Honey Word Generation to Identify Attacker in Purchase Portal

K. Baby Shalini¹, R. Rakshitha², R. Sharmiladevi³, S. Sarah⁴
B. Tech IT Student¹, ², ³, Assistant Professor⁴
Kingston Engineering College, Vellore, Tamilnadu, India

Abstract:
The System may be vulnerable to DDOS attacks affecting the whole system. The passwords are easily hacked by the hacker using online guessing attacks. So there is no big security implementation in the existing system. Honey words are used to detect Hackers by inducing them for attacking there by DDOS can be avoided. User’s Original password is hashed and stored along with Honey words. Attacker will fetch any one of the password so that intermediate server will filter the wrong password. Honey words are generated based on the user information provided and the original password is converted into another format and stored along with the Honey words. We deploy intermediate server, shopping server for purchase and cloud server for maintaining user account details.

Keywords: Honey words, DDOS, Intermediate server, Cloud server.

I. INTRODUCTION

Disclosure of password files is a severe security problem that has affected millions of user and companies like Yahoo, Rock You, LinkedIn, eHarmony and Adobe, since leaked passwords make users target the many possible cyber attacks. Event demonstrated that the weak password storage methods are currently in place on many web sites. For example, the LinkedIn passwords were using the SHA-1 algorithm without a salt and the passwords in the eHarmony system were also stored using unsalted MD5 hashes. Indeed, once a password file is stolen, it is easy to arrest most of the plaintext passwords. In this deference, there are two issues that should be considered the security problems. First, password must be protected by taking appropriate protection and store with their hash values computed through salting or some other multipart mechanisms. The second point is a secure system whether a password file disclosure incident happened or not to take appropriate actions. In this study, we focus on the latter issue and deal with fake password or account 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, any one of the honey pot passwords get used. This idea has been modified by Herley and Florencio to protect online banking accounts from password brute-force attacks. According to the study, for each user incorrect login attempts with some passwords lead to honey pot accounts, i.e., malicious behavior is recognized. For instance, there are 108 possibilities for a eight-digit password and let system links 10,000 wrong password to honey pot accounts, so the adversary performing the brute force attack 10,000 times more likely to hit a honey pot account than the genuine account.

Use of decoys for building theft-resistant was introduced by Bojinov. In this model, the fake password sets are stored with the real user password set to conceal the real password, by forcing an adversary to carry out a considerable amount of online work before getting the correct information. Recently, Juels and Rivest have presented the honey word mechanism to detect an adversary who attempts to login with cracked passwords. Basically, for each username a set of sweet words is constructed such that only one element is the correct password and the others are honey words (decoy passwords). Hence, when an adversary tries to enter into the system with a honey word, an alarm is triggered to notify the administration about a password leakage. The details of the method will be given in the next section. In this study, we analyze the honey word approach and give some remarks about the security of the system. Furthermore, we point out that the key item for this method is the generation algorithm of the honey word such that indistinguishable from the correct passwords. Therefore, we propose a new approach that use password for other users in the system for honey word sets, i.e., realistic honey words are provided. Moreover, this technique also reduces the storage cost compared with the honey word method.

In this study security properties and demonstrate a comparison between our approach and the original methods. Then overview the methods on generation of honey words given in the study and discuss some points that can cause some security problems. Basically, a simple but clever idea behind the study is the insertion of false passwords called as honey words associated with each user’s account. When an adversary gets the password list, she 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 system administration if a login attempt is done with a honey word by the adversary. We use the notations and definitions depicted into simplify the description of the honey word scheme.
II. ARCHITECTURE DIAGRAM

III. FEATURES OF PROPOSED SYSTEM

1. User Registration
2. Server
3. Honey Word generation
4. Intermediate server deployment & shopping server deployment
5. Password Hacking process
6. Identification of attacker & avoidance of DDOS attacker.

1. USER REGISTRATION

We are going to create a User application by which the user is allowed to access the data from the server. Here first the user wants to create an account and then only they are allowed to access the Network. Once the User creates an account, they are allowed to login into their account to access the application. Based on the User’s request, the Server will respond to the User. All the User details will be stored in the Database of the Server. The bank user details are registered with the fields like username, password, and personal details with some set of questions and answers. These details are saved into the server. After proper registration only the user can allow to login into the server.

Figure 1.1 Architecture of Honey words in Purchase Portal.

Figure 2. User Register the application

2. SERVER

The Server to access the database and web based application. Server will verify the user and generates honey word for save the user password. In case, illegal actions happened means server will generate alert and intimate it to user. The Server will monitor the entire User’s information in their database and verify them if required. Also the Server will store the entire user information in their database. Server has to establish the connection to communicate with the Users. The Server will authenticate each user before they access the application. So that the Server will prevent the Unauthorized User from accessing the Application.

Figure 3. User Stored Server
3. HONEY WORDS GENERATION

Password files have got a lot of security problem that has affected million of users as well as many companies. Password file is generally stored in encrypted format, if a password file is stolen or theft by using the password cracking techniques and decryption technique it is easy to capture most of the plaintext and encrypt passwords. So in this Honey Word Generation will deployed honey word creations. That is the user’s password and registered question are combined and then it will generate a key as unknown Name.

Figure 4. Conversion of Honey word generations

4. INTERMEDIATE SERVER AND SHOPPING SERVER DEPLOYMENT

An intermediate server is a program that handles communications requests to a resource manager program on behalf of a user program. The user program can be referred to as a client of the intermediate server. Here we will generate the Intermediate server to make communication between user and Server. All requests comes from the users are first sent to the intermediate server to verifies the password and user details. Shopping server is used to collect the details from customer and sent to the details to the intermediate server for verification.

Figure 5. Intermediate the server

5. PASSWORD HACKING PROCESS

Hacking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly is to repeatedly try guesses for the password. Another common approach is to say that you have “forgotten” the password and then change it. Password Hacking is blocked in this Process. We modify the users’ original passwords into unknown Name and saved into server.

Figure 6. Attacker hack the Password

6. IDENTIFICATION OF ATTACKERS AND REMOVE DDOS ATTACKS

A distributed denial of service (DDOS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resource, from banks to news website and present a major challenge to making sure people can publish and access important information. If there is anybody trying with wrong password or any illegal action means server will block that action and intimate to the specified Users? If the same request comes from user or means server will blocks that action also. This is done in DDOS attack.

Figure 7. Block the DDOS attacker

IV. PROPOSED SYSTEM:

The proposed systems are using Honey words to provide more security for access the application. The user has 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. The cracked password files can be detected by the server if a login attempts is done with a honey word by the adversary.

ADVANTAGES

- The attackers are not able to guess and hack the passwords.
- It provides high security to data owner.
- The basics of passwords hashing, look at password cracking software and hardware.
• It will develop a novel taxonomy of methods and techniques.

• It is comparatively easy to approximate and directly relevant for security engineering.

V. RELATED WORK

Password strength: The current, state of the art heuristic password cracking algorithm, due to Weir et al., is based on probabilistic, context free grammars. In a recent study, Kelley et al., characterize the vulnerable of user generated password to Weir-style cracking attacks under various password composition policies. One such policy is a common, weak one dubbed “basic8,” in which users are instructed, “Password must have at least 8 characters”. Based on study of published password including one representing 70 million Yahoo! Users, he estimates that a majority of passwords have little more than 20 bits of effective entropy against an optimal attacker. Onneu and Preibuscher offer an excellent survey of current password management practices on popular web sites, including password composition requirements and advice to users, account lockout policies, and update and recovery procedures. Herley and van Oorschot argue that use of passwords will persist for many years, and highlight key research questions on how to create strong passwords and manage them effectively.

Password strengthening: The take a tail method may be viewed as a variant on previously proposed password strengthening schemes. Forget et al., randomly interleave system generated characters into a password. The user may request a reshuffling of these characters until she obtains a password regards as memorable. Houshmand and Aggarwal recently proposed a related system that applies small tweaks to user supplied passwords to preserve memorability while adding strength against cracking, specifically. Various schemes, e.g., password Hash, have also been proposed to strengthen passwords within password managers.

Password storage and verification: There are stronger approaches than honey words for splitting password related secrets across servers. Some proposed and commercialized methods employ distributed cryptography to conceal password fully in the event of a server breach. While such methods are preferable to honey word where practical, they require substantial changes to password verification system and, ideally, client side support as well. Honey words may be seen as a stepping stone to such approaches. Password authenticated key exchange methods, such as the Secure Remote Password Protocol (SRP), provide another approach towards verifying parties without having to trust either party. remote party must have a trusted computer to perform the necessary mathematical operations. If successful, both parties end up with the same secret key, which they may use to encrypt and authenticate further communications.

Decoys: The use of decoy resources to detect security breaches is an age old practice in the intelligence community. Honey words also bear some resemblance to dress code, plausible looking but invalid secrets that users may submit to trigger a silent alarm. A related idea are “colissionful” hash function, these yield hash values with multiple, feasible computed pre-image, thus creating ambiguity as to which pre-image is correct. Mostly closely related to our proposed use of honey words is the Kamouflage system of Bojinov et al. The setting in that work differs from ours, though. Kamouflage aims to protect a user’s list of passwords in a client side password manager against misuse should the user’s device (e.g., laptop to tablet) be stolen or otherwise compromised. Kamouflage conceals the correct password list within a set of decoy lists, which contain honey words created using the scheme. Password consuming servers need not be aware of Kamouflage deployment.

VI. CONCLUSION

In this study, 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, we 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 sweet words. 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. Further, we demonstrated the weak and strong points of each method introduced in the original study. It has been shown that DOS resistance of the chaffing-by-tweaking method is weak and also its flatness can be questioned by regarding Remark. Although some weaknesses of the chaffing-by-tweaking techniques are accepted by their creators, we believe that it should not be considered the alternative method due to its predictable nature and a potential DOS weakness.

VII. REFERENCES


[8]. S.Sarah, Persi Pamela,”Secure Transmission by Employing Multi-Biometric Authentication in Cloud Computing” International journal of rend in Research and...


