Rat Trap: Inviting, Detection & Identification of Attacker Using Honey Words In a Purchase Portal

Mahesh khanna R[1] Vaibhav Narayananan V[2] Raj Mohan S[3] Kalai chelvi T[4]
[1,2,3]Student [4]Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Panimalar Institute Of Technology, Chennai-600123

Abstract— Honey words are generated based on the user info provided and the original password is converted into another format and stored along with the Honey words. This project deploy Intermediate server, Shopping server for purchase and Cloud server for maintaining user account details. Attacker who knows the E mail account of original user can easily reset the password of the cloud server. Attacker is invited to do attack in this Project, so as to find him out very easily. Now attacker logins into the purchase portal, where he is been tracked unknowingly & he is allowed to do purchase. Server identifies the attacker and sends the info to the Original owner and also it blocks the attacker even doing transaction from his original account.

Key words: Honeywords, DDOS, Dictionary attack, Brute force attack

I. INTRODUCTION

DISCLOSURE of password files is a severe security problem that has affected millions of users and companies like Yahoo, RockYou, LinkedIn, eHarmony and Adobe, since leaked passwords make the users target of many possible cyber-attacks. In this respect, there are two issues that should be considered to overcome these security problems: First, passwords must be protected by taking appropriate precautions and storing with their hash values computed through salting or some other complex mechanisms.

Hence, for an adversary it must be hard to invert hashes to acquire plaintext passwords. The second point is that a secure system should detect whether a password file disclosure incident happened or not to take appropriate actions. The project focus on the latter issue and deal with fake passwords or accounts as a simple and cost effective solution to detect compromise of passwords. Honey pot is one of the methods to identify occurrence of a password database breach. In this approach, the administrator purposely creates deceit user accounts to lure adversaries and detects a password disclosure, if any one of the honey pot passwords get used.

II. EXISTING SYSTEM

In the EXISTING SYSTEM, system may be vulnerable to DDoS attacks affecting the whole system. The passwords are easily hacked the hacker using online guessing attacks. So there is no big security implementation was introduced in the existing system.

A. Disadvantages:

Security is very low, so that the attacker can easily hack the passwords of the users and can do anything.
Passwords can be hacked using guessing attacks.

III. PROPOSED SYSTEM

In the PROPOSED SYSTEM, we are using Honey words to provide more security for access the application. The user has user id and password while registration process and these also stores set of honey passwords (false passwords) with each user account. Then During the login process, when attacker gets the password list, attacker recovers many password candidates for each account and it cannot be sure about which word is genuine. Hence, the cracked password files can be detected by the server if a login attempts is done with a honey word by the adversary. During the user registration asking user liked questions like games, job, vehicle using, players etc. user name, hash value of original password and added with honey words (generated from user likes) is stored in the database. This link is allowed to steal by attacker. So we can track exact attacker.

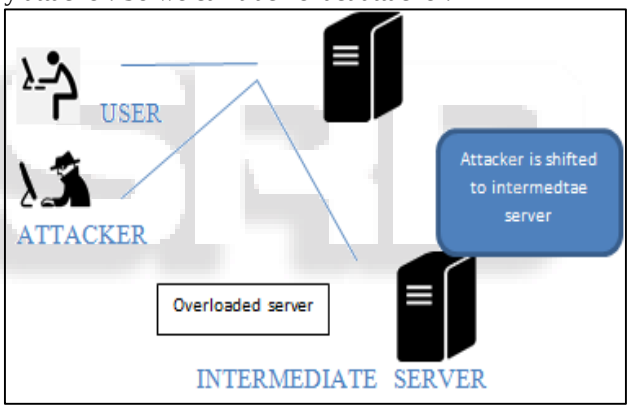

Fig. 1: means that different servers deployed

A. Advantages:

The attackers are not able to guess and hack the passwords.
It provide high security to data owner

IV. ARCHITECTURE DIAGRAM

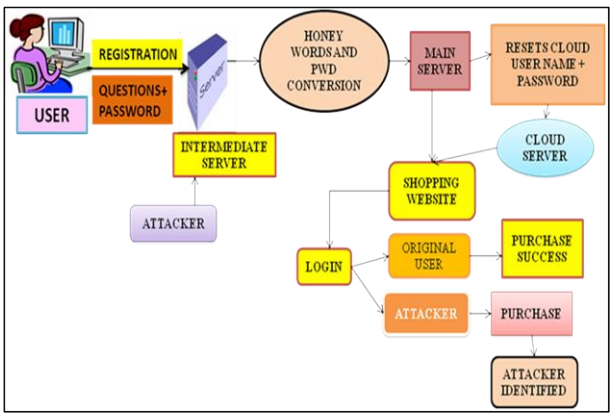

Fig. 2: gives the architecture diagram of our proposed system

V. CONCLUSION

The study have analyzed the security of the honey word system and addressed a number of flaws that need to be handled before successful realization of the scheme. In this respect, the study have pointed out that the strength of the honey word system directly depends on the generation algorithm, i.e., flatness of the generator algorithm determines the chance of distinguishing the correct password out of respective sweetwords. Another point that we would like to stress is that defined reaction policies in case of a honey word entrance can be exploited by an adversary to realize a DoS attack.

REFERENCES

[1] D. Mirante and C. Justin, "Understanding password database compromises," Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, New York, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.
[2] A. Vance, "If your password is 123456, just make it hackme," New York Times, Jan. 2010.
[3] K. Brown, "The dangers of weak hashes," SANS Institute InfoSec Reading Room, Maryland US, pp. 1–22, Nov. 2013, [Online]. whitepapers/authentication/dangers-weak-hashes-34412.
[4] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in Proc. 30th IEEE Symp. Security Privacy, 2009, pp. 391–405.
[5] F. Cohen, "The use of deception techniques: Honeypots and decoys," Handbook Inform. Security, vol. 3, pp. 646–655, 2006.
[6] M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, "Improving security using deception," Center for Education and Research Information Assurance and Security, Purdue Univ., West Lafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013-13, 2013.
[7] C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in Proc. 23rd Int. Inform. Security Conf., 2008, pp. 681–685.
[8] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-resistant password management," in Proc. 15th Eur. Conf. Res. Comput. Security, 2010, pp. 286–302.

