Rat Trap: Inviting, Detecting and Identifying the Attacker Using Honey Words in Purchase Portal

T.Sherin

* Department of Computer Science and Engineering, Dr.APJ Abdul Kalam Centre for Research, Adhi College of Engineering And Technology, Sankarapuram - 631605, Tamilnadu, India.
sherin.cse@adhi.edu.in

Abstract

The main objective of this paper is to provide good authentication and identifying the attacker and also avoids DDOS attacks in online purchase portal. In our proposed model, honey words are created when the user register with the server and it generates password based on the user information provided and the original password is converted into another format and stored along with the honey words. Attacker will fetch any one of the password so that intermediate server will filter the wrong password based on the queries so that DDOS can be avoided. We deploy Intermediate server, shopping server for purchase and cloud server for maintaining user account details. Attacker who knows the Email 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 them out easily. Now attacker logins into the purchase portal, where they can be tracked unknowingly and allowed to do purchase. Server identifies the attacker and sends the information to the original owner and also it blocks the attacker even doing transaction from the original account.

Keywords: Authentication, DDOS attack, cloud server.

INTRODUCTION

Cloud computing is a fast-growing technology that has established itself in the next generation of IT industry and business. Cloud computing promises reliable software, hardware, and IAAS delivered over the Internet and remote data centers. Cloud services provides the powerful architecture to perform complex computing tasks and span a range of IT functions from storage and computation to database and application services.

The need to store, process, and analyze large amounts of datasets has driven many organizations and individuals to adopt cloud computing. Most of the scientific applications for extensive experiments are currently deployed in the cloud and it may continue to increase because of the lack of available computing facilities in local servers, reduced capital costs, and increasing volume of data produced and consumed by the experiments.

In the Existing system, honey words (decoy passwords) are used to detect attacks against hashed password databases. For each user account, the legitimate password is stored with several honey words in order to sense impersonation. Honey words are selected properly, a cyber-attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honey words for any account. In the existing system, DOS resistance is weak and expense of increasing the storage requirement. The current system which is used for several mechanisms are used to prevent DDOS attack and provide securities are not sufficient and also the attacker is not identified. Due to this insufficient security the system with good authentication and security policy is required to avoid DDOS attacks and identify the attacker.

The purpose of this system is to provide good authentication and identifying the attacker and also avoids DDOS attacks in online purchase portal. It selects the honey words from existing user passwords in the system in order to provide realistic honey words and also to reduce storage cost of the honey words scheme. We have compared the proposed model with other methods with respect to DOS resistance, flatness, and storage cost and usability properties.

In proposed system there are two servers. One is main server and the other is an intermediate server. Main server is used for authentication while intermediate server is used for transaction. Since more than one servers are used, the load is reduced. DDOS attacks can be removed since the intermediate server filters the incoming requests. The information of user are stored in cloud so that the cost of storage is reduced. It provides Usability and flatness to the user.

LITERATURE SURVEY

Jules and Rivets proposed honey words (decoy passwords) to detect attacks against hashed password databases. For each user account, the legitimate password is stored with several honey words in order to sense impersonation. If honey words are selected properly, an adversary who steals a _le of hashed passwords cannot be sure if it is the real password or a honey word for any account. Entering with a honey word to login will gives an alarm to alert the administrator about a password breach. At the expense of increasing storage requirement by 20 times, the authors introduce a simple and effective solution to detection of password file disclosure events. In this study, we scrutinize the honey word system and present some remarks to highlight possible weak points. Also, we suggest an alternative approach that selects honey words from existing user passwords honey word generation method {and also to reduce storage cost of the honey word scheme.[1]