IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 39-46
www.iosrjournals.org

Implementation of Knowledge Based Authentication System Using Persuasive Cued Click Points

Devi Srinivas[1], M.L.Prasanthi[2]
[1](M.Tech, Computer Science and Engineering, Vardhaman College of Engineering/ JNTU Hyderabad, India)
[2](Associate Professor, Computer Science and Engineering, Vardhaman College of Engineering/ JNTU Hyderabad, India)

Abstract : *In this project, a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.*
Keywords *- Security, Graphical password, Persuasive Cued Click Points.*

I. Introduction

The Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memo ability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP), and conducted user studies evaluating usability and security.

It is now beyond any doubt that USER AUTHENTICATION is the most critical element in the field of Information Security. To date, Text Based Password Authentication (TBPA) has shown some difficulties that users have tended to write passwords down manually or save them on hard disc. This tendency is caused by passwords being strong and thus difficult to memorize in most cases. This has inadvertently given rise to security issues pertaining to attack. Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY &SECURITY. The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA's.

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments. Although security researchers have made great strides in fighting these threats by protecting systems, individual users and digital assets, unfortunately the threats continue to cause problems. The principle area of attack is AUTHENTICATION, which is of course the process of determining the accessibility of a user to a particular resource or system.

Today, passive or active users are the key consideration of security mechanisms. The passive user is only interested in understanding the system. The active user, on the other hand, will consider and reflect on ease of use, efficiency.

Memorability, effectiveness and satisfaction of the system. Generally authentication methods are classified into three categories:

1.1 Inherit Based Authentication

The Inherent Based Authentication category which is also known as Biometric Authentication, as the name suggests, is the automated method/s of identity verification or identification based on measurable physiological or behavioral characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods. Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users nor be stolen as happens with tokens, keys and cards. Unlike the security of a user's password, biometric characteristics, for instance the user's fingerprint or iris pattern, are no secret. Hence there is no danger of a break in security.

1.2 Token Based Authentication

The Token Based Method category is again as the name suggests authentication based on a TOKEN such as: a key, a magnetic card, a smart card, a badge and a passport. Just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

1.3 Knowledge Based Authentication

The concept of Knowledge Based Authentication is simply the use of conventional passwords, pins or images to gain access into most computer systems and networks. Textual (alphabetical) and graphical user authentications are two methods which are currently used.

1.4 Existing system

In the existing system**,** Brostoff and sasse carried out an empirical study of pass faces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Pass logix Corporation, the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to pass points. In ccp, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning).It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. 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. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems

Disadvantage: The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable.

The objective is to provide the security for any websites by using graphical passwords with view port and persuasive cued click-points.

1.5 Proposed system:

In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

1.6 Levels:

Level 0:

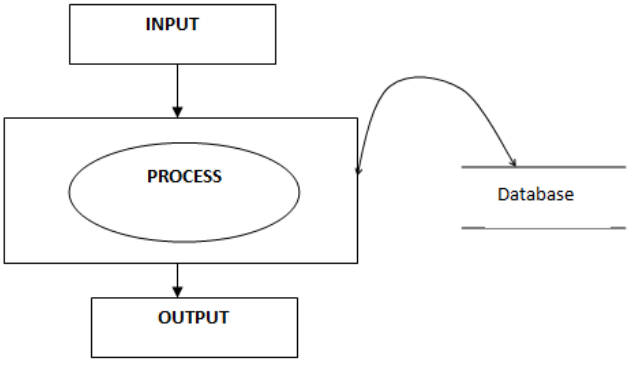


figure 1: level 0

Level 1:

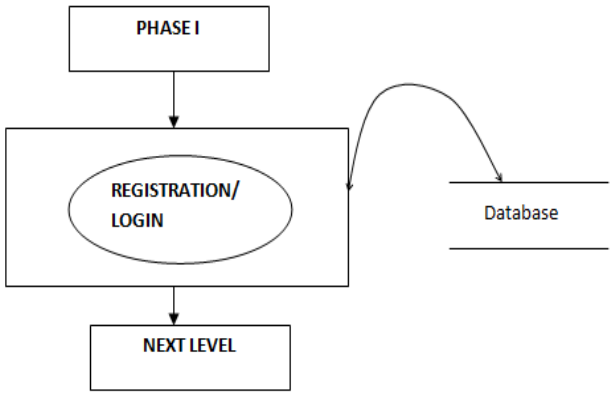


figure 2: level 1

Level 2:

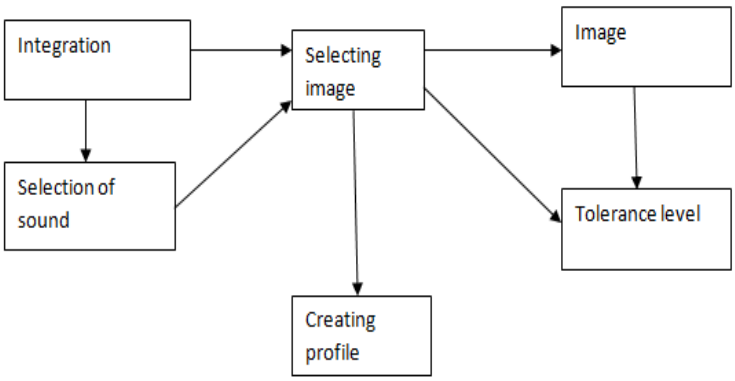


figure 3: level 2

Level 3:

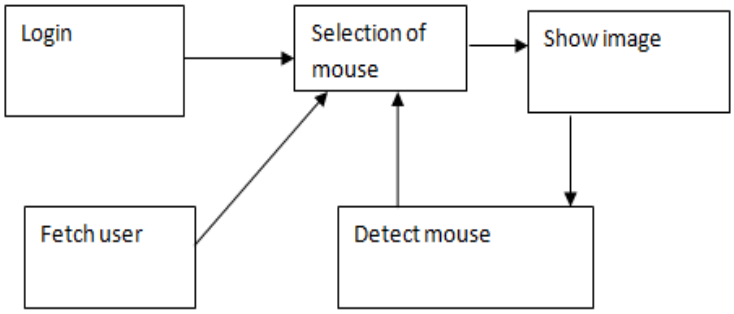
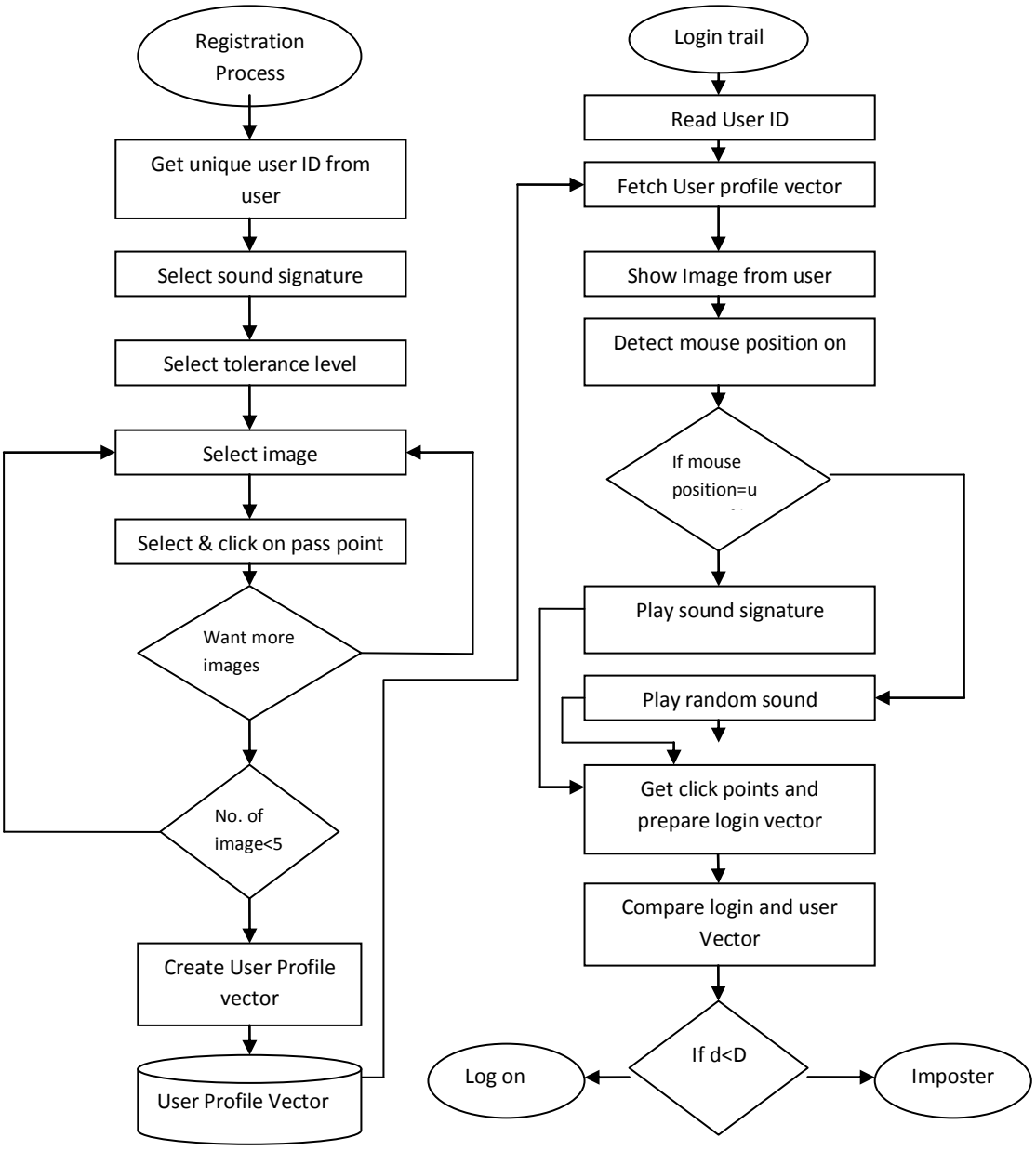


figure 4: level 3

1.7 System flow chart:



II. Algorithms

Algorithm Details

1. MD 5(Message-Digest)
2. DES(Data Encryption Standard)

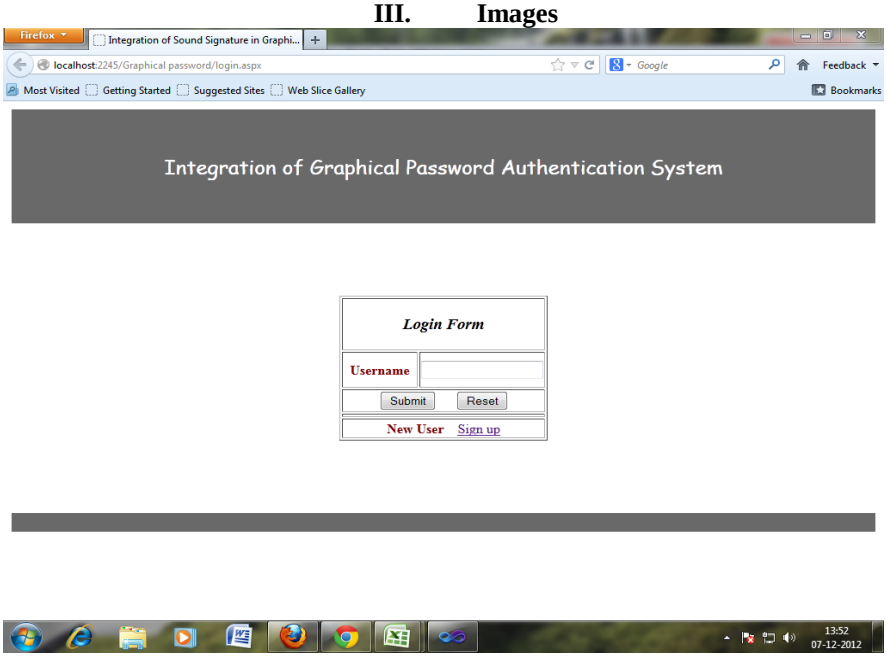
MD5 Algorithm Description

- We begin by supposing that we have a b-bit message as input, and that we wish to find its
- Message digest, Here b is an arbitrary nonnegative integer; b may be zero, it need not be a
- Multiple of eight, and it may be arbitrarily large. We imagine the bits of the message written
- down as follows:
- m_0 m_1 ... m_{b-1}
- The following five steps are performed to compute the message digest of the message.

DES (Data Encryption Standard)

- The choice of the primitive functions **KS, S_1, ..., S_8** and **P** is critical to the strength of an encipherment resulting from the algorithm
- The recommended set of functions are described as **S_1, ..., S_8** and **P** in the algorithm.
- The first part of the table determines how the bits of C_0 are chosen, and
- the second part determines how the bits of D_0 are chosen.
- The bits of **KEY** are numbered 1 through 64.

III. Images



figuure 5: home page

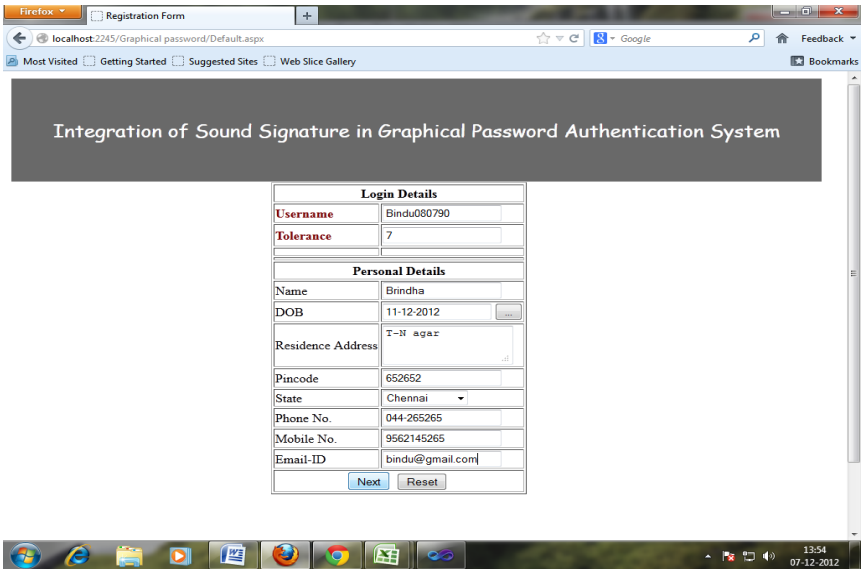


figure 6: sign up

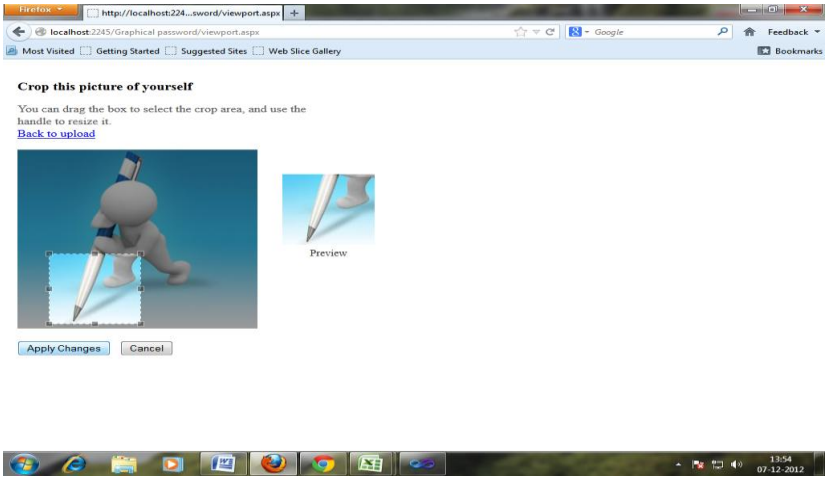


figure 7: upload images

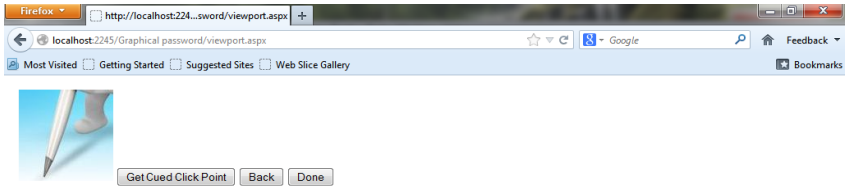


figure 8: get click points

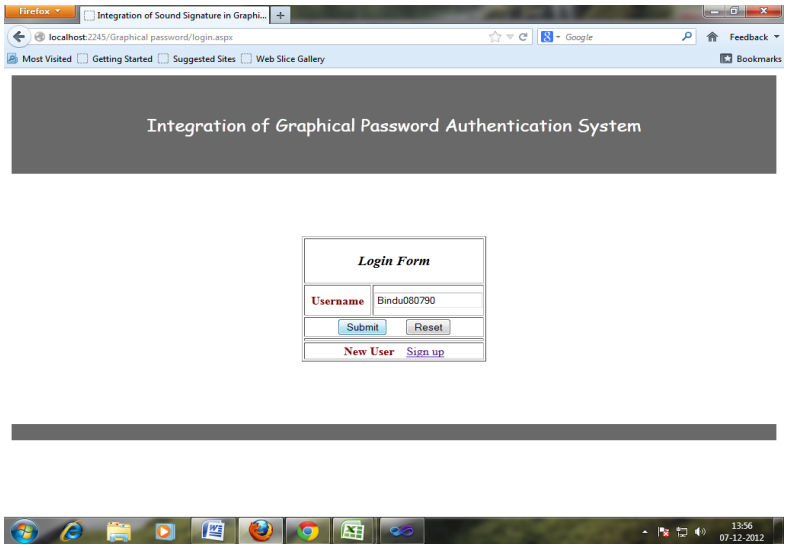


figure 9: login page

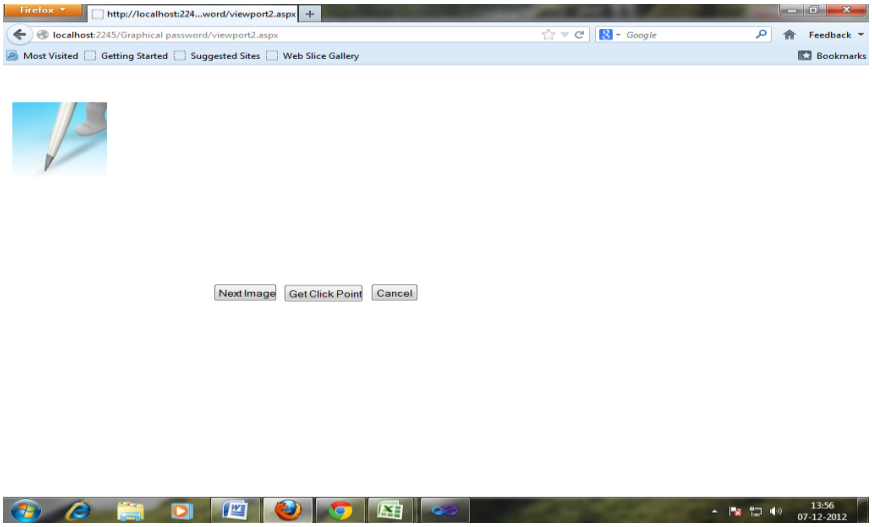


Figure 10: get image

figure 11: mail service

IV. Conclusion

A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred (at some cost in usability) from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember.

Providing instructions on creating secure passwords, using password managers, or providing tools such as strength meters for passwords have had only limited success. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions. In PCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection. Another often cited goal of usable security is helping users from accurate mental models of security. Through our questionnaires and conversations with participants in authentication usability studies, it is apparent that in general, users have little understanding of what makes a good password and how to best protect themselves online. Furthermore, even those who are more knowledgeable usually admit to behaving insecurely

(such as reusing passwords or providing personal information online even when unsure about the security of a website) because it is more convenient and because they do not fully understand the possible consequences of their actions. Guiding users in making more secure choices, such as using the viewport during password creation, can help foster more accurate mental models of security rather than vague instructions such as "pick a password that is hard for others to guess." This persuasive strategy has also been used with some success to increase the randomness of text passwords [40].Better user interface design can influence users to select stronger passwords. A key feature in PCCP is that creating harder to guess password is the path of least resistance, likely making it more effective than schemes where secure behaviour adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space.

To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points. System showed very good Performance in terms of speed, accuracy, and ease of use.

Acknowledgements

We would like to thank Prof.L.V.N.Prasad and Prof.H.Venkateshwara Reddy, Vardhaman College of Engineering for their help in web based techniques and Ms.M.L.Prasanthi Associate Professor CSE Department for her guidance throughout this paper.

REFERENCES

Journal Papers:

[1] Sonia Chiasson, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism VOL. 9, NO. 2, MARCH/APRIL 2012

Books:

[2] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "on purely automated attacks and click-based graphical passwords" (Proc.Ann. Computer Security Applications Conf. (ACSAC), 2008).

Chapters in Books:

[3] Image Pointers: A. Baddeley and R. Turner, "Spatstat: An R Package for Analyzing Spatial Point Patterns," (J. Statistical Software vol. 12, no. 6, pp. 142, 2005).

[4] Graphical Password Security :" Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," (E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle"Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010).

Theses:

[5] Implementation of Knowledge based Authentication System Using Persuasive Cued Click Points, JNTU Hyderabad, India.

Proceedings Papers:

[6] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp.Usable Privacy and Security (SOUPS), July 2007.