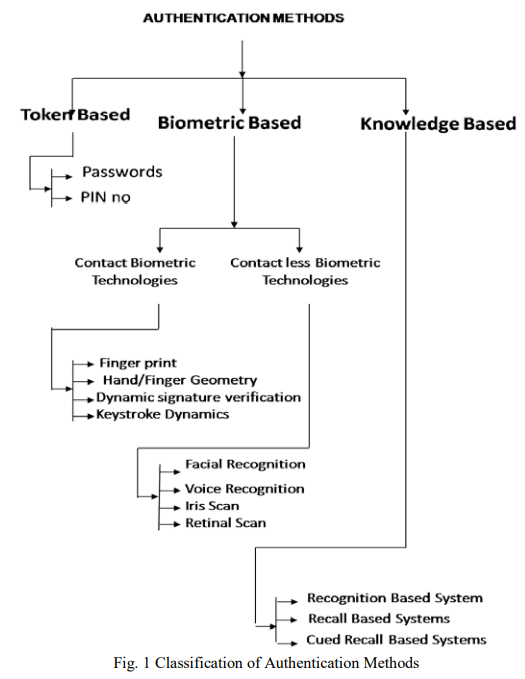
Name : A Graphical Password Based System for Small Mobile Devices

Author Name : Wazir Zada Khan1 , Mohammed Y Aalsalem2 and Yang Xiang3

Contents :

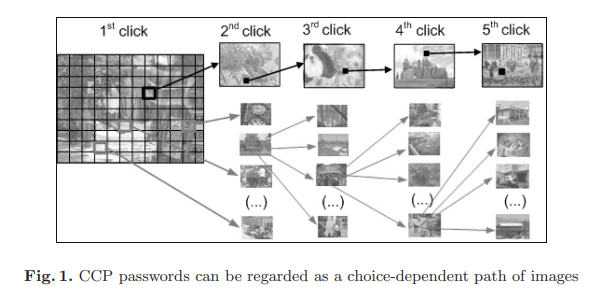
1. In this paper, considering the problems of text based password systems, we have proposed a new graphical password scheme which has desirable usability for small mobile device.
2. During the first phase called Registration phase, the user has to first select his username and a textual password. Then objects are shown to the user to select from them as his graphical password. After selecting the user has to draw those selected objects on a touch sensitive screen using a stylus.
3. During the second phase called Authentication phase, the user has to give his username and textual password and then give his graphical password by drawing it in the same way as done during the registration phase. If they are drawn correctly the user is authenticated and only then he/she can access his/her account.
4. It has also some limitations and issues like all the other graphical based password techniques.
5. **Proposed System :** we have proposed a hybrid system for authentication. This hybrid system is a mixture of both recognition and recall based schemes.



Name : Graphical Password Authentication Using Cued Click Points

Author : Sonia Chiasson, P.C. van Oorschot, and Robert Biddle

Content :

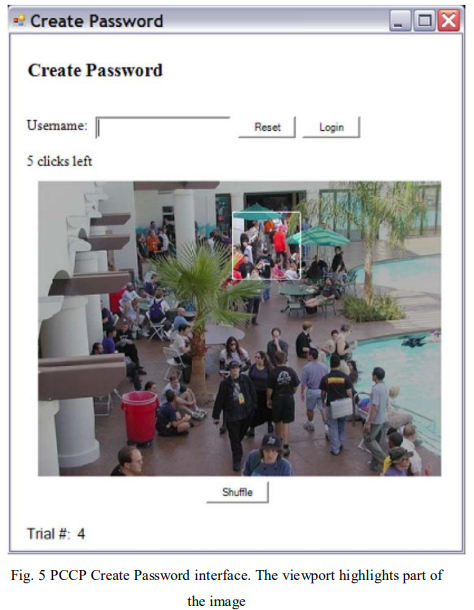
* A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in.
* CCP is not intended for environments where shoulder-surfing is a serious threat.
* During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys.
* Davis et al. [5] proposed an alternative scheme, Story, that used everyday images instead of faces and required that users select their images in the correct order.
* A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.
* We believe that CCP offers a more secure alternative to PassPoints. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.
* **Proposed System** : They proposed a “robust discretization” scheme [1], with three overlapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key.
* The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism . 

Name : Survey on Various Techniques of User Authentication and Graphical Password

Author : Vikas K. Kolekar, Milindkumar B. Vaidya

Content :

* In this paper Authentication methods and techniques are currently available in sufficiently but each has its own profits and loss. Main discussion for graphical based passwords is that people are better at remembering picture passwords than text based passwords.
* 1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
* 2. System defines pictures: pictures are selected by the user from the database of the password system
* **Proposed System** :



Name : Shuffled Input Graphical Password Authentication Schemes Built On Captcha Technology

Author : Vikas K. Koleka , Milindkumar B. Vaidya

Content :

* We used click based captcha as graphical password and based on that we proposed and implemented shuffled input password scheme. With the correct use of image processing and AI techniques, we provided solution to online password guessing attack, dictionary attack, and relay attack.
* Overall, we provided smart solutions as far as password security and attacks are concerned with the help of AI.
* **Proposed System** : Shuffle Input is a recognition based scheme with shuffled input. In this scheme we used captcha as graphical password.
* **OPTION 1:** SHUFFLED PASSWORD In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 1, user can provide his password in shuffled way. For example, if password, P = {“h”, “e”, “l”, “l”, “o”} then user can provide “llohe” or “helol” etc. While login user first has to select the option 1 from drop down menu followed by clicking shuffled password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered option then it allows all possible combinations of password alphabets. Each time user can provide combination of his original password hence it is a smart solution for shoulder-surfing as well as dictionary attack.
* **OPTION 2:** REVERSED PASSWORD In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 2, user can provide his password in reverse way. For example, if password, P = {“h”, “e”, “l”, “l”, “o”} then user can provide “olleh”. While login into system, user first has to select the option 2 from drop down menu followed by clicking reverse password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered option then it allows reverse of password alphabets. Each time user can provide reverse of his original password hence it is a smart solution for shoulder-surfing and dictionary attack.
* **OPTION 3:** SKIPPED PASSWORD In this option user will get captcha challenge image having alphabets, numbers and special characters on it. In option 3, user can provide his password by skipping particular words from his password in sequence. For example, if P = {“h”, “e”, “l”, “l”, “o”} is password then user can jump over one character in sequence then user can provide “hlo” etc. To login user first has to select the option 3 from drop down menu followed by clicking skipped sequence of password. Then authentication server verifies user name and fetch its original password. After that it checks the option if it is registered then it allows skipped sequence of password alphabets. Each time user can provide skipped sequence of password of his original password hence it is a smart solution for shoulder surfing, dictionary attack and online guessing attacks.

