "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment." Hindawi Security and Communication Networks , 2018.
[2] Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer Society IEEE. pp. 80-84, 2017.
[3] Antonakakis, Manos, et al. "Understanding the mirai botnet." 26th USENIX Security Symposium. pp. 1093-1110, 2017.
[4] Ari Juels, et al. "Honeywords: Making Password-Cracking Detectable", ACM, pp. 145-156, 2013.
[5] Vasundhara R.Pagar, Rohini G.Pise, "Strengthening Password Security through Honeyword and HoneyEncryption Technique", IEEE, pp. 827-831, 2017.
[6] Sohaib Khan, Fawad Khan, "Attempt based Password", in Proceedings of 13th International Bhurban Conference on Applied Science and Technology. IEEE, pp. 300-304, 2016.
[7] C.E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, pp. 379-423, 1948.
[8] Taha, Mariam M., et al. "On password strength measurements: Password entropy and password quality." In ICCEEE, IEEE, 2013.
[9] Wantong Zheng, et al. "CombinedPWD: A New Password Authentication Mechanism using Separators between Keystrokes", 13th ICCIS Conference IEEE, pp. 557-560, 2017.
[10] Aakansha Gokhale,et al., "A Study of Various Passwords Authentication Techniques" International Journal of Computer Applications(0975–8887) International Conference on Advances in Science and Technology (ICAST), 2014
[11] Pa, Yin Minn Pa, et al. "Iotpot: A novel honeypot for revealing current iot threats." Journal of Information Processing 24.3, pp. 522-533,2016.
[12] John the Ripper password cracker, http://www.openwall.com/john/

## Authors Profile

*Ms. Payal* pursed Bachelor of Technology from MDU, Rohtak in 2016 and currently pursuing Master of Technology from Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana India. Her main research work focuses on Information Security.

*Dr Suman Sangwan* has been into teaching and research for about 16 years. She did her Ph.D. from Deenbandhu Chhotu Ram University of Science and Technology, Murthal(Haryana) India. Her research areas include Network Security and Heterogeneous Wireless Networks. She received her M.Tech. degree in Computer Science & Engineering from Kurukshetra University, Kurukshetra, INDIA. She has published more than 20 papers in various journals and conferences of repute.

*Mr. Arun Malik* pursed Bachelor of Technology from College of Engineering Roorkee, Roorkee in 2016 and currently pursuing Master of Technology from Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India. His main research work focuses on Information Security.

 