iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4446

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Honeywords: The New Approach for Password Security

Prof. Vruhali Thakur[1], Akash Kamble[2], Abhishek Hatankar[3], Rushikesh Jagdale[4], Ankita Talekar[5]
[1, 2, 3, 4, 5]*Information Technology, Saraswati College of Engineering*, Mumbai, India

Abstract: Abstract: The traditional systems only use username and password hashes for security. The research in the area of security shows that most of the passwords hashes have possibility of being compromised by hackers. Honeywords (false passwords) generation system is appropriate to protect hashed password files. In our system Honeywords are stored along with the original user password in the password file of the database. If the database is compromised by the hacker the hacker will not be able to recognize the real password. When the hacker tries to login into the system with one of the Honeywords, the system will trigger and redirect the hacker to the fake website and notify the user (via text message and mail).
Keywords: Honey words Chaffing, Authentication, Hashing.

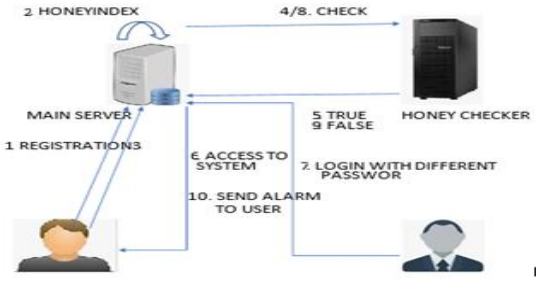
I. INTRODUCTION

Compromisation of the password files is a very huge security problem which has affected many users and big companies like yahoo, rock you, LinkedIn, eHarmony and adobe target of many possible cyber-attacks. For example, the LinkedIn passwords were using the-e SHA-1 algorithm without a salt and similarly the passwords in the eHarmony system were also stored using unsalted MD5 hashes [3]. Indeed, once a password file is stolen, by using the password cracking techniques like the algorithm of Weir et al. [4] it is easy to capture most of the plaintext passwords. This idea has been modified by Herley and Florencio [7] to protect online banking accounts from password brute-force attacks. According to the study, for each user incorrect login attempts with some passwords lead to honeypot accounts, i.e. malicious behavior is recognized. In this model, the fake password sets are stored with the real user password set to conceal the real passwords, thereby forcing an adversary to carry out a considerable amount of online work before getting the correct information. Recently Juels and Rivest [11] have introduced the honeyword mechanism to detect a hacker/attacker who attempt to login with the cracked passwords. Basically, for every username a set of honeywords is constructed such that it only has one original password and the others are decoy passwords to fool the hacker/attacker. Hence, when an attacker/hacker tries to enter onto the system with a honeyword, an alarm is triggered to notify the admin about the compromised password file.

II. PROTOTYPE

In this paper we proposed honey words (decoy passwords) to detect attacks against hashed password databases. For each user account, the legitimate password is stored with several honey words in order to sense impersonation. If honey words are selected properly, a cyber-attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honey word for any account. However, entering with a honey word to login will trigger the alarm notifying the admin about a password file has been compromised. Also, we suggest a new approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honey word generation method – and also to reduce storage cost of the honey word scheme.

A. Diagrams



System Architecture

1) User Registration (Sign In / Sign Up): Username and password are required from the user to register the system.
2) Creating HoneyIndex: Honeyindexes are generated periodically honeyindex set of each account should be regenerated.
3) Generating Honey Words: Is an auxiliary service, honeychecker is employed to store correct indexes for each account.
4) Alarm to the user: Here hacker login to the system. And if he/she tries to access the system and if he/she enters any honeyword from password file then the notification or alert message is given to the real user.

B. Applications

System have ton of applications such as:

1) Online banking transaction in our proposing system we are going to to create and store honeywords in the Honeywords that are generate from the user details. Because of doing this if any unauthorized attacker/hacker will try to guess the password and if that guess password match with the honeywords then alert will generate for the legal user and only login fail message will shows to that user.
2) System Security: Our system will provide password security.
3) Online shopping transaction system

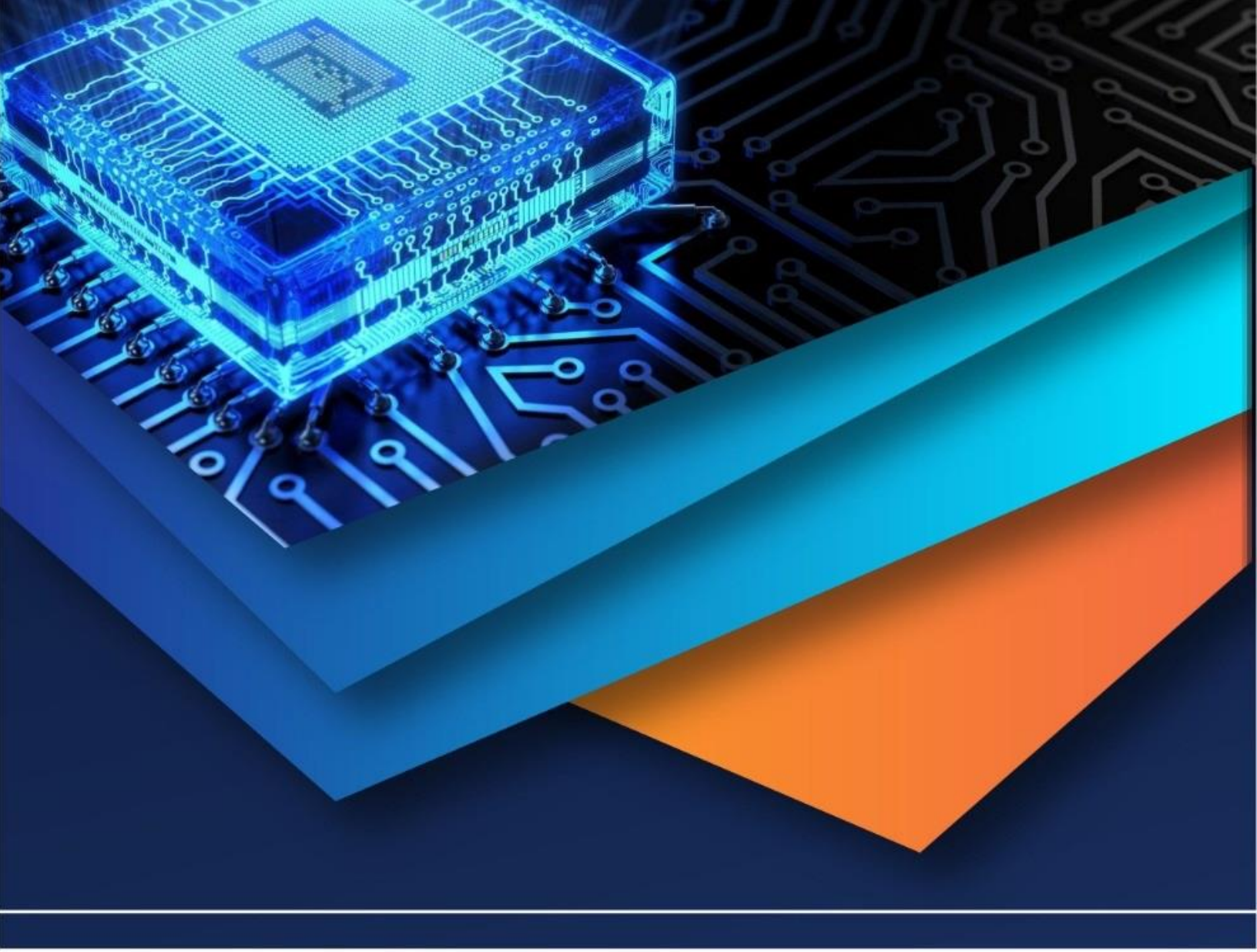
III.FUTURE SCOPE & CONCLUSION

Adding up to this system, in near future we can add more protocols and algorithms which can strengthen up the security and can be more effective towards protecting the system. Various new aspects such as hybrid generation algorithm can be added which will help to increase the level of security which would make it difficult to be accessed by unauthorized user.

With all the conceptual and practical knowledge that we have attained we predetermined the security of honeyword framework wherein we look upon to provide maximum security to user's personal or business data. This concept works on creating a fake password or a decoy password which helps to detect if there is any attack on the system and if security level breach is detected. Once the system detects unauthorized access the system diverts the intruder to another website or url thus diverting his attention and safeguarding the users information. A counter step is taken by system by notifying the user by sending an email of the possible threat along with the necessary action that needs to be taken. In all this system adds up a vital level of security besides normal security levels present. We look upon to provide a user friendly and a system on which a user can confidently rely on.

REFERENCES

[1] Imran Erguler," Achieving Flatness: Selecting the Honeywords from Existing User Passwords",DOI 0.1109/TDSC.2015.2406707, IEEE Transactions on Dependable and Secure Computing.
[2] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of the 9th USENIX Security Symposium, 2000.
[3] The LinkedIn Hack: Understanding Why It Was So Easy to Crack the Passwords: https://www.linkedin.com/pulse/linkedin-hack-understanding-why-so-easy-crack-tyler-cohen-wood
[4] Weir, M., Aggarwal, S., de Medeiros, B., Glodek, B.: Password cracking using probabilistic context-free grammars. In: Security and Privacy, 2009 30th IEEE Symposium on, IEEE (2009) 391–405 D. Mirante and C. Justin, "Understanding Password Database Compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TRCSE-2013-02, 2013.
[5] D. Mirante and C. Justin, "Understanding Password Database Compromises," Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TRCSE-2013-02, 2013.
[6] A. Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times, vol. 20, 2010.
[7] Herley, C., Florencio, D.: Protecting financial institutions from brute-force attacks. In: SEC'08. (2008) 681–685.
[8] A Security Analysis of Honeywords Ding Wang, Haibo Cheng, Ping Wang Peking University@pku.edu.cn.
[9] Honeywords for Password Security and Management by Manisha Bhole June -2017. https://www.irjet.net/archives/V4/i6/IRJET-V4I695.pdf
[10] Examination of a New Defense Mechanism: Honeywords Ziya Alper Genc , S¨uleyman Kardas¸ Mehmet Sabir Kiraz∗
[11] A. Juels and R. L. Rivest, "Honeywords: Making Password cracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 145–160. [Online].Available: http://doi.acm.org/10.1145/2508859.2516671



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY