INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ACCOUNT SECURITY USING TWO LEVEL AUTHENTICATIONS

RAJESHREE N. GAIKWAD, CHARUSHEELA P. PATIL

Department of Information Technology, C. K. Thakur A.C.S. College, New Panvel, India

Accepted Date: 16/08/2014; Published Date: 01/09/2014

Abstract: In this paper we have Account Security concerns with concept of designing a secured account is the most important task in any enterprise or organization development. Securing an account mainly involves applying policies and procedures to protect account from unauthorized access. Servers such as web servers, file servers, mail servers, etc., are the important devices in a network. Each server has various accounts such as admin account, user account, etc. Security for each account is very important. Administrator account is a very important account because information stored in this account is highly confidential and not for public viewing. Therefore, securing these accounts is the first and foremost step followed in every security implementation mechanism. This paper work demonstrates the tasks needed to enhance the account security. Developed a new mechanism for securing the account using two levels of authentication.

Keywords: Account security, Two Level Authentication, Digital Key Generation

Corresponding Author: MS. RAJESHREE N. GAIKWAD

Access Online On:

www.ijpret.com

How to Cite This Article:

Rajshree Gaikwad, Charusheela Patil; IJPRET, 2014; Volume 3 (1): 10-14

PAPER-QR CODE

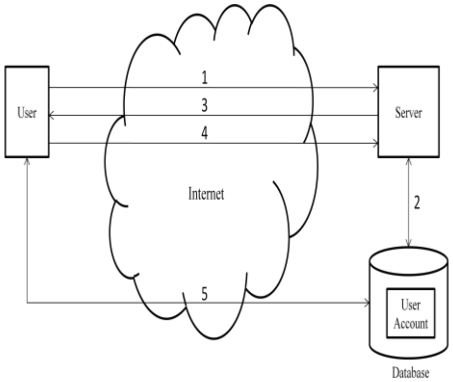
INTRODUCTION

The main feature of the two levels of authentication program implementation is account authentication i.e. verification of account during logon process is done twice. In the traditional logon process includes only username and password where user enter username and password to gain access to his/her account. But this is only one time authentication, that's why become more hack-able. The authentication of person who enter username and password doesn't identified by computer.

The main purpose of two level authentications is to provide more security to an account at a time of logon process. After an user get successfully login to account by entering the correct username and password , a random number called as 'Digital Key' is generated and will be sent to the user through SMS, as they have registered their mobile number during registration time. Then user has to enter that digital key. This username, password and digital key will be sent back to server for authentication. So this gives two level safe login for user and help to provide security to account which will protect account from unwanted hacking attempts.

PROPOSED WORK

Initially if the user is new then first he/she has to do the registration. After the registration, the user will get username and password, and then the user can login successfully. If the user is already registered he/she has its username and password. After entering correct the username and password user get successfully login and they will get the digital key through SMS. Then by entering this key authentication is done. When user get successful login at that time the username get saved as primary key in database. Digital key is random i.e. unique for every time login attempt. Even if one user login to his/her account twice in day then also he/she get unique digital key for every login time. So due to this if hacker knows username and password then also hacker can't gain access to user account.



1. User login with username and password.
2. Server verify user account with this username and password in database.
3. If the login information is right then server send digital key or if login information is wrong then send message to resend correct login information and step 1 and step 2 will repeated.
4. After receiving digital key though SMS user enter that key for second level authentication.
5. If that key match with originally sent key then server provide user access to its user account.

APPLICATIONS

There are various areas where we can deploy this system to prevent unwanted access to systems and for hacking prevention.

1) Many Social Networking Sites: Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe. . While there can be benefits from the collaborative, distributed approaches promoted by responsible use of social networking sites, there are information security and privacy concerns. The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information. The same technologies that invite user participation also make the sites easier to infect with malware that can shut down an organization's networks, or keystroke loggers that can steal credentials. Common social networking risks such as spear phishing social engineering, spoofing, and web application attacks attempt to steal a person's identity. Such attacks are often successful due to the assumption of being in a trusting environment social networks create. So, by using Two Level Authentication accounts will be more secure on social networking sites.

2) E-mail Oriented Sites: Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. The Two Level Authentication will help to provide security to Email Oriented Sites.

3)Centralized Information Storage: Data storage centralization, centralized management, and consolidation are challenges that all companies face in order to store and share data .So by Two Level Authentication Data storage centralization provides safety and gives users the ability to stream and download files provided by network users.

4) Local System Representation on LAN: The easiest way to keep your data and information secure from the outside world is to avoid connecting to the Internet. If everything done inside your intranet is local, the outside world can't see what's going on and can't get to it. In other words, if you aren't connected to the Internet, there is very little chance that anyone can hack into your system. But that means that your intranet is slightly less functional and slightly less valuable. If you can't communicate with the outside world as well as you can with the people inside your network, and if you can't take advantage of the bevy of resources on the Internet, you're not fully taking advantage of technology .The Two Level Authentication will maintain more security.

5) Any Service where Identification of User is Critical: Any service where identification of user is necessary or important at that place we can implement this two level authentication.

CONCLUSION

From the result it is clear that our proposed technique of Two Level Authentication using digital key is better result producing as compared to one time authentication using only username and password. Our method is essentially based on method of generation of random number i.e. digital key and it will take less time even if there is two levels authentication.

FUTURE ENHANCEMENT

For future enhancement of account security we will trying to take image of person who enter username and password and send that image with digital key through SMS so that if any hacker trying to hack account then his/her image will capture and save in database which is useful for identifying that hacker.

REFERENCES

1. Deven N. Shah “Information Security” Wiley-INDIA.

2. Kotadia, Munir. “Microsoft Security guru: Jot down your password”. May 2005.

3. Cameron, Kim. “The Laws of Identity”. May 2005.

4. Brown, Keith. “Security Briefs: A First Look at InfoCard”. April 2006.

5. Theodore Parker.”Security Concepts”

6. Chris McNab .”Network Security Assessment, 2nd Edition.”