Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 2, February 2018, pg.120 – 123

Prevention of Data Using Concept of Honeywords

Mumtaz Parveen[1], Ifra Khan[2], Sadia Patka[3]

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

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

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

[1] mumtaj181296@gmail.com; [2] ifra9321@gmail.com; [3] sadiya.patka13@gmail.com

Abstract*— Data Security plays a pivotal and decisive role in current times. Passwords could be authenticated easily using brute forces. Various other technologies used such as an OTP or code generators require third hand devices. Users authentic password are amalgamated with honeywords and stored as sweet words in an encrypted file within the database. These sweet words even after getting in the hands of an invader bewail him. The proffered system has an additional security authentication i.e. the key validity stage. The intruder when enters password with conjecture then after three attempts he will be directed towards a page showing decoy files and at the same time an alert will be send to the genuine user notifying him about the infringement.

Keywords — honeypot, honeywords, intruder, authentication, security, password

I. INTRODUCTION

Passwords used are often fragile and could be easily guessed by mere speculation of users personal details. Also people tend use the same passwords on multiple sites, thus making them an easy prey to a hacker. In recent times there has been a breach of passwords and almost 1.4 billion passwords were hacked and leaked online .The cumulative database contained simple text testimonial leaked from Bitcoin, Pastbin, LinkedIn MySpace , Netflix, Last.FM, Zoosh, Redbox,etc.This shows how effortless it is to hack passwords and infringe data security. Hence the incentive behind this project is to make data invulnerable by preventing password cracking and at the same time detecting the invader by using Honeywords.

Honeywords create uncertainty for an invader. It confuses him by making him belief that the passwords hacked are real. Honeywords are combined with original passwords and placed together .This combination is known as sweet words. These sweet words when in hand of an adversary won't let him exploit the data as he would not know the genuine.

Honeywords are originated from honeypots .Honeypot is a trap to detect ,deflect an intruder to unauthorized usage of data by creating fake accounts .On the counterpart honeywords are fake passwords used to create ambiguity for an adversary upon its authorization to information system. Honeyword method has various feasible passwords for each account out of which one is true. When an adversary tries to login into the organization with honeywords he will be tracked down by the authorization through the alarm which sets up upon the entry of honeywords or even without using honeywords and just by intruders supposition of passwords.

Honeywords and the absolute passwords are placed within an encrypted file which is per user password. The propound system comprises of a key level authentication to which the user gets access only when he enters the accurate password at the

time of login. If the trespasser gets admit to the login and comes to the key authentication level then here also after three attempts he will get access to decoy files and an alarm will be sent to the faithful user informing him about the contravention.

II. LITERATURE SURVEY

This Section includes the literature review of existing systems with their limitations.

TABLE 1: LITERATURE REVIEW

PAPER NAME	AUTHOR NAME	PROPOSED SYSTEM	DRAWBACKS
Honeywords: Making Password—Cracking Detectable	Ari Juels, Ronald L. R.	This paper Introduced the honeychecker and honey word mechanism. The system provide honeyword generation Method.[1]	This system is not concoct with data thwarting because there is feasibility that the attacker can succeed to original password.
Honeywords For Password Security And Management	Ms. Manisha Bhole	Here, this classification create honeyword i.e. a fake word using a flat generation method. therefore trapping the invader and also not letting the original data to be breached [2].	This methodology does not render alarm warning at the time of data violation.
Achieving Flatness : Selecting Honeywords From Existing User Passwords	Prashant Muthiya, Sachin Padvi, DevendraPatil, Dipak Patil	This system declares a simple idea to insert honeywords with each user accounts [3].	This paper has only admin login and admin is given the sole power to access and control users data.
Generating Honeywords From Real Passwords With Decoy Mechanism	Ms. Komal Naik Prof.Varsha Bhosale	This system state the idea of honeywords being able to discover attacks against hash password databases [4].	This scheme does not have key level authentication as well as encryption of the sweetwords i.e. honeywords with original passwords.

III. PROPOSED SYSTEM

Honeypots are designed to purposely engage and deceive intruder, hackers malicious activities performed over the internet and identify them. Honeypot is an artifice used for luring an adversary into the organisation's system and making it manipulate the susceptibility thereby letting the administrator learn about the deficiencies that need to be revamped (altered). By knowing these weaknesses the organisation could build a more secure system that would possibly be invulnerable to hackers in future.

From sighting 'Honeywords' it can be relate it to sugar coated words, taking "sugar coated" as to make a thing superficially acceptable. Similar is the objective of honeywords in data security. Honeywords creates false identity i.e. fake passwords.

Honeywords in contrary to other technologies does not require any additional devices nor could they be detected by brute force attack. In fact even after getting exploited by an invader it would just make him buoyant with ambiguity.

The proposed system consists of a basic technique for enhancing data security as well as the identification of an intruder into the system. Two aspects taken into consideration are that passwords must be safeguarded by taking appropriate provision and storing with their hash values computed as well as the system should be able to detect whether a password file divulge incident happened. When the user registers into the account, system will check the password eligibility and if it is correct then it will generate honeywords and store them into database as sweet words i.e. original password and honeywords within an encrypted file.

The proposed system has two level security authentications, during registration user will be asked some questions and the answers given to these questions will form a key which will be used at the second level to validate the user to its data only after the user logins into the system with the correct and genuine password. When an intruder tries to login into the system with honeywords he/she will get access to decoy files after three attempts and at the same time an alert notification will be sent to the authorized user of the data that his/her account is being exploited (violated).

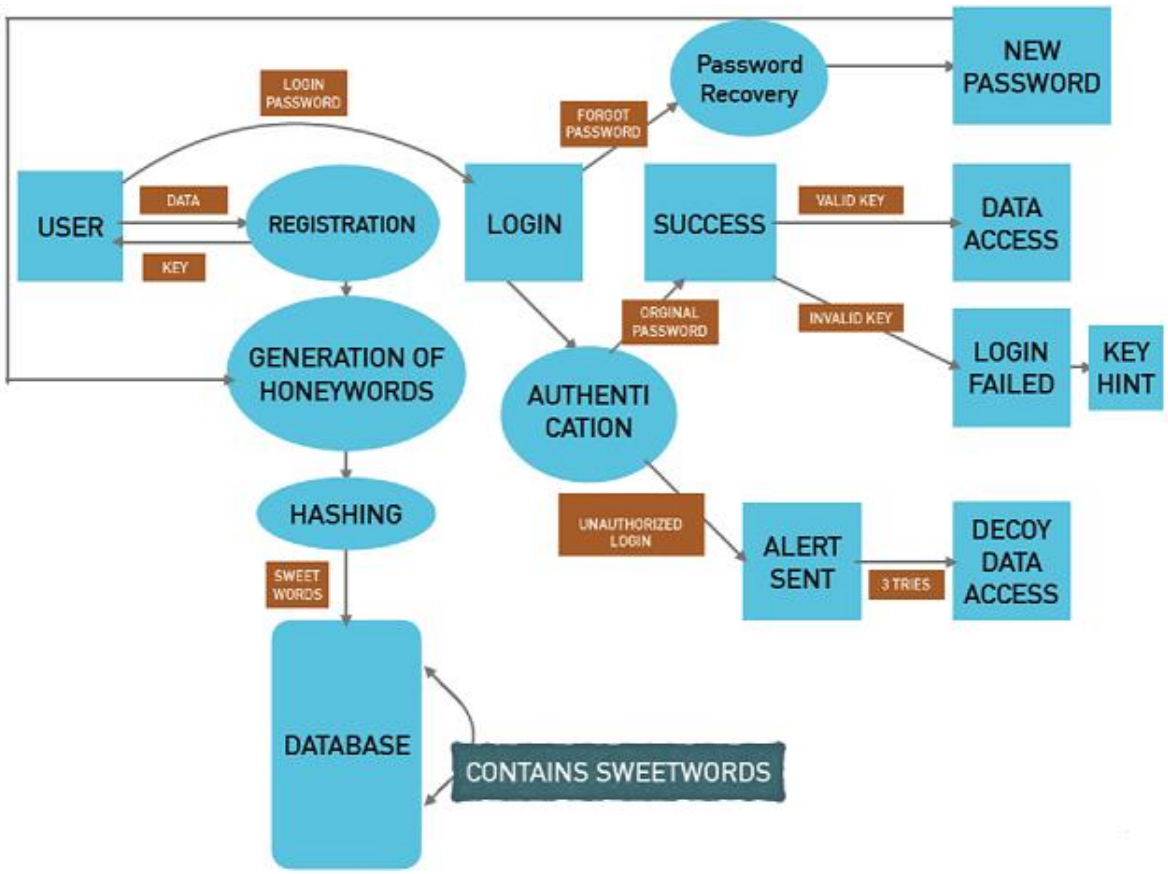

Fig. 1: Proposed System Architecture

IV. 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.

ACKNOWLEDGEMENT

We would like to thank our guide **Prof. Sadia Patka** who guided us throughout this course and we would also like to thank our team members for their co-operation and support.

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, ser. CCS '2013. New York, NY, USA: ACM, 2013, pp. 145–160.

[2] 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 .

[3] 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.

[4] 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 .

[5] F.Cohen, *The Use Of Deception techniques*: Honeypots and Decoy, Handbook of Information Security, vol. 3, pp.646655, 2006.

[6] C.Herley and D. Florencio, Protecting nancial institutions from brute-force attacks, in SEC08, 2008, pp. 681685

[7] K.Brown,"The Danger Of weak Hashes," SANS Institute InfoSec Reading Room, Tech.Rep.2013.

[8] *https://www.techopedia.com/definition/10278/honeypot*

