Data Prevention Using Honeywords

Pranav Bhagat[1], Ifra Khan[2], Sadia Ameen[3], Mumtaz Parveen[4], Sadia Patka[5]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[5]Asst. Professor, Dept of Computer Science and Engineering,
[1, 2, 3, 4, 5] Anjuman College of Engineering &Technology, Rashtrasant Tukadoji Maharaj , Nagpur University, Nagpur, Maharashtra, India

Abstract- *Security of data plays a significant and vital role in recent times. The techniques available for securing data nowadays could be easily speculated by mere guessing and also some procedures require the use of third hand devices such as OTP generators. Data prevention using honeywords is a new and better technique than the ones talked about earlier. Here user's legitimate passwords are combined with honeywords forming a set of sweet words which are stored in the database within an encrypted file. Even if an intruder gets these sweet words he won't be able to get through the data of the system as it will just confuse him with the honeywords . Also if he tries to login with these sweet words he won't be able to get access to the data but will be given access to a page containing decoy files after his 3 attempts for password login. This system also contains a second level of authentication i.e. the key validation step. The user will also get notified of the breach after the adversaries three attempt during login.*

I. INTRODUCTION

Passwords are a crucial part of data security , users generally tend to have passwords which are related to their personal details which they use them at miscellaneous sites thus becoming an easy victim to the intruder .Honeywords are originated from honeypot .Honeypot was a trap made to detect and deflect an invader to unapproved usage of data by creating fake accounts. On the other hand honeywords are fake passwords used to invent ambiguity for an invader. Honeywords are amalgamated with user's genuine passwords forming sweetwords .These sweetwords even after getting hacked by an attacker creates confusion for him as he does not know which is the real password. If he tries to login with or without these sweetwords then after 3 attempts he will be designated to a page containing decoy files. If anyhow he gets access to the login page then also he has to enter a key which is given to the legitimate user at the time of registeration. For this also if the invader applies guessing of the key then after 3 attempts he will be given access to decoy files. For both the login and key validation step the user will be warned (notified) about the infringement after the intruders 3 attempts with or without the honeywords[1].

II. LITERATURE REVIEW

Prof. Ronald L. & Ari Juels in their paper "Honeywords: Making Password Cracking Detectable" where they proposed a method for improving the security hashed passwords related with each user's account. The use of honeywords may be very helpful in the current environment, and is easy to implement. The fact that it works for every user account is its big advantage over the related technique of honeypot accounts [2]. But they did not prepare with data prevention as still there was probability that the adversary can get to the real password.

Prashant Muthiya & Sachin Padvi in their paper "Achieving Flatness: Selecting Honeywords from Existing User Passwords". In this system they survey the honey word system and present some remarks to highlight possible weak points at any attacker who's able to steal a copy of a password file won't know if the information it contains is real or fake. They pointed out that the strength of the honeyword system directly depends on the generation algorithm, i.e., the generator algorithm determines the chance of distinguishing the correct password out of respective sweetwords [2].

III. PROPOSED SYSTEM

The proposed system targets on preventing the data from exploitation and also to identify the act of violation i.e. data breach. Honeywords are generated after user registers into the system which is placed in conjunction with the user's original password in an encrypted file within the database. The two major features of this system is to safeguard the data from an invader and also to track down the infringement of the data violation occurred. The system has two levels of authentication first being the login of the user and second is the key validation step .The key is formed at the time of registration by the user where he/she will be asked questions and based upon the answer given by the user a key will be formed which will be given to the user only once at the time of registration. If the intruder tries to hack into the account with or without the sweetwords then after three attempts he will be directed to a page containing decoy files and at the same time an alert message will be send to the genuine user telling him about the breach . This same thing happens during the key validation step .

The proposed work is done by dividing it into various modules as follows:

- Registration: Here user is enlisted into framework. At the time of enlistment, entering password, framework will create honeywords along with them genuine password's is stored at particular arbitrary position. Moreover, user will be inquired for a few questions and the reply of those questions will allow user a key which will act as a second password.

- Login: Here user is going to log in to the system. If both the password and the key matches, user is authenticated .

- Adversary: Here Adversary will log into the system. In the event if he tries to break into the system and enters any honeyword then the alert is sent to the real user. And if suppose he try combination of password and it goes more than three attempt and also entered password does not coordinate with the honeywords then he get access the file but all files are decoy files.

- File Upload and View: Authenticated user to the system can upload file into the System and can view his uploaded files too.

- Admin Login: Here admin is log into the system. Admin has the privileges to control over the mechanism. Admin has the authorization to maintain the user accounts.

- Decoy File Upload: Here admin can add the decoy file of the uploaded file. If unauthorized user tries to attempt log in and fails to succeed three attempts, then he/she can get access to files but those files will be decoy files.

IV. RESULTS AND DISCUSSION

The results include the user registration page where he needs to enter the valid email-id and the password.

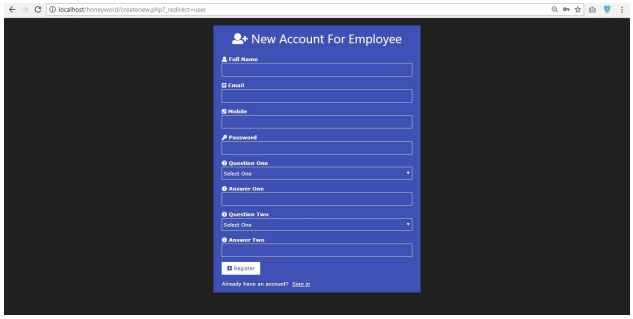

Fig 01: Registration Page

Above figure shows the registration page , were user will enter his details and get his unique key .

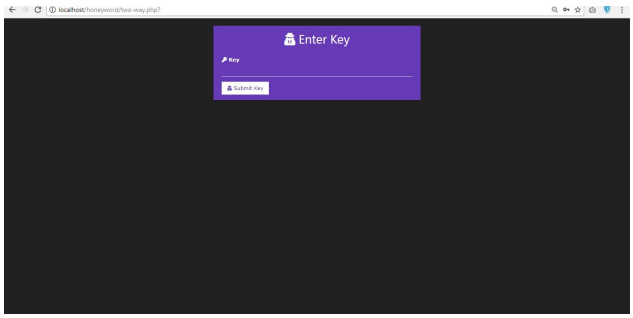

Fig 02: Key Page

Above page will come after the valid password is entered at the login screen ,then at this page the user will enter the unique key he gets . If the enter the correct key only then he will get access to the account details and its files.

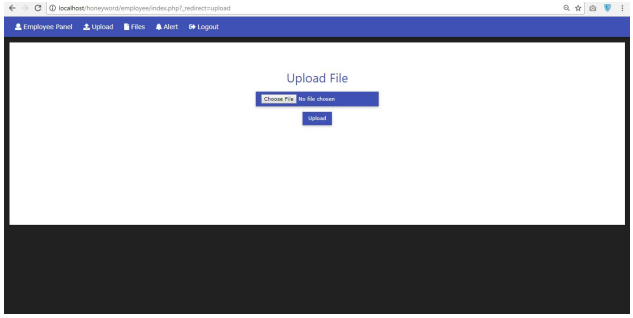

Fig 03: File Uploading Page

After successful log in the user can upload files which he wants to protect using this framework of honeywords.

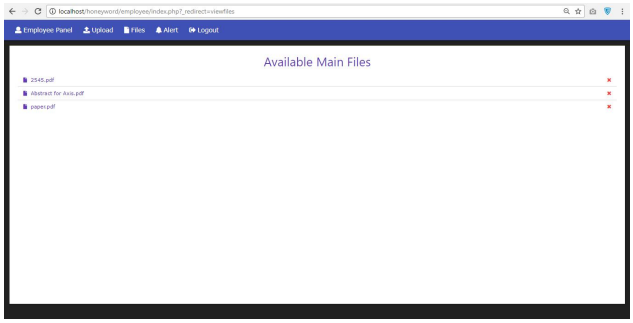

Fig 04: Viewing Files uploaded by User

Above figure depicts the files which user has uploaded.

V. FUTURE SCOPE

Password security has always been a domain of active research. The big difference between the traditional methods and when honeywords are used is that a successful brute-force password attack does not gives the attacker confidence that he can log in into system successfully without being detected.

This system can be applied on various domains like:

- In Online shopping , nowadays expensive things are also sold online so information and location of the items can be protected using this system.
- In Banking OTPs can be replaced by this system, as its a hassle to handle OTP.
- Vaults System in various domains can have this system to protect valuable items.
- E-mail clients can use this mechanism.
- Surveillance system can use to keep there data secure from hackers.
- This System can be used with fingerprint Scanner or Face Recognition can become a unbreakable security system.

VI. CONCLUSION

Password security has always been a domain of active research. The big difference between the traditional methods and when honeywords are used is that a successful brute-force password attack does not gives the attacker confidence that he can log in into system successfully without being detected. The use of decoy data mechanism will secure the confidential data of the authorized users from the hacker. In honeyword based authentication approach, it is sure that the attacker will be detected. The main aim of project is to validate whether data access is authorized or not when abnormal information access is detected. Confusing the attacker with decoy data protects from the misuse of the user‘s real data. With the use of an additional level of validation i.e. a key and the encryption of file where sweet words are stored provides more reliability from data breaching and trespassing by an intruder.

REFERENCES

[1] Mumtaz Pareveen & Ifra Khan , "Prevention of Data using Concept of Honeywords" in Journal of International Journal of Computer Science and Mobile Computing ,ISSN:2320-088X, Volume 07 , Issue :02 ,Feb - 2018 ,pp. 120 - 123.

[2] Pranav Bhagat & Sadia Ameen et. al. , "Review on Data Prevention using Honeywords" in Journal of International Journal of Scientific Research in Science and Technology (IJSRST), e-ISSN:2395-602X ,ISSN:2395-6011, Volume 04 , Issue :03 ,Jan - 2018 ,pp. 403 - 405 .

[3] A. Juels and R. L. Rivest, "Honeywords: Making Password-crackingDetectable" in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communication Security, ser. CCS ‟2013. New York, NY, USA: ACM, 2013, pp. 145–160.

[4] Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 284 - 1295, February 2015.

[5] Manisha Bhole, "Honeywords for Password Security and Management" in Journal of International Research Journal of Engineering
and Technology(IRJET)– e-ISSN:2395-0056 ,ISSN:2395-0072, Volume 04 , Issue :06 ,June - 2017 ,pp. 534 - 538 .

[6] Prashant Muthiya & Sachin Padvi et. al.,"Achieving Flatness : Selecting Honeywords From Existing User Passwords" in Journal of International Journal for Engineering Application & Management (IJREAM)– ISSN: 2494-9150 , Volume 02 , Issue :10 , Jan - 2017 ,pp. 25-27.

[7] Ms. Komal Naik & Prof. Varsha Bhosale et. al.,"Generating Honeywords From Real Passwords with Decoy Mechanism " in Journal of
International Journal for Engineering Application & Management (IJREAM)–ISSN:2494- 9150 , Volume 02 , Issue :04 , July -2016 .

[8] Pratik Mongal & Ravindra Suryawanshi et. al. , "Making Honeywords from Actual Passwords with Distraction Mechanism" in Journal of
International Journal of Emerging Technology and Advanced Engineering–ISSN:2250-2459 ,Volume 06 , Issue : 9 , Sept - 2016 ,pp. 178-181.

[9] Gary C. Kessler,"Passwords-Strengths and Weaknesses" in proceesing of Internet and Internetworking Security , J.P. Cavanagh(ed.)
, Anerbach, 1997