icAuth: Image Color Based Authentication System

Pramod Verma
Johns Hopkins University
Baltimore MD, 21218
pramod@cs.jhu.edu

ABSTRACT
Authentication interfaces are GUIs that provide the protection for an application or system. In this paper, we present icAuth: a novel image and color based authentication interface for the authentication process. We enhance the existing Image Based Authentication (IBA) with an additional interactive method. In our approach, the user not only chooses image(s) as a key during the registration process, but also clicks on various regions on the image to generate an additional key. This additional key is in the form of a sequence of colors that correspond to the clicked areas. In essence, the user chooses a color sequence along with the selected images. During the next authentication process, the user has to produce the same color sequence on the recognized images. The user is required to remember the same switching sequence among the images, without having to memorize the precise location of the initial clicks during setup.

Author Keywords
IBA, Security, Usability

ACM Classification Keywords
H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

INTRODUCTION
Image Based Authentication (IBA) is more usable than Text Based Authentication (TBA)[1]. In a basic IBA, during the registration process, the user has to choose images from a given set of images and recognize them during the authentication process[2]. Researchers also experimented to select and recognize objects or patterns in the given image for the authentication process. We extend the basic IBA process by using an interactive approach described in next section.

ARCHITECTURE
icAuth system needs a pointing device to click or some kind of interactive technique such as a touch screen to click or touch the images. The system has two components: Client and Server. Client gets user credentials and the server does authentication based on authentication protocol described below.

Protocol: During the registration process, the user first chooses images as a key. Then user produces an additional key by clicking on the image regions. The user can switch to any image during the clicking process, but needs to memorize both the color sequence and switching sequence. The key is a sequence of colors related to the clicked areas of the respective images. Colors are sampled to a few levels to reduce complexity. During the authentication process the user has to reproduce the key. To make it more usable, in a given image, the user is not required to click on the exact locations to generate the desired color sequence. The protocol described here is a generalized version that can be customized according to one's requirements.
GRAPHICAL USER-INTERFACE
GUI for icAuth has two interfaces. First GUI helps the user to register a color key. The user selects images and generates a key. To assist the user, we display the key sequence underneath the key-image. In the second GUI on the Client side, the user enters a token or user name and submits the request. Afterwards, the Server sends sets of images back to Client GUI. The user then selects appropriate images and generates the color key sequence to complete the authentication.

IMPLEMENTATION
We implemented the icAuth system for the authentication of a website using aforementioned protocol and GUIs. Interfaces were built using PHP and AJAX on the Apache2 web server.

We also implemented the icAuth system on an iPhone4G handheld device. The login page contains an image(s) on which user has to produce a key-color sequence for a successful authentication. Most of these handheld devices have touch screen capabilities, where it may be easier to generate key sequences by tapping than by typing using a virtual keyboard.

To address the precision and fuzziness of colors matching we set following equation.

\[ \alpha \leq \frac{\hat{c}_1 \cdot \hat{c}_2}{\|\hat{c}_1\| \|\hat{c}_2\|} = \cos \theta \leq 1 \]

(1)

Where \( \hat{c}_1 \) and \( \hat{c}_2 \) are two color vectors with \( c_i [R_i, G_i, B_i, I_i] \) and they are treated the same if their dot product (or cosine similarity) is greater than or equals to a predefined threshold \( \alpha \) such as 0.99. \( \hat{c}_1 \) and \( \hat{c}_2 \) can be estimated by averaging the color vectors or pixels values of clicked areas with a small radius \( r \).

DISCUSSION
Our approach is easy to implement and adds an additional layer of security in IBA. The system can be used at various places where small PIN like identification is required via keyboard entry on handheld devices, where a user frequently enters the passcode to unlock the device. For example, Google’s Android uses a pattern based authentication interface.

One another advantage of the icAuth system is that it creates an associating memory in the user’s brain regarding the password. For instance, in Figure 3, the password can be easily remembered by viewing objects such as red leaves, green grass, blue sky, etc.

It has similar drawbacks as IBA, such as brute force attack. However, it can be used with combination of other robust methods. In addition, the system has a limitation that users with color blindness are unable to use the icAuth system. Furthermore, sometimes users may have trouble distinguishing precise colors in specific light conditions. But, we can choose appropriate images to overcome these issues.

icAuth relies not only on a sequence of different regions in one image but on a sequence of different colors in a sequence of images; therefore, the system would utilize images that can be fully or partially segmented into few sections of colors.

CONCLUSION AND FUTURE WORK
We present a novel idea for image and color based authentication. Future work may involve designing and performing a detailed user study comparing authentication methods using desktop and handheld interfaces.

REFERENCES