IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

False Positive and False Negative Authentication System

Arun Malik[1*], Suman Sangwan[2], Devender Rathee [3], Vineet Nandal [4], Payal [5]

[1,2,3,4,5] Department of CSE, DCRUST, Murthal, India
[*]*Corresponding Author: arun.dcrust@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i5.922924 | Available online at: www.ijcseonline.org

Accepted: 18/May/2019, Published: 31/May/2019

***Abstract*—** Weak passwords, default passwords in combination with bruteforce attack and dictionary attack are one of the most dangerous combination for security of systems across the globe. False Positive and False Negative Password Authentication System is an attempt to decrease the efficiency of Dictionary, Bruteforce Attack which can be implemented in any authentication system without any significant changes.

***Keywords*—**Bruteforce, Dictionary, Attacks, Botnets, Authentication System

I. INTRODUCTION

Authentication is one of the core aspect of digital world. In physical world authentication is generally done by issued Photo ID Cards, Signatures, Biometrics, Shared Secrets etc which are generally verified by human agents and access is granted. But in digital world password based authentication has been in prevalence, Verification logic matches user supplied password with system stored password and access is granted. Physical world Authenticators (humans) are intelligent, they can think beyond simple verification logic and detect anomalies if any and take any unprecedented action. 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. False Positive and False Negative Password Authentication System is an attempt to decrease the efficiency of Dictionary, Bruteforce 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 architecture and algorithm, Section V describes the efficiency of the system.

II. RELATED WORK

Bruteforce Attack is such one such attack which is threat to security of system.

In Bruteforce attack, attacker keeps trying several passwords (usually entire keyspace) until he finds out correct password.

Dictionary Attack is a slightly more targeted attack where attacker only tries passwords which are most likely to be correct.

Dictionary attack are more efficient over systems with default passwords or simple passwords. Some systems even have backdoor accounts or accounts whose passwords can't be changed. Such systems are the best targets for dictionary attacks.

With rise of IoT, abundance of internet connected devices have increased manifold. The abundance of same (hardware,software) type of IoT makes the ideal target for "malicious user". If the "malicious user" discovers a "0day" vulnerability on any one of the device it is very likely it can be leveraged to millions of same devices across the internet.

"Botnets" generally favour these IoT devices. Because of small size, capacity, processing power, power requirements these IoT devices tend to be simple. Multiple examples have shown they even lack basic security systems.[1][4][5]

"Remote Access" is one of the main aspect of IoT devices. Due to limited processing power, traditionally IoT devices have relied on Plaintext and/or TELNET based Remote access authentication.

These devices generally have no password strength policy defined, and possibility to change default passwords.

Some devices even have hidden backdoor accounts which can be easily discovered by reversing the firmware and / or by dumping the memory of device.

Recently discovered one of the most powerful botnet variant "Mirai" used dictionary attack to compromise millions of devices worldwide. The botnet used its dictionary of limited passwords and easily attacked devices.

III. METHODOLOGY

Strength of bruteforce and dictionary based attack lies in the fact password either the system accepts password or denies password (Binary Nature). We propose to introduce fuzziness, say "Positive Fuzziness" in the authentication system, thus turning strength of bruteforce attack to its weakness.

If the system denies the correct password even once, it wont make any sense to try the same password again in the context of traditional systems and Bruteforce attack.

If system denies correct password even once it will be assured the system will withstand the attack. This approach alone does not make system 100% secure.

We further propose add another fuzziness, say "Negative Fuzziness" to the system by adding Honeypot layer. Bruteforce attack will fail if it has reason to believe it has found the correct password.

Now this fuzziness will make attacker believe his incorrect password is correct because of Honeypot redirection which will lead to failure of "Bruteforce" attack.

Both of these fuzziness combined will significantly improve security of device with negligible effort.

When correct password is rejected as incorrect password - False Negative.

When incorrect password is apparently accepted as correct password- False Positive.

IV. ALGORITHM

0. Set THRESHOLD = (1-100)

1. Begin

2. Enter password

3. If attempts < SAFE_ATTEMPTS

    If password = Correct_Password

        Welcome

        EXIT

    ELSE

        GOTO 2

4. Else

5. If password = Correct_Password

6. r_no = Gen Random No.(1-100)

7. If r_no <= THRESHOLD

8. Welcome

9. EXIT

10. Else

11. REDIRECT TO HONEYPOT

12. EXIT

THRESHOLD and SAFE_ATTEMPTS are tweakable parameters.

V. EFFICIENCY

A system is simulated based on above algorithm on Java. A sample dictionary containing 3107 passwords [8] was tested

against the system, with 1000 iterations with passwords at different positions in dictionary (for example correct password in 4th attempt, 5th attempt and so on)

Efficiency here is defined as the number of times dictionary attack was defeated by the proposed system.

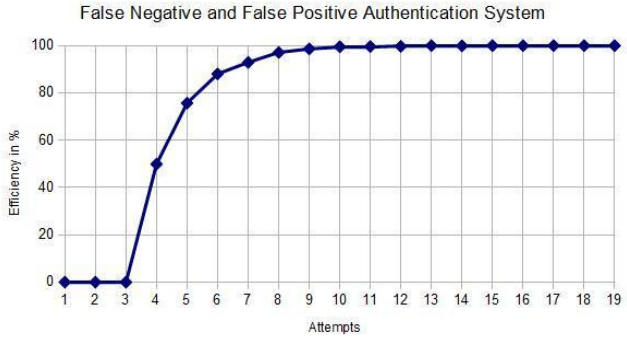

Figure 1. Efficiency of False Negative and False Positive Authentication System when THRESHOLD = 50, SAFE_ATTEMPTS = 3

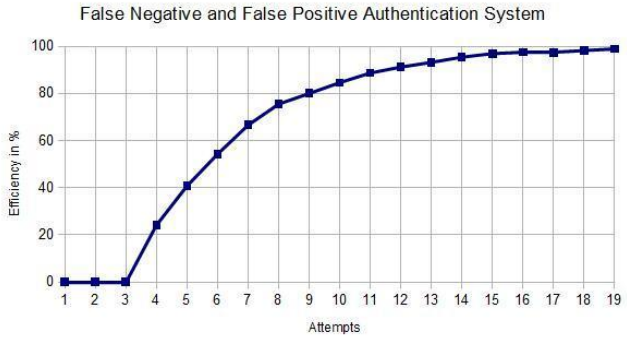

Figure 2. Efficiency of False Negative and False Positive Authentication System when THRESHOLD = 75, SAFE_ATTEMPTS = 3

VI. CONCLUSION AND FUTURE SCOPE

By changing the THRESHOLD and number of SAFE_EVENTS the efficiency of this False Negative and False Positive authentication system can be varied. The system is sufficiently secured from dictionary attacks when correct password is not tried in initial attempts. This system can be easily implemented in any existing authentication system with minor changes.

REFERENCES

[1] Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer 50.7 (2017): 80-84.

[2] "'BrickerBot' Results in PDoS Attack," Radware, 5 Apr. 2017; security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-Service.

[3] S. Edwards and I. Profetis, "Hajime: Analysis of a Decentralized Internet Worm for IoT Devices," Rapidity Networks; 16 Oct. 2016; security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

[4] Antonakakis, Manos, et al. "Understanding the mirai botnet." USENIX Security Symposium. 2017.

[5] De Donno, Michele, et al. "Analysis of DDoS-capable IoT malwares." Computer Science and Information Systems(FedCSIS), 2017 Federated Conference on. IEEE, 2017.

[6] Sharaf-Dabbagh, Y., & Saad, W. "On the authentication of devices in the Internet of things" 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks .

[7] Pinkas, Benny, and Tomas Sander. "Securing passwords against dictionary attacks." Proceedings of the 9th ACM conference on Computer and communications security, ACM, 2002.

[8] John the Ripper password cracker, http://www.openwall.com/john/

Authors Profile

Mr. Arun Malik pursed Bachelor of Technology from Uttarakhand Technical University, Dehradun, India 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.

Dr Suman 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. Devender Rathee pursed Bachelor of Technology from Hindu College, Sonipat, India in 2017 and currently pursuing Master of Technology from Deenbandhu Chhotu Ram University of Science and Technology, Murthal. His main research work focuses on Information Security.

Mr. Vineet Nandal pursed Bachelor of Technology from MDU, Rohtak India in 2014 and currently pursuing Master of Technology from Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India. His main research work focuses on Software Testing, Information Security.

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.

