© 2018 IJSRST | Volume 4 | Issue 3 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
29th January 2018
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur,
Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

Review on Data Prevention Using Honeywords

Pranav Bhagat[1], Sadia Ameen[1], Sadia Patka[2]

[1]Student, Department of Computer Science and Engineering, Anjuman College of Engineering & Technology, Rashtrasant Tukadoji Maharaj Nagpur University, Maharashtra, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anjuman College of Engineering & Technology, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra, India

ABSTRACT

In today's world , data security is the important for the growth of organizations and to maintain their historical and current data . These data are generally secured or protected using passwords. But what if the passwords get into wrong hands or get cracked? To solve this problem and to prevent data from unauthorized access the idea of Honeywords came into existence .The concept of "Honeywords" is to store multiple decoy passwords with the original password that the user itself has created. Whenever an unauthorized person tries to access the data using the decoy password he/she gets access to decoy files. Honeywords creates ambiguity for the adversary to get to real password and prevents password.

Keywords: Security, Password, Honeypot, Honeyword, Sweetword

I. INTRODUCTION

In this decade of Technology data security is very crucial. Data Breach can compromise the secrecy of any organisation. Also, Passwords are inheritably weak form of authentication. Password breaching has become a common thing in today's world. So to overcome this, scheme of Data Prevention i.e "Honeywords" was proposed. Honeyword concept says that for each user account, the legitimate password is stored with several honeywords in order to sense an unauthorized access to the data.

The idea of Honeywords was derived from the concept of "Honeypot". Now, honeypot is a computer system that is set up to act as a decoy to lure cyber-attackers, and to deflect, detect, or study attempts to gain unauthorized access to information systems. But honeypot introduced risk to the environment and also Finger printing was possible. So, the idea of Honeyword was brought to overcome the disadvantages of honeypot mentioned above.

If honeywords are selected by a cyber-attacker who steals a file of passwords cannot be sure if it is the real password or a honeyword for any account. Moreover, entering a honeyword to login will trigger an alarm notifying the administrator about a password file breach.

Basically, sweetwords are constructed for each legitimate username such that only one of them is the correct password and the others are honeywords (decoy passwords). Hence, when an adversary tries to enter into the system using a honey word, an alert message or alarm is triggered to notify the administration about a password leakage occured.

II. RELATED WORK

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 [1]. But they did not prepare with data prevention as still there was probability that the adversary can get to the real password.

Imran Erguler proposed in his paper Achieving Flatness: Selecting the Honeywords from Existing User Passwords that at the expense of increasing the storage requirement by 20 times, they introduce a simple and effective solution to the detection of password file disclosure events .It suggests an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords a perfectly flat honeyword generation method-and also to reduce storage cost of the honeyword scheme[2].

Ms. Manisha Bhole in her proposed work on Honeywords for Password Security and Management did work on Honeyword Generation method i.e chaffing-with-tweaking and made some improvements such as handling the brute force attack and social engineering attacks and introduce an enhanced model as a solutiom to an open problem that also overcomes the previous drawbacks of honeyword generatio[3].

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 honey-word system directly depends on the generation algorithm, i.e., the generator algorithm determines the chance of distinguishing the correct password out of respective sweetwords [4].

Ms. Komal Naik and Prof. Varsha Bhosale proposed the concept of honeywords in "Generating Honeywords from Real Passwords with Decoy Mechanism". In this mechanism if adversary enters the honeyword for login it will it will trigger an alarm notifying the administrator about a password file breach. If the number of attempts exceeds the count of three or enters the password other than honeyword then the access will be issued but the files available will be decoy files. Thus, decoy mechanism secures the data of the legitimate user. System keeps the data of tracked IP's with them and uses them to take appropriate action against the malicious users [5]. But what if the adversary luckily chooses the original password from the sweetwords, then the data is in wrong hands.

III. DISCUSSION

Reviewing of these existing work results to that, more improvements can be made. So, to carry out the work and to eliminate the previous drawbacks some enhancements like key protection will be added which will act as a two step authentication method to get access to the original data.

IV. FUTURE SCOPE

The Future scope of honeyword concept is very vast. 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 OTP's can be replaced by this system, as it's 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 to protect their valuable documents and mails.
- ✓ Surveillance system can use to keep their data secure from hackers.
- ✓ This System can be used with fingerprint Scanner or Face Recognition can become more secure.

V. CONCLUSION

Security system based on Honeywords addressed a number of faults that need to be handled before successful release of the scheme. In this way, the strength of honeywords will be figured out and used for Data Prevention in this system .There is a huge scope of Honeywords in future as passwords cannot extinct and also they are the base of security & protection.

VI. REFERENCES

[1]. 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.

[2]. 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.

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

[4]. 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.

[5]. 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 .

[6]. 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.

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