Implementation of Secure Authentication Scheme for Mobile Device

Priti Jadhao, Lalit Dole

Abstract – Authentication is a fundamental aspect of system security. It confirms the identity of any user trying to log on to a domain or access network resources. Due to the numerous advantages of authentication systems, it can be used in various applications. The common application involving authentication is, a computer program using a blind credential to authenticate to another program, Using a confirmation E-mail to verify ownership of an e-mail address, using an internet banking system, Withdrawing cash from an ATM .The main purpose of these systems is to validate the user's right to access the system and information, and protect against identity theft and fraud.

Keywords – Image Processing, Watermarking Techniques, Walsh code, DCT (Discrete Cosine Transform).

I. INTRODUCTION

Passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. The main aim for using passwords is to restrict unauthorized users to access the system. Passwords are necessary but, still they are not considered much safe to provide the security to the users because of many flaws in the conventional password systems[1]. A large number of attacks on many systems are related to the passwords. This paper describes password attacks and Implementation of password authentication scheme.

II. TECHIQUES

In this Paper, introducing new techniques of password authentication using image water mark technique and Walsh code. Image processing is any form of signal processing for which the input is an image, the output of image processing can be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it.
Watermark Adding a visible watermark it is a common way of identifying images and protecting them from unauthorized use online. Watermarking technology plays an important role in preventing copyright as it allows to place an perceptible. Watermark depending on the requirement in the multimedia data to identify the legitimate owner or detect malicious tampering of the document. A watermark is an invisible mark placed on an image that is designed to identify both the source of an image as well as its intended recipient. Watermark techniques are used for Proof of Ownership (copyrights and IP protection) , Copying Prevention, Broadcast Monitoring and Authentication.

Manuscript received on June 2013.
Priti Jadhao, CSE DEPT, G.H.Raisoni college of engg., Nagpur, India.
Lalit Dole, CSE DEPT, G.H.Raisoni college of engg., Nagpur, India.

The significant portions of the host image, e.g. the low frequency components have to be modified in order to encode the information in reliable and robust way[2].
A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from loss compression of audio and images to spectral methods for the numerical solution of partial differential equations on, it turns out that cosine functions are much more efficient. Many image transforms have been considered like DCT (Discrete Cosine Transform)[2]. DCTs are also widely employed in solving partial differential equations by spectral methods.

III. DESIGN AND IMPLEMENTATION

In this we proposed authentication scheme in which we made three phases for user to go though three phases and makes secure their data from the attackers. These three phases are interconnected to each other[5][6].

- **Phase I – Registration Form**
- **Phase II – Generation of Password**
- **Phase II – Login Form**

A. Phase I - Registration Phase :

In this design form, first go through Registration Phase here new user register fill all the details which are given in registration for like first name , middle name , last name , birth date ,login id ,city, state ,country ,pin code ,email address , mobile no. , gender, question and select any image from the given images. As shown below

FIGURE 1 : MAIN PAGE OF WEBSECURITY

Click on button Sign Up for the new user

FIGURE 2 : REGISTRATION PAGE

After this fill all the details which are given in registration form and fill it carefully.

B. Phase II – Password Generation :

As first phase is completed then the WebSecurity Scheme generates a unique password of six digit. As shown below

FIGURE 3 : PASSWORD GENERATION

C. Phase III – Login

As we are login to our WebSecurity Account have to go through the login phase where we placed three steps to complete that login process.

FIGURE 4 : ANDROID EMULATOR

Step 1 : Enter your login id then click on the button Login. As shown below

FIGURE 5 : LOGIN PAGE

Step 2 : After entering login id we are going to next step is answer the question which is user is given at the time of registration

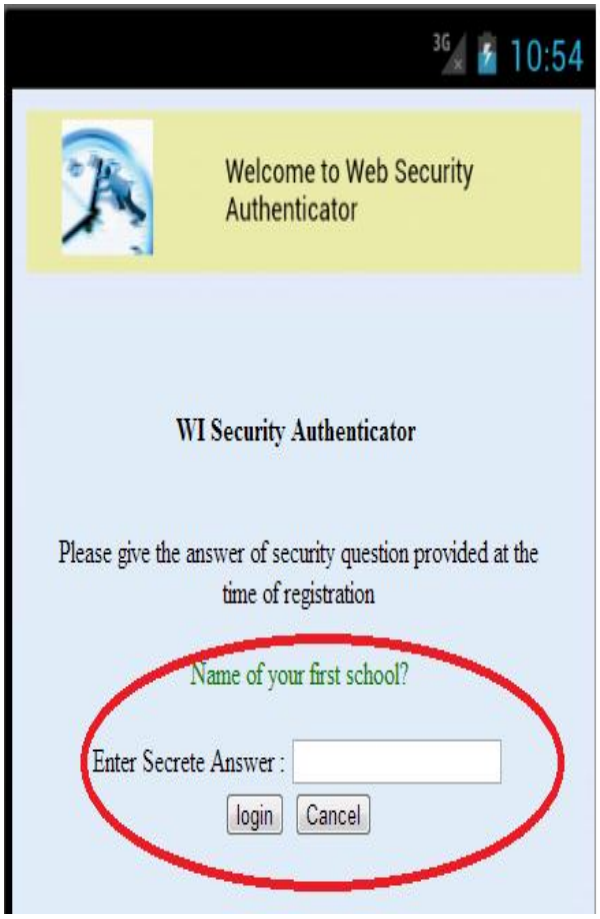

FIGURE 6 : PASSWORD LEVEL ONE- ANSWER OF QUESTION

Step 3: After giving question answer and give correct answer the next is our is displayed image is correct then enter your password and get entry in your account.

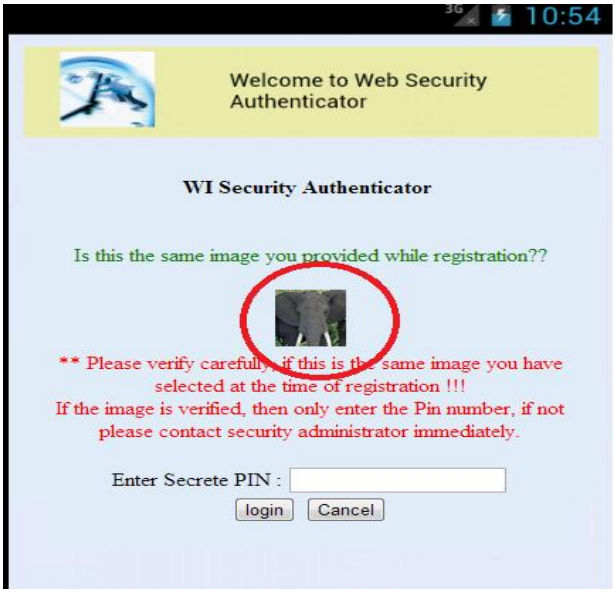

FIGURE 7 : MAIN PASSWORD PAGE

After entering pin click on login button and go to WebSecurity Account.

FIGURE 8 :WEBSECURITY ACCOUNT

IV. CONCLUSION

In this paper discuss about the generation a new authentication password that is totally different from the other password scheme .Authentication password scheme uses for the security purpose. As Authentication scheme generate password which able to defend the attacks like brute force attack, shoulder surfing attack etc. In this Authentication scheme we gave five things which is never be same for any user is login id, security question, security answer, selected image , pin ie password these things are never be same for any user. By this we can make our data secure .It make secure to user from fake site.

REFERENCES

1. Fermi National Accelerator Laboratory, Office of Science / U.S Department of Energy: Strong Authentication at Fermilab, Sept 2006
2. Bin Hu, Qi Xie, Yang Li- Automatic verification of password based authentication protocols using smart card (2011).
3. W. E. Burr, D. F. Dodson, W. T. Polk. Electronic Authentication Guideline. Technical Report 800-63, National Institute of Standards and Technology,2008
4. .<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.
5. CA.Managing strong Authentication: A Guide to Creating an Effective Management System, 2007.
6. Fadi Aloul, Syed Zahidi and Wassim El-Hajj “Two factor authentication using mobile phones” in Pro 2009 IEEE/ACS International Conference on Computer Systems and Applications, ISBN: 978-1-4244-3807-5.
7. [6] Do van Thanh; Jorstad, I Jonvik, T, Do van Thuan “Strong authentication with mobile phone as security token” in Pro Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on.
8. Pernilla Stolpe Johansson “Economic aspects of web authentication” in Project Report for Information Security Course Linköping University, Sweden. In 2011.