CHANGE IN METHODOLOGY OF PASSWORD SECURITY OVER NETWORK BEYOND ALPHABETS, NUMBERS AND SPECIAL CHARACTERS

Pradeep Peter[1], Mr Manu Bhaijha[2]
[1]M.Tech, [2]Asst Prof, UCER Allahabad.

Abstract: In password security over the network we traditionally use the alpha numeric password all over the internet as security. Here the methodology used for security enhancement over the internet will be some graphical password, bio-matrix, colour combinations as a user authentication over the internet. As we have the traditional approach using the alphabets, numbers and some special characters over the password generation. Now a days it is very easy to crack the combinations of 26 alphabets, 0 to 9 number combinations used with some special characters.

I. INTRODUCTION

Password protection is very essential now a day over every electronic data over internet. The scheme used is usually of some alphabets, numbers & special characters. As technology changing we need to enhance the methodology over the password generation which would be using some human activity such that every human nature differs from each other as all the humans have different DNA in their body. Using this phenomenon we can increase complexity over password creation using human behaviour and activity and thinking individually.

These are the following schemes which all are related to human activities thinking and behaviour so that every individual would be selecting their password combination beyond these alphabets numbers & special symbols.

- Images(Graphics)
- Bio-Matrix(Individual Identity)
- Human brain choice(human thinking)

Using this we can break the boundaries of simple combinations. There would be a new contribution of human activity to access the user personal, private, important, confidential information over internet.

II. OBJECTIVE

The objective of this paper is enhancing the security of user password protection over the internet sites using the three layered technology of password authentication. Using the Image (graphical) combination, Bio-matrix, colour combinations associated with the User Identification Name. Here the motive is to break the boundaries of 26 alphabets (A-Z), number combinations i.e. (0-9) & special symbols i.e. (~!@#$%^&*_+-`). Now using this layered combination the user will be much secured and according to the situation and changing technology the complexity will be razed many times over the authenticating the genuine user.

III. METHODOLOGY

Over thousands of sites we need to login and we have to make account so we try to make some common user identification and some similar passwords such that a human mind could remember all the time when needed else we just make different account and write those user identification and password and make a note of it and keep in somewhere so it again increase the risk of attack over your personal information. To reduce it we will implement this methodology types such that a user brain involved not just with the remembrance but with some activities to get authenticated.

1. Images(Graphics)

In image methodology we have User Identification name as they create as per own choice then for selecting password the user has to upload some combinations of images that individual user want to make the password. After user selection of images these images are merged with some other images over a matrix of images. Every time when the user enters there User Identification name and click on enter password then a matrix of active images comes over the screen which will be having the user selected images. When the user selects all the correct images then the user will be moved towards the next level of authentication. This method could be implemented over the mat lab such that some random images and the images related to the user identification could be shuffled properly so that the positions of the image randomly changes every time this would be helping the user to get secured from the shoulder suffering attack.

2. Bio-Matrix(Individual Identity)

In this scheme the user has to use Bio matrix hardware devices for entering the thumb impression. It would be the unique identification of the user and this couldn’t be communicated. This kind of authentication always needs the user thumb to access every time. Here in all over the internet sites user’s thumb impression would be uploaded and using technology of computer science these user thumb impression would be matched and only when the user created thumb impression get matched the user will be allowed to access into the account. Here the methodology used for the bio matrix would be at the time of registering the user account the user will be asked to upload the thumb impression that would be used to verify the thumb impression at the time of login of user. Using this technology over the internet as password will help the user to be secured as much better as user was before. Again this bio matrix methodology over the internet will involve the human physical identity that no one can copy and provide without the help of user. Bio matrix hardware is now a day are there and those devices which are not having are modifying these hardware so designing this concept over the internet for cloud storage, social networking and all important human accounts over internet would be secured.

3. Human brain choice (human thinking)

Human brain choice is a concept that will use the human memory again. Here the user gets the frame of colour combinations in sequence. When any user comes over the third security level the user is generating colour combinations in sequence for authentication. By mode of selecting colour boxes is same pattern that the user has selected at the time of registration this kind of password. This methodology can be used for authentication over internet as third layer of security such that the user any kind of account will me much secure then alphabet, numbers and some special characters.

IV. CONCLUSION

In password generation the user has some things related to their daily life. It's easy to keep in mind all the time and physical presence needed to grant access over the internet. Apart from that we would be breaking the boundaries of password generation. Yes, it will be much complex and time taking but when the matter comes over the business money security time and complexity can be considered. Technology is changing according to that traditional things are easy to hack and attack. So we need to move one step ahead so that the security over the internet remains protected.

REFERENCES

[1] G. Agarwal, S. Singh and R.S. Shukla Security Analysis of Graphical Passwords over the Alphanumeric Passwords Int. J. Pure Appl. Sci. Technol., 1(2) (2010), pp. 60-66.

[2] Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan, Graphical Passwords Qualitative Spatial Relations.

[3] Susan Wiedenbeck Jim Waters, Jean Camille birget, Alex Brodskiy, Nasirm Memon Authentication Using Graphical Passwords: Basic Results.

[4] Bandawane Reshma B., Gangadhar Mahesh M. Kumbhar Dnyaneshwar B., Data Security Using Graphical Password and AES Algorithm for E-mail system IJEDR1401200 International Journal of Engineering Development and Research (www.ijedr.org).

[5] Jake Spitzer, Cal Singh, and Dino Schweitzer A SECURITY CLASS PROJECT IN GRAPHICAL PASSWORDS.

[6] Owen, G. S., Suo, X., and Zhu, Y., Graphical passwords: a survey, Proceedings of the 21st Annual Computer Security Applications, IEEE, 463-472, 2005

[7] Reducing Shoulder-Surfing by Using Gaze-based Password Entry Author(s): Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd.

[8] Susan Wiedenbeck, Jean-Camille Birget "Authentication Using Graphical Passwords: Basic Results" Computer Science Department Polytechnic University.

[9] Data Security and Privacy in Cloud Computing Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu International Journal of Distributed Sensor Networks Volume 2014 (2014), ArticleID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903.