Integration of audio in image password protection system

G.SANGEETHA
Department of Computer Science and Engineering
Prist University, Puducherry

J.R.THRESPHINE
Department of Computer Science and Engineering
Prist University, Puducherry

Abstract — **Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.**

Keywords—**Authentication, graphical passwords, usable security**

I. INTRODUCTION

In this project, the authentication or security is provided by means of the image processing. Here the users are registered and their passwords are generated with the help of axis co-ordination in the picture. The values of x and y axis are combined to generate a password for the user. If the user forgets his axis (password) another option of sound file is given for recalling the password. The matching process is done with the help of the Hash Visualization Algorithm.

Passwords are used for –

(a) Authentication (Establishes that the user is who they say they are).

(b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and

(c) Access Control (Restriction of access-includes authentication & authorization).

Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Numbers of graphical password systems have been developed; Study shows that a text-based password suffers with both security and usability problems. According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords .It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods

II. BACKGROUND

Text passwords are the most popular user authentication method, but have security and usability problems. Graphical passwords offer another alternative, and are the focus of this paper.

2.1 Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere .Of interest herein are cued-recall click-based graphical passwords. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include Pass Points and Cued Click- Points (CCP)

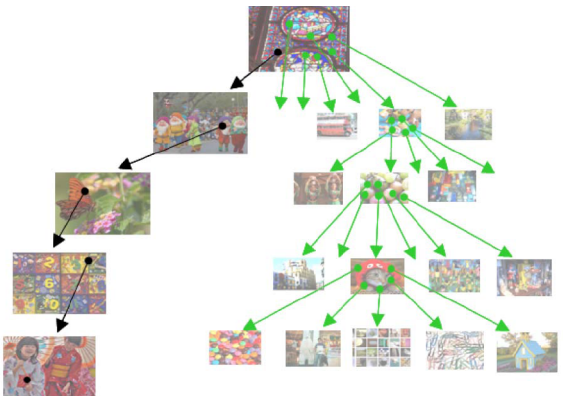

Fig.1. A user navigates through images to form a CCP password. Each click determines the next image.

In Pass Points, passwords consist of a sequence of five click- points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although Pass Points is relatively

usable, security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess Pass Points passwords. Users also tend to select their click-points in predictable patterns (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against Pass Points based on image processing techniques and spatial patterns are a threat.

III. PERSUASIVE CUED CLICK POINTS

Previous work (see above) showed that hotspots and patterns reduce the security of click-based graphical passwords, as attackers can use skewed password distributions to predict and prioritize higher probability passwords for more successful guessing attacks. By adding a persuasive feature to CCP, PCCP encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport (see Fig. 2). The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. The viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like Pass Points and CCP.

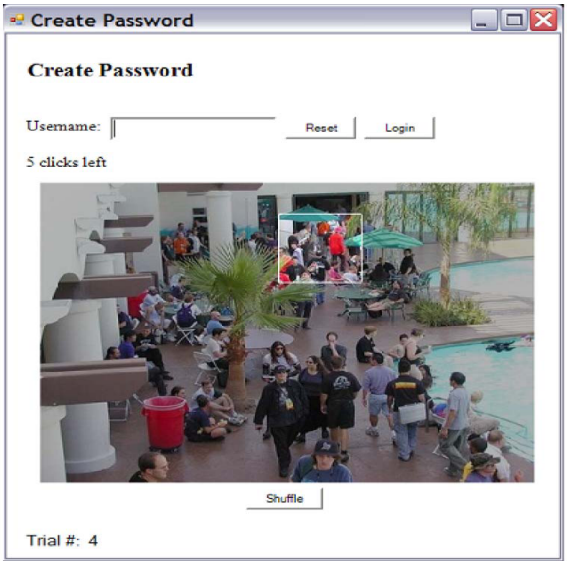

Fig. 2. PCCP Create Password interface. The viewport highlights part of the image.

IV. HASH VISUALIZATION ALGORITHMS

A hash function is a function h which has, as a minimum, the following two properties:

1. Compression: h maps an input x of arbitrary finite length, to an output h(x) of fixed bit length n.
2. Ease of computation: given h and an input x, h(x) is easy to compute.

Three most desired properties:

1. Pre image resistance: for any pre-specified output y, it is computationally infeasible to find the input x such that h(x) = y.
2. 2nd-preimage resistance: given any input x, it is computationally infeasible to find an input x' such that h(x') = h(x).
3. Collision resistance: it is computationally infeasible to find any two distinct inputs x; x' which hash to the same output, h(x) = h(x').

A one-way hash function is a hash function h with two additional properties: pre-image resistance and 2nd-preimage resistance. A collision resistant hash function is a hash function h with the additional property of collision resistance [3].

4.1 Requirements for hash visualization Algorithms.

A hash visualization algorithm(HVA) is a function hI which has, as a minimum, the following two

Properties

1. Image-generation: hI maps an input x of arbitrary finite length, to an output image hI(x) of fixed size.
2. Ease of computation: given h and an input x, hI(x) is easy to compute.

S.No	Login ID	Actual Point	Login Point	Accept	Reject
1	U1	I_1	(x_1,y_1)	YES	NO
2	U2	I_2	(x_2,y_2)	YES	NO
3	U3	I_3	(x_2,y_2)	YES	NO
4	U4	I_4	(x_2,y_2)	YES	NO
5	U5	I_5	(x_2,y_2)	YES	NO

Table 1 : Attempts by Authenticated users

V. CONCLUDING REMARKS

The "Integration of audio in image password protection system" has been successfully developed and implemented with a high degree of awareness and competence with the environment.

The system was tested for a range of inputs and found to be error free. User with minimum computer awareness can easily operate this system, as the system is user friendly and menu driven. The forms have a very high technology of handling the records in the database.

The overall objective of efficiency and maintenance has been achieved particularly. All the information regarding this system have been documented and east to modify with less effort.

REFERENCES

[1] User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.

[2] Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.

[3] Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.

[4] Data Communications and Networking, by Behrouz A Forouzan.

[5] Computer Networking: A Top-Down Approach, by James F. Kurose.

[6] Baeza-Yates and B.Ribeiro_Neto, Modern information retrivel.Addison Wesley, 1999.

[7] R.M. Colomb, Information Spaces: The Architecture of Cyberspace. Springer, 2002.

[8] A. Doan, J. Madhavan, P. Domingos, and A. Halevy, "Learning to Map between Ontologies on the Semantic Web," Proc. 11th Int'l Conf. World Wide Web (WWW '02), pp. 662-673, 2002.

[9] Z. Cai, D.S. McNamara, M. Louwerse, X. Hu, M. Rowe, and A.C. Graesser, "NLS: A Non-Latent Similarity Algorithm," Proc. 26th Ann. Meeting of the Cognitive Science Soc. (CogSci '04), pp. 180-185, 2004.

[10] L.M. Chan, Library of Congress Subject Headings: Principle and Application. Libraries Unlimited, 2005.

[11] E. Frank and G.W. Paynter, "Predicting Library of Congress Classifications from Library of Congress Subject Headings," J. Am Soc. Information Science and Technology, vol. 55, no. 3, pp. 214-227,2004.

[12] R. Gligorov, W. ten Kate, Z. Aleksovski, and F. van Harmelen, "Using Google Distance to Weight Approximate Ontology Matches," Proc. 16th Int'l Conf. World Wide Web (WWW '07), pp. 767-776, 2007.

