Protected Utilizable Verification Using Strong Pass text Passwords

G. Haripriya[1], J.S. Ananda Kumar[2]

[1] *Student, Dept. of MCA, KMM Institute of Post Graduate Studies*

[2] *Assistant Professor, Dept. of MCA, KMM Institute of Post Graduate Studies, Tirupati, A.P*

Abstract- **Traditional character set passwords used for remote user authentication doesn't provide usability and security. To improve usability and security Graphical passwords were projected as an alternative to these textual passwords. This paper proposes a remote user authentication scheme that extends the present pass text scheme. The usability and security of the projected scheme is analyzed using Morea tool the Usability of the proposed scheme is investigated.**

Index Terms- **Authentication, Graphical passwords, Pass Text passwords, Usability.**

I. INTRODUCTION

As pc security plays a significant role in our everyday life, it's necessary to demonstrate users to different systems to avoid unauthorized access. In general, the alphabetical passwords and PINs are used for remote user authentication to access the remote services. These matter passwords may be either

1. Sturdy passwords: Difficult to recollect
2. Weak passwords: simple to recollect

Users tend to choose weak passwords, which may be remembered simply and simple to use for authentication. But these passwords are vulnerable to estimate, dictionary and brute-force search attacks. so as to boost the security of those passwords, users are instructed to use Sturdy passwords that are hard to recollect and hard to crack them with machine-driven tools. Alphanumerical passwords are unprotected to various attacks. To beat the disadvantages of classical or alpha-numerical passwords, there exists a wealth of different authentication mechanisms. This section offers the short summary of those Authentication techniques.

A. AUTHENTICATION TECHNIQUES

These techniques are classified into three sorts supported the following characteristics of the user:

i. Location of the user
ii. Owning of the user
iii. User's information

i. Location of the user

Location of the user is that the mechanism to search out the location of the user at a rapid. GeoBio indicator and phone call verification are the techniques to spot the Location of the user. However these two techniques are accustomed get the geographic location of the user however not the user.

ii. Owning of the user

This is a biometric approach during which user is authenticated by exploitation bio-password and pass thoughts mechanisms. The Bio-password is nothing however user's iris scan, face, voice, tokens like smartcards and fingerprints can be taken as Arcanum for this classification. Pass thoughts technique is planned by, in which user is authenticated through the behavior of the user. User is rejected to access the system resources once he shows suspected behavior. These 2 mechanisms require special hardware and extremely costly to put in and maintain.

iii. User's Information

This mechanism is further divided into matter and graphical Arcanum system. Textual passwords: Textual Arcanum approach is once more divided into 3 types that are,

- Syntactical
- Semantic
- One-time passwords

II. ALGORITHM

A. STURDY PASSTEXT PASSWORD FOR REMOTE USER AUTHENTICATION

A secure usable user authentication method by obtaining a strong pass text password from the text file which is chosen by the user is proposed in this section. In this proposed scheme, the user registers himself with the system with a user id and selecting a file from among several files stored in the database and few changes are made to the document, and then the user selects an index number. The indexed value letters in the words of modified document is concatenated to form the password which is hashed and stored at the server. As the user makes the change to the retrieved text file and also it is combined with selecting the characters in the index valued letters in each word of the modified text the password becomes very strong, but the user has to remember only the changes he made to the text file and the index position. Guessing of the password also becomes difficult as the attacker has to learn both the changes made to the text file and the position and he will not be able to retrieve the password directly as it is random in nature (concatenation of index numbered letters of the words). Thus usability and security of the system is enhanced with this proposed scheme. This scheme has been extended to provide authentication between the client and the server.

The notations used in this paper are as follows:

U: The user.

ID: The user Identification.

S: Server system.

PW: The password of user U.

h (.): A one way hash functions.

E(y, x): encryption of y with key x

D(y, x): decryption of y with key x.

B. TYPES OF REMOTE USER AUTHENTICATION

1. Registration phase:

This phase is executed only once at the time of registration. The steps involved in registration phase are:

Step 1. User chooses a user id.

Step 2. User selects one of the files among multiple files from the server or their own text file. User is presented with the .txt file and needs to change the document like add the text, delete or replace the words in the selected file. Then the user selects an index number to create unique strong pass text password by combining the index numbered character in each line of the modified document.

Step 3. The original document will be saved in the server in a CLOB format for future purpose and the strong pass text password is hashed and stored in the database at the server against the user id.

2. Authentication phase:

This phase involves two sub phases: Login Phase and the verification phase and will be executed every time a user wants to login to the server.

a. Login Phase:

Step 1. User enters the user id and sends to the Remote System.

Step 2. System sends the associated text file according to the user ID and a random challenge (nonce) x.

Step 3. User needs to do the same modifications to the file as done in the registration process.

Step 4. User needs to enter the index value to obtain random unique strong Pass Text password (pw) from text file by concatenating the indexed numbered character in each line of the modified text.

Step 5. User encrypts the password (pw) with the random number x and sends it to the Remote System.

b. Verification Phase:

Step 1. System decrypts the encrypted password by random number x.

Step 2. Now, the decrypted Pass Text password is hashed, compared with the password hash stored against the user id in the database and if it is matches the user is successfully authenticated to the system.

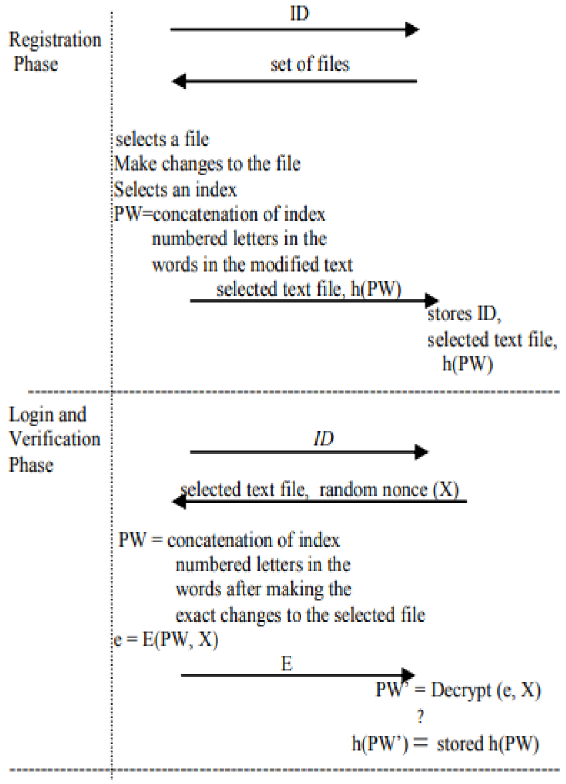
3. Password change phase:

Users have the freedom to change his or her password as follows:

Step 1. User should prove himself or herself as authorized user as similar to login phase. Step 2.

Now, an authenticated user can change pass text password same as in the registration process.

Step 3. The original document in CLOB format and strong pass text password is hashed and stored in the database for future login.


Registration Phase
ID
set of files
selects a file
Make changes to the file
Selects an index
PW=concatenation of index numbered letters in the words in the modified text
selected text file, h(PW)
stores ID, selected text file, h(PW)
Login and Verification Phase
ID
selected text file, random nonce (X)
PW = concatenation of index numbered letters in the words after making the exact changes to the selected file
e = E(PW, X)
E
PW' = Decrypt (e, X)
h(PW') ?= stored h(PW)

III. CONCLUSION

This project is easy to learn, the proposed scheme defends varied security attacks such as approximation attacks, shoulder aquatics attack, replay attack etc. The usability of the planned scheme is Analyzed exploitation Morea tool and it's been found that the average System Usability score is seventy. The proposed system has the advantage that the user needn't to store the file utilized in generating the password, as it is maintained by the server, reduce the memory requirements at the user's aspect.

REFERENCES

[1] R. Dhamija and A. Perrig, Deja Vu: A User Study. Using Images for Authentication, Proceedings of the 9th USENIX Security Symposium, Denver, Colorado, August 2000.

[2] N. I. G. T. Force., Player id, age verification and border control technology forum. Available at: http://www.nevadaigtf.org/TechnologyForum.html, Retrieved October 23, 2005.

[3] D. Weinshall and S. Kirkpatrick, Passwords you'll never forget, but can'trecall,Availableat: http://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf, Retrieved October 24, 2005.

[4] The complete reference VB .Net , Third Edition, Tata McGraw-Hill Edition 2006, by Naughton Schildt.

[5] F.S. Lane, "The naked employee: How technology is Compromising workplace privacy" AMACOM Div American Mgmt. Assn.,2003, pp.128-130.

[6] L. Valeri "Screen Recording System For Windows Desktop" Russian-Korean International Symposium Science and Technology conf., 2004, pp.107-109

[7] M Agarwal , M Mehra "Secure Authentication using Dynamic Virtual Keyboard Layout" ICWET – TCET, Mumbai, India, 201