**CHIPPWORDS**

**Passwords simplified**

Snehitha Barukula

AP18110010438

CSE - G (07) (2nd year)

Department of Computer Science

SRM University – AP

**Abstract**

As there is an increase in usage of computers and smart devices, security concerns are brought to limelight. Chippword is a 3D password customization and interesting way of authentication. Nowadays the passwords are completely based on the fact of human memory, we usually set easy and simple ones so as to recall them quickly. Authentication to any system means providing security. Due to which the human memory has to merry go round the facts of recognition, recalling, biometrics or token-based authentication. Each of these mentioned procedures has some limitations and drawbacks, in order to avoid these flaws this new technology is introduced.

The Chippword GUI opens up once you get logged into a secure website. This can be any additional textual password that the user can put. Chippword is a multilevel authentication scheme that uses java technology, so whenever the user goes through the first phase of authentication a 3D virtual room appears on the screen. The room contains various virtual objects. The user has to traverse through this environment and interacts with the objects. Chippword combines the four facts of human memory on authentication basis. This is done by the virtual objects that requests information that has to be recalled and recognize, the tokens to be granted and biometric data that has to be verified. The main objective of the project is to combine the authentication of existing systems and providing high level security to the user also this will enable the user to in selecting more than one password scheme. The action towards an object that is in location (x1, y1, z1) is different from an object that is at another location (x2, y2, z2) and hence the user has to follow the pattern. This means that the user has to interact with the virtual objects that reside at the exact location and perform the same action in the proper sequence. Adding with biometric and token verification the scheme becomes difficult to crack.

**Introduction**

3D or graphical passwords were first recognized by Blonder in 1996. According to his concept of study the user will be displayed with an image and has to select specific regions, if the regions selected by the users are correct the user will be authenticated.

The huge increase in computer usage has given rise to security concerns. Certifying a person’s identity is still a challenging task in society. There are three ways in which the authentication can be done. One way is to check the person based on the occupation like keys, ID card, ID numbers etc. Second way is to certify the person based on human knowledge such as passwords, PIN numbers etc. Third way includes authentication based on human features like biometrics. There are high chances that items under possession and human knowledge may be forgotten one day. However, in this digital world things are getting progressed eventually and the authentication based on biometrics is observed everywhere. Limitations to these ways can be overcome, by combining all the three ways into a single system. The proposed Chippword is a multifactor authentication scheme that combines all the existing factors into a single virtual environment. The room contains various virtual objects. The user has to traverse through this environment and interacts with the objects.

The virtual object can be any object that we encounter in our daily lives. Any actions or interactions that we do in our day to day lives can be done in a virtual environment towards the 3D object. Any Kind of user input can be taken as part of Chippword. The main application domain is to provide security for critical systems and resources. We can observe the use of Chippwords in critical servers, military services, airplanes, etc. A small virtual room can be created for a few systems like ATM, Desktops, laptops, personal digital assistants, etc.

**Literature Survey**

3D or graphical passwords were first recognized by Blonder in 1996. According to his concept of study the user will be displayed with an image and has to select specific regions, if the regions selected by the users are correct the user will be authenticated.

GRAPHICAL PASSWORD

RECOGNITION BASED

HYBRID SCHEMES

RECALL BASED

CUED RECALL BASED

PURE RECALL

BASED

Later then Dhamig and Perig developed a recognition based graphical password system. The user has to select a portfolio from given portfolios that include randomized art. Each image is classified from an 8B seed. Another recognition-based password is passfaces. The algorithm here works by having the user select a subgroup of k faces from a group of n faces. During the authentication process the system displays m faces and of the face belongs to the subgroup of k faces. As a result, the user has to select multiple times to complete the authentication process. Another way is story-based authentication that include selecting objects in the pictures like cars, traffic lights, people etc. Davis et al concluded that user’s preference in choosing the passface or a story line would result in password spacing which is far less than theoretical entropy.

The Blonder Scheme is considered as recall based system as the user has to remember all the selected locations. However, PassPoint is a recall-based authentication where a picture is provided in the background to the user and he is free to select anywhere in the picture as his password. Draw a secret DAS is a graphical password system which is launched by Jermyn et al. The user can create drawings on a simple grid. The strokes in the user’s drawing are considered as passwords. The probability of password space is based on complexity and size of the drawing. However, the limitations are left to human error as one has to recall the where the drawings started and ended.

Authentication now a days is based on who you are, in other words they are based on human features. Biometric authentication systems are exhaustively used worldwide. Finger prints, iris recognition, voice recognition, face recognition and palm printing are few common practices for biometrics.

* Human features are exposed to nature and may transform over a period of time.
* People are not convenient with biometrics all the time. They resist sometimes as having a copy of user’s finger print is not safe and may be used for fraud.
* Biometrics cannot be nullified, which leads the user to a dilemma in the data that has been forged. Unlike other authentication systems where the user can create a new password if he/she forgets the current passwords, Biometrics are unique and cannot be replaced.

**Problem Statement**

The three-level authentication system validates the user to access a particular system only if the input password is selected correct. The project involves multilevel authentication scheme which increases the password space. While on the other hand we have many other authentication systems which have failed or limited due to bot attacks. Most of us find the textual passwords unfriendly. Hence in the three-level authentication system we try to create a user interface and provide users with comfortable way in solving password. Therefore, the aim of the project Chippword is to provide maximum security to authentication process.

One of the areas where 3D passwords work effectively is in airplanes and jet planes but lately it has been misused by the politicians for personal agendas. The main strategy behind this project is to protect such airplanes with high authentication systems also nuclear and military should be provided with these powerful systems for high level security locations.

**Levels of authentication:**

**First level:** In the first level the user has to initially create a text password with few specifications.

**Second level:** In the second level the user will have to upload a picture of his choice into the system and create the password by segmenting and assigning serial numbers. Therefore, when the user logins the system automatically disperses the images segments and user will arrange them in a proper set as they did initially.

**Third level:** In the third stage the user will set the graphical password based on color and RGB button combinations.

**Proposed System**

This application uses java technology. The virtual room is called 3D arena is a obj file is downloaded and then coded into java technology.

Software requirements: windows XP / windows 10

NetBeans IDE/Eclipse IDE

Arena 3d model

Hardware components: processor: i3 or latest

Memory – 1gb ram

Let us consider a 3D virtual room of dimension K\*K\*K such that it’s coordinates is represented by (x,y,z) = [1,…………….,K] \*[1,…………..K]\*[1,……………..K]. The images are distributed in the virtual environment with unique (x,y,z) coordinate points. Assuming that the user uses any input device like mouse, keyboard, iris scanner, fingerprint scanner etc. to navigate along the room. We consider the path in which the user interacts with previous input devices as his 3D password.

For example, consider a user that navigates through the 3d environment virtual room contains a bedroom and locker. Let us assume that the user in in the virtual bedroom and around to the door located in (11,25,92) and opens it. Then the user closes the door. Then the user finds a laptop to the left at the position (5,35,19), and he types “CHIPPGANG”, then he opens the locker and picks some money located at (20,34,90) and then he presses login button. Therefore, the user’s location is recorded as follows:

(11,25,92) Action = “Opens the door”

(11,25,92) Action = “Closes the door”

(5,35,19) Action = typing, “C”

(5,35,19) Action = typing, “H”

(5,35,19) Action = typing, “I”

(5,35,19) Action = typing, “P”

(5,35,19) Action = typing, “P”

(5,35,19) Action = typing, “G”

(5,35,19) Action = typing, “A”

(5,35,19) Action = typing, “N”

(5,35,19) Action = typing, “G”

**Pseudo code for creating Main Screen**:

**public** **class** mainscreen **extends** JFrame {

**public** mainscreen () { // creating a constructor

**super**("3D arena"); // set the borders,layouts,size for the frame

**try** {

// attach the file containing the arena model

} **catch** (MalformedURLException ex) {

Logger.getLogger(mainscreen.**class**.getName()).log(Level.SEVERE, **null**, ex);

}

}

**public** **static** **void** main(String args[]){

**new** mainscreen();

}

}

Brute Force algorithm: As discussed earlier when the virtual room appears the user will have to traverse with different actions and reactions. The algorithm followed here is brute forced with n number of possibilities for a password. Although we need to take few considerations into account

1. the time required to login: According to the research and study the time taken for a successful login varies and depends upon the no. of obvious actions and reactions by the user.
2. the total cost required: on the other hand, we need to create a 3D virtual environment and creating such an environment is quite expensive.

**Pseudo code for creating a screen:**

**public** **class** screen1 **extends** javax.swing.JFrame {

**public** screen1() {

initComponents();

} // a constructor is created and this method is called from within the constructor to initialize the form //

**private** **void** initComponents() {

jLabel2 = **new** javax.swing.JLabel();

jButton1 = **new** javax.swing.JButton();

jLabel1 = **new** javax.swing.JLabel();

jButton2 = **new** javax.swing.JButton();

setDefaultCloseOperation(javax.swing.WindowConstants.***EXIT\_ON\_CLOSE***);

jButton1.setText("Next");

jLabel1.setIcon(**new** javax.swing.ImageIcon(getClass().getResource(".PNG")));

jButton2.setText("Next");

pack();

}

**public** **static** **void** main(String args[]) {

**try** {

**for** (javax.swing.UIManager.LookAndFeelInfo info : javax.swing.UIManager.*getInstalledLookAndFeels*()) {

**if** ("Nimbus".equals(info.getName())) {

javax.swing.UIManager.*setLookAndFeel*(info.getClassName());

**break**;

}

}

} **catch** (ClassNotFoundException ex) {

java.util.logging.Logger.*getLogger*(screen1.**class**.getName()).log(java.util.logging.Level.***SEVERE***, **null**, ex);

} **catch** (InstantiationException ex) {

java.util.logging.Logger.*getLogger*(screen1.**class**.getName()).log(java.util.logging.Level.***SEVERE***, **null**, ex);

} **catch** (IllegalAccessException ex) {

java.util.logging.Logger.*getLogger*(screen1.**class**.getName()).log(java.util.logging.Level.***SEVERE***, **null**, ex);

} **catch** (javax.swing.UnsupportedLookAndFeelException ex) {

java.util.logging.Logger.*getLogger*(screen1.**class**.getName()).log(java.util.logging.Level.***SEVERE***, **null**, ex);

}

//declaring the variables//

**public** **void** run() {

**new** screen1().setVisible(**true**);

}

});

}

// end of declaration //

**Performance Analysis**

The 3D password space can be calculated by using π(Lmax, K) on a 3D virtual room that has space (k\*k\*k) for a password of length Lmax or less.

Mathematically, П (Lmax, G) = ∑ (m + g (AC)) n.

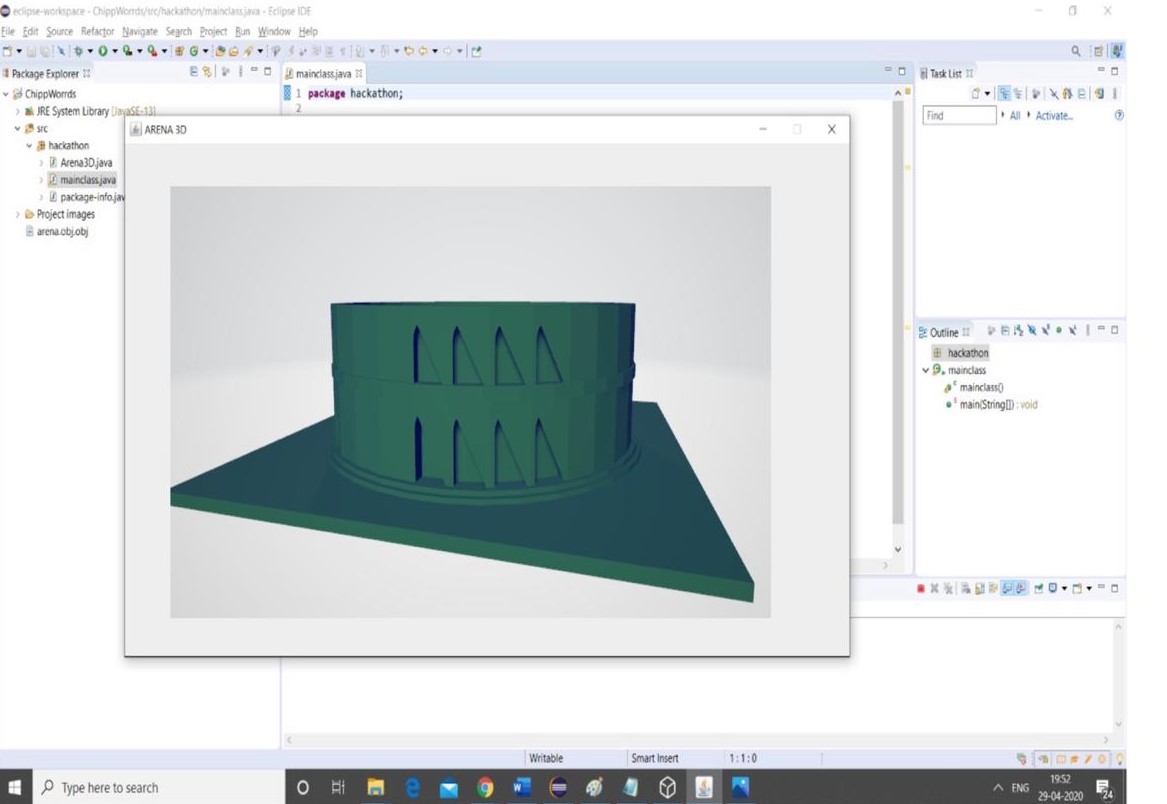
In the above expression:

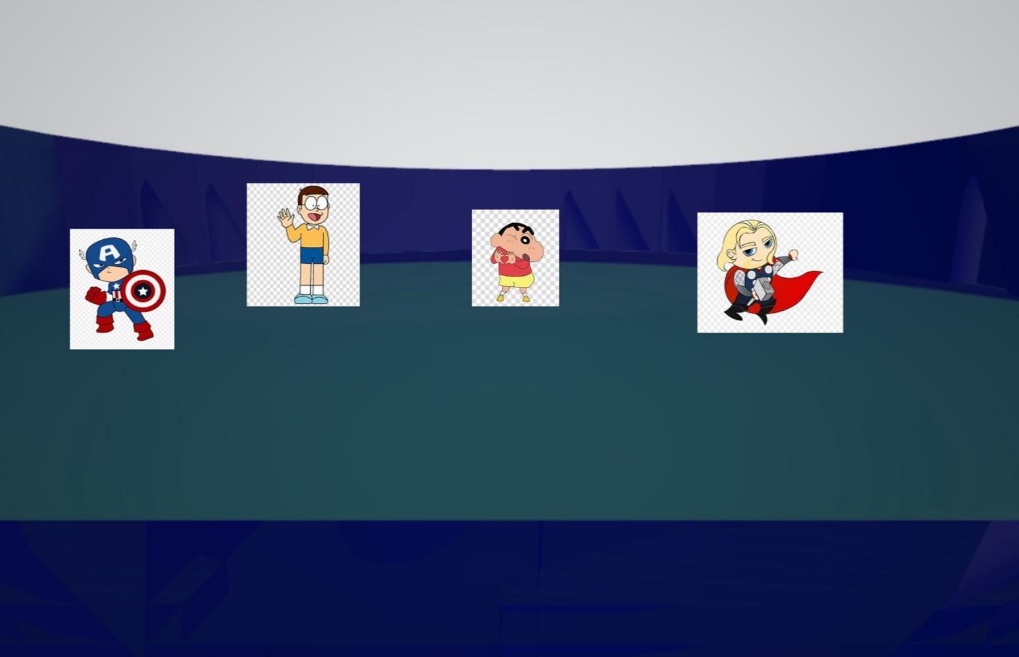
g(AC) represents total no of actions and interactions made with the environment.

Lmax is the maximum length of the password the user can put which is generally the images on each side of the cube

M stands for possible no. of actions towards the objects in the environment.

Therefore, the value of the equation gives the total no of spaces required to store password for the 3D environment.

****

****

The graph represents the no. of possible actions and reactions of a Chippword within the 3D environment. The size of each bit in Klein study is (3\* 10^6) dictionary of eight-character textual password

According to Klein the above graphs points two important textual password points. Here point a specifies only two actions and reactions as a 3D password while point b specifies the full textual password of 8 character or less. Hence from the previous equation we can observe that the type of action and interaction between the user and the virtual environment determines the password space. Therefore, creating a 3D environment plays a crucial role for creating a 3D password.

Time complexity:

Time complexity of the program is Am + Bn where m is time required to communicate with the system and n is the time required to process each algorithm in the virtual environment.

Space complexity:

The 3D password is stored as a database in the system as (x, y, z) coordinate point. Since it is a 3D password the three dimensions are considered for virtual environment.

The objective of graphical passwords is to reflect what people see in day-to-day life. The objects that the user sees in the virtual room should look similar to ones in real life. However, 10 objects at the same place may confuse the user when he re-visits the same place after a month and hence they should be distinguished properly. Creating and designing a proper 3D environment affects the usability and acceptability of the Chippword system. Hence building Chippword system is to design a good virtual environment that meets the administration and security needs. The following guide lines were taken into account while creating the design:

**State diagram of a possible Chippword system:**

.

Typing a letter or number

Performing a graphical password

user

Typing a textual password

Moving into the 3D environment

Filing a user name

Performing biometrics

access not granted login pressed

Object status

Verifying the user

Access granted

**Conclusion**

The available sources of passwords today include textual passwords and graphical passwords. But they are restricted to some limit. However, there are many Authentication systems under research and they might require additional factors for commercial use. Chippword is multifactor authentication scheme that combines all the existing schemes. The virtual room can contain any of the existing authentication systems as a result the password space increases. The user can choose and construct a desired 3D password. The 3D password authentication system is at its early stage and still new to major part of the world. Designing various kinds of virtual rooms, password spaces, and translating user feedback and experiences will enhance and improves the user experience towards Chippword. The future work of the researchers should include how to overcome gathering attacks from different background activities. Inclusion of biometrics ends up in increasing cost and hardware in the scheme, to scale back this can be still a field of research. Shoulder surfing attack, brute force attack, timing attack are still possible and effective against 3D passwords Hence the Chippword systems can be employed in various applications as discussed earlier. Thus, this paper gives a clear study about 3D password systems. Implementing Chippword for mobile applications is another important future work of this project.

**References**

[1] G.E. Blonder, “Graphical Password,” U.S Patent 5 559 961, Sep.24, 1996.

[2] study of three - dimensional password authentication system. (2016), Retrieved from

<https://ijarcce.com/wp-content/uploads/2016/11/IJARCCE-ICRITCSA-27.pdf>

[3] A Framework for secured 3D password using Genetic Algorithm. (2015), Retrieved from

<https://www.researchgate.net/publication/271508763_A_Framework_for_Secure_3D_Password_using_Genetic_Algorithm>

[4] 3D Password Based Authentication System Using Multiple Layers. (2014), Retrieved from

<https://www.researchgate.net/publication/276281665_3D_Password_Based_Authentication_System_Using_Multiple_Layers>

[5] Virtual Realization Using 3D password. (n.d), Retrieved from

<https://pdfs.semanticscholar.org/6c5a/98ccf829fd49be6cffd6642491dea0806ee8.pdf>

[6] Security Using 3D Password. (2015), Retrieved from

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.6431&rep=rep1&type=pdf>