© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 11 Issue: 02 | April - June 2020
Paper is available at http://www.jrps.in | Email : info@jrps.in

Detection of Burglar and Password Security Through Honeywords With IP Blocking

Ujwal Malik, Akshay Ilkar, Amit Dharmik,Tauqir Ali Sayyad
B.E. Student, Department of Computer Science

Prof. Mohammad Sajid,
Assistant Proferssor, Department of Computer Science

ABSTRACT

This abstract presents the work related to the password security. The presented work consists of two main parts. The first part is related to the generation of Honeywords and the second part is associated with IP blocking.

For the first part of generation of Honeywords, we will use the method of chaffing-by-tail-tweaking method in which the last t positions of password are chosen and are altered. Using this mechanism, Honeywords are generated.

For the second part of IP blocking, we have to first log the IP of the user to monitor its activity and based on that we can choose whether to block the IP or not. For logging the IP, we have to use environment variables of the server.

INTRODUCTION

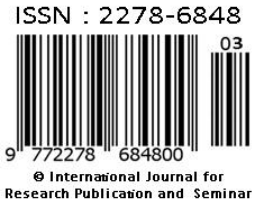
The basic terminologies of this work are given below:

I. **Honeywords**

Honeywords are decoy (or false) passwords that can be used to trick the malicious user. By using Honeywords we can detect possible data breaches and can be used to make systems a little more secure. Whenever Honeywords are entered by the user, it will indicate a possible data breach. Honeywords can be used in almost anywhere where passwords are to be stored.

The confidential data of the companies as well as the users can be in the hands of hackers

II. **Encryption**



Encryption is a technique used for obfuscating certaintext, generally the sensitive text such as passwords. There are many popular encryption methods which are used for different purpose. We used SHA-256(Secure Hash Algorithm) for encrypting the passwords as well as Honeywords because storing passwords in plain text is dangerous.

III. **IP Logging**

Whenever a user visits the website, he will have to first request the server for the website. The server will process the request and send it back to the IP from which this request was generated. As the server knows the IP, it can log it using some environment variables. This IP can be used to flag use based on their activity on the system or the website they are using.

Literature Review

1. Honeywords: Making Password-Cracking Detectable

Juels and Rivest [1] have introduced the concept of Honeywords. For every registered user, a list of Honeyword is generated. These Honeywords are produced using Honeyword generating algorithm. They used a server named honeychecker which was used to check whether if the credentials entered are real passwords or Honeywords. But in this system some possible attacks were highlighted such as attacking the honeychecker.

2. Dangers of Weak Hashes

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 11 Issue: 02 | April - June 2020
Paper is available at http://www.jrps.in | Email : info@jrps.in

due to password leaks. Thus, it was concluded that strong hashing mechanisms are needed to be implemented for the security purpose which are not broken and does not have any hash collisions which accounts for a bad hashing algorithm.

3. SQL injections

According to C. Sharma and S.C. Jain [3], we should never trust on user provided data as the user can provide some data which can make the system act in a weird way. In the fields of login credentials, the user can enter SQL (Structured Query Language) queries that can either dump the whole database or can delete the entire database. Some commands can also be entered which can result in Cross-Site-Scripting (XSS) which provides remote code execution.

OUR APPROACH

In our approach, we used Honeywords as a trigger which will be set off when these Honeywords are entered by unauthorized users. Honeywords are also a good way to confuse the unauthorized users with wrong information for securing the original data. We will generate a list of Honeywords so For hashing, we used SHA-256 algorithm which is good (i.e. not broken, does not have any hash collisions) and does not use high computing power so quicker response times. Whenever these Honeywords are used, they will trigger an alarm indicating a possible data breach. This system keeps a track of the user's IP. Using IP logging we can block users based on their activity on the system.

B. IP Logging

To monitor the activity of user, one of the methods is to use its IP address. Through IP address we can tell if the user is authorized to access the system or not. We can use the environment variables of the server .Moreover, to minimize the over-head, we will only log the IP when the user has done some malicious activity on the system.

According to K. Brown [2], for a system to be secure it is necessary to use methods for hashing that are strong and which are not broken. Many companies which does not follow good hashing methods had to compromised their password files which had affects their reputation a lot.

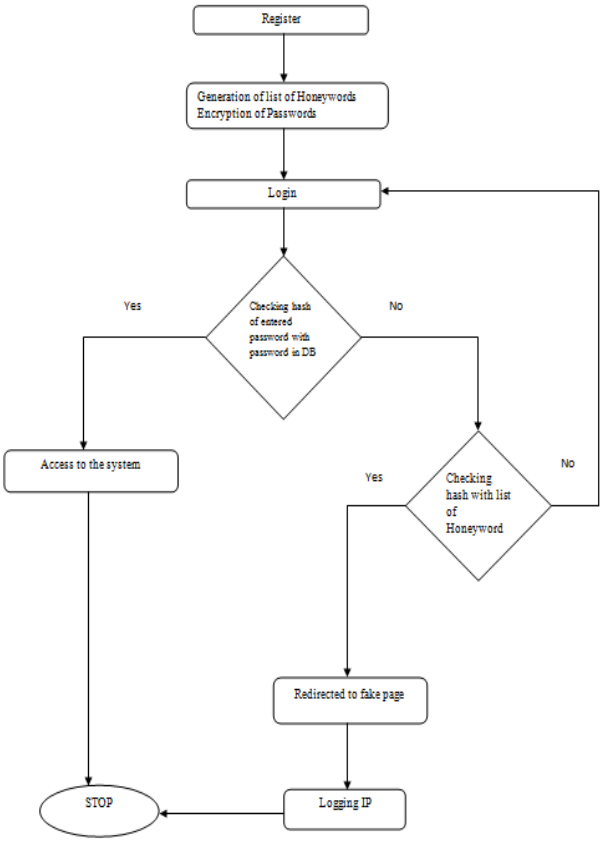


Fig 1: Data Flow Diagram

A. Honeyword Generation

As already mentioned, Honeywords are decoy passwords which are very similar to the actual passwords. Before using we have to first generate the list of Honeywords to be used. For generating a list of Honeywords, we are changing only last two characters to a random ASCII printable character. This makes the list of Honeywords look similar to the actual password thus confusing the hacker about the real password ad tricking him into entering the Honeywords which then sets an alarm. Also, these passwords are not stored as-it-is, only the SHA-256 hash values of the passwords and Honeywords are stored which makes them a little hard to crack.

as to provide security to a greater extent. For Honeyword generation, we implemented a

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 11 Issue: 02 | April - June 2020
Paper is available at http://www.jrps.in | Email : info@jrps.in

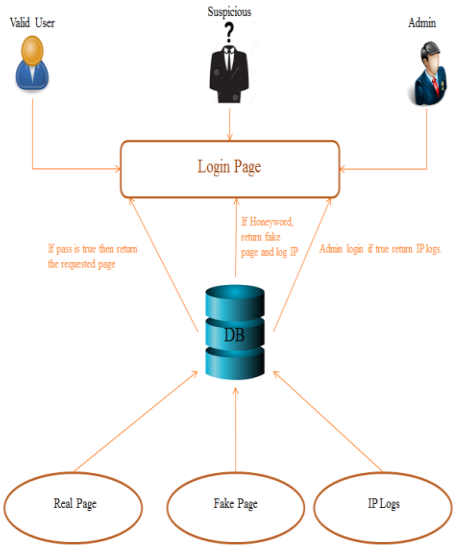


Fig 2: Basic Overview of System

RESULTS AND DISCUSSION

For accessing the system, the user must be registered on the system, i.e. its entry should be on the database. Whenever the user registers, a list of Honeyword is generated.

By using the concept of Honeywords, we can trick the hacker and indicate any possible data breaches.

Whenever an unauthorized user tries to log in to the system with fake credentials, his IP address will be logged.

CONCLUSION

Confusing the attacker with the fake information was the primary goal of this work and by using the concept of Honeywords we achieved this goal. This approach protects the user's real data. We propose a new approach for making the system a little more secure by using decoy information mechanism. We use this Honeyword technology for giving hackers fake data and securing the user's real data.

The addition of IP logging helps to block the unauthorized users from accessing the system thus providing the system a little more security.

Honeyword generator function which generates only printable ASCII characters and produces Honeywords.

REFERENCES

[1] A. Juels and R.L. Rivest, "*Honeywords: Making Password Cracking Detectable*", In Proceedings of the 2013 ACM SIGSAC conference on Computer & communication security, *p. 145-169, November 2013*.

[2] Brown and Kelly, "*The dangers of weak hashes*", SANS Institute Infosec Reading Room, *November 2013*.

[3] C. Sharma and S.C. Jain, "*Analysis and classification of SQL injection vulnerabilities and attacks on web applications*", 2014 International Conference on Advances in Engineering & Technology Research, *August 2014*