**Three-Dimensional Password for More**

**Secure Authentication**

**Abstract:**

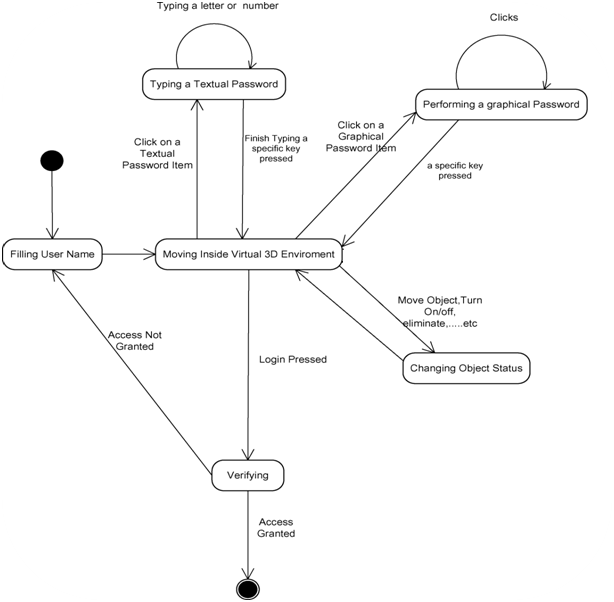
Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user’s 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.

**Introduction:**

Normally the authentication scheme the user undergoes is particularly very lenient or very strict. Throughout the years authentication has been a very interesting approach. With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or to hack someone’s password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the sane number coming is rare.

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. Mostly textual passwords follow an encryption algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning).Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Ten years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play. Therefore we preset our idea, the 3D passwords which are more customizable, and very interesting way of authentication.

**Architecture:**

****

**Working:**

Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. Say a virtual garage.

Now in a day to day garage one will find all sorts of tools, equipments, etc. each of them having a unique properties. The user will then interact with these properties accordingly. Each object in the 3D space, can be moved around in an (x, y, z) plane. That’s the moving attribute of each object. This property is common to all the objects in the space. Suppose a user logs in and enters the garage. He sees and picks a screw-driver (initial position in xyz coordinates (5, 5, 5)) and moves it 5 places to his right (in XY plane i.e. (10, 5, 5).That can be identified as an authentication.

Only the true user understands and recognizes the object which he has to choose among many. This is the Recall and Recognition part of human memory coming into play. Interestingly, a password can be set as approaching a radio and setting its frequency to number only the user knows. Security can be enhanced by the fact of including Cards and Biometric scanner as input. There can be levels of authentication a user can undergo. More the confidentiality more the complexity. In that scenario a virtual environment can be developed as a globe, a city or simply a garage.

**Modules:**

* 3D Visualization Module – to be designed using Java 3D and Processing IDE
* Event Handling – Event handling is done in Java 3D by capturing mouse and keyboard events using Java Event Handling. This is required to update the 3D environment as well as to store user interaction sequence in 3D environment.
* SMTP email client-– An Email client will be implemented for SMTP mails using Apache Commons Net Library.
* GUI – Using AWT / Swing

**Application:**

* Critical servers
* Nuclear and military facilities
* Airplanes and jetfighters
* ATMs
* Personal digital assistants
* Desktop computers and laptop logins
* Web authentication.