GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

A. Achuthram, S. Samrat, P. Nithish
Dr. G. PRASAD ACHARYA (Guide)
Sreenidhi Institute of Science and Technology
Hyderabad

ABSTRACT:

Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, this method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques.

1.Introduction

Human factors are often considered the weakest link in a computer security system. If we point out that there are three major areas where humancomputer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. User authentication is a fundamental component in most computer security contexts. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using image as passwords. Human factors are often considered the weakest link in a computer security system. Patrick, et al. [1] point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broke. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using pictures as passwords

2.Over view of authentication methods

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

3.Graphical Password :

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should be more resistant to brute- force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques. With increasing technical advancements the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online. With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentication available for users to secure their accounts. Recognition based Authentication: A user is given a set of images and he has to identify the image he selected during registration. For example, Pass faces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the preselected image from the several images presented to him. Recall based Authentication: A user is asked to reproduce something that he created or selected at the registration stage. For example, in the Pass point scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login. Cued Recall: Cued Click Points (CCP) is an alternative to the Pass Points technique. In CCP, users click one point on each image rather than on five points on one image unlike Pass Points. It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click point.

3.1Recognition Based System

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. Recognition- based systems, also known as cogno metric systems [4] or search metric systems [3], generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images from among decoys. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly [8], [9]. From a security perspective, such systems are not suitable replacements for text password schemes, as they have password spaces comparable in cardinality to only 4 or 5 digit PINs (assuming a set of images whose cardinality remains reasonable, with respect to usability). Recognition based systems have been proposed using various types of images, most notably: faces, random art, everyday objects, and icons. Renaud [3] discusses specific security and usability considerations, and offers usability design guidelines focusing on recognition-based systems. In some graphical password schemes, the system must retain knowledge of some details of the shared secret, i.e.,user specific profile data e.g. in recognition schemes, the system must know which images belong to a user's portfolio in order to display them. This information must be stored such that its original form is available to the system (possibly under reversible encryption), and thus may be available to anyone gaining access to the stored information. E.g. Phishing attack and shoulder surfing attack. Dhamija and Perrig

[4] proposed a graphical authentication scheme based on the Hash Visualization technique [9]. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (figure 1). Later, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user. Akula and Devisetty’s algorithm [10] is similar to the technique proposed by Dhamija and Perrig.

The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's. Weinshall and Kirkpatrick [11] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. After one to three months, users in their study were able to recognize over 90% of the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training. Sobrado and Birget [12] developed a graphical password technique that deals with the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (figure 2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow. Man, et al. [14] proposed another shoulder -surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code.

During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. [13] later extended this approach to allow the user to assign their own codes to pass-object variants. Figure 3 shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

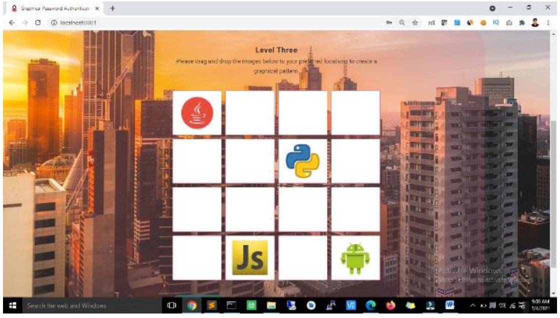
3.2 Recall Based System

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred to as draw metric systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid (which may arguably act as a mild memory cue). Recall is a difficult memory task because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such, transforming the task into one of cued-recall, although one where the same cue is available to all users and to attackers. Text passwords can also be categorized as using recall memory. With text passwords, there is evidence that users often include the name of the system as part of their passwords. Although there is currently no evidence of this happening with graphical passwords, it remains a plausible coping strategy if users can devise a way of relating a recall based graphical password to a corresponding account name. These systems are generally susceptible to shoulder surfing to the extent that in many cases, the entire drawing is visible on the screen as it is being entered, and thus an attacker need accurately observe or record only one login for the entire password to be revealed. Blonder designed a graphical password scheme in which a password is created by having the user click on several locations on an image.

During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Pass logix has developed a graphical password system based on this idea. In their implementation, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. A similar technique has been developed by sfr. It was reported that Microsoft had also developed a similar graphical password technique where users are required to click on pre-selected areas of an image in a designated sequence. But details of this technique have not been available.

4.Proposed System

In graphical authentication there are various techniques to secure your password. Here we are proposing a new algorithm of authentication using images. We used a grid based approach to authenticate by using image as a reference . Shoulder surfing is a major drawback of graphical password authentication. To overcome this we have developed SSR (Shoulder Surfing Resistant) shield. The shield containing multiple fake mouse pointers are programed in such a way that it moves randomly in an image area and the original pointer will look exactly as fake mouse pointers. This shield provides a top layer for grid clicking as well as confusing other person. At the time of registration, user will upload his/her image or set of images along with all details; then user selected image will appear on the page with transparent grid layer on it. So user will select certain grids to set his/her password as shown in the figure below.



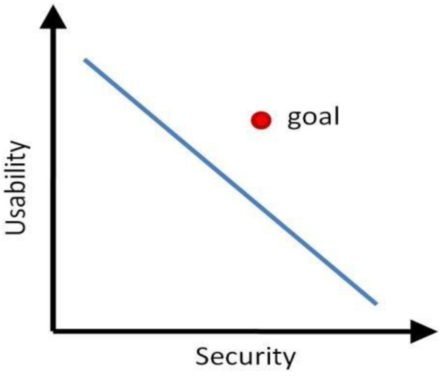
Level Three

Please drag and drop the images below to your preferred locations to create a graphical pattern.

Grid approach.

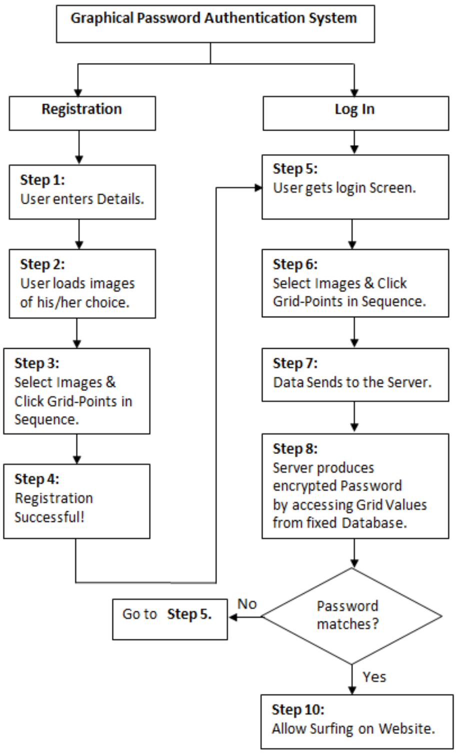
5.Implementation and Discussion

The proposed system was implemented using PHP, CSS, JavaScript and Macromedia flash 2008(Action Script 2). This Graphical Password can be implemented in authenticating several systems and websites. The implementation has few focuses: • Login: Contains username, images, Graphical password and related methods. • Grids: Contains unique grid values and grid clicking related methods.

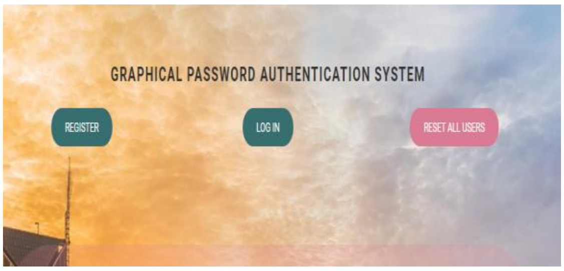


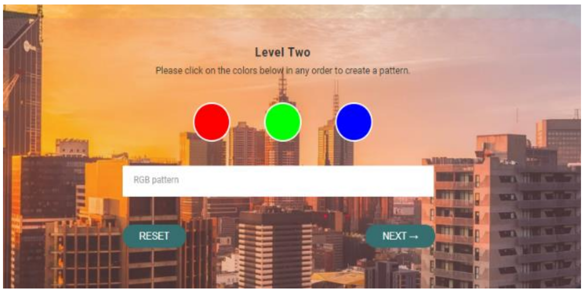
Usability vs Security.

Our main aim is to achieve this goal. In which the usability as well as the security of the system is maintained in such a way that we don’t need to compromise on either of these constraints The working of our system is shown with the help of a flow graph in given figure:-

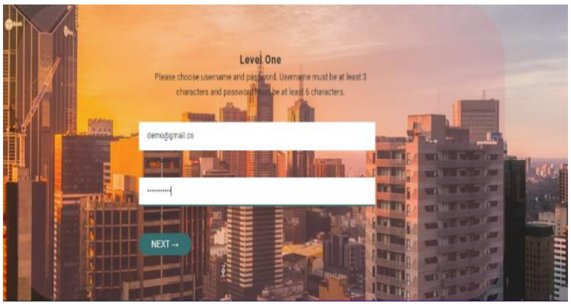

Graphical Password Authentication System
Registration
Log In
Step 1:
User enters Details.
Step 2:
User loads images of his/her choice.
Step 3:
Select Images & Click Grid-Points in Sequence.
Step 4:
Registration Successful!
Step 5:
User gets login Screen.
Step 6:
Select Images & Click Grid-Points in Sequence.
Step 7:
Data Sends to the Server.
Step 8:
Server produces encrypted Password by accessing Grid Values from fixed Database.
Password matches?
No
Go to Step 5.
Yes
Step 10:
Allow Surfing on Website.

7.Screenshots


GRAPHICAL PASSWORD AUTHENTICATION SYSTEM


Level Two

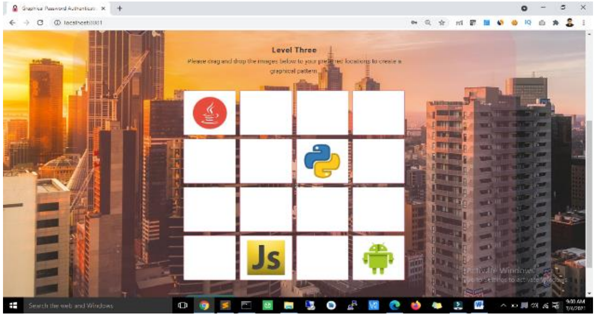
Please click on the colors below in any order to create a pattern.



Level One

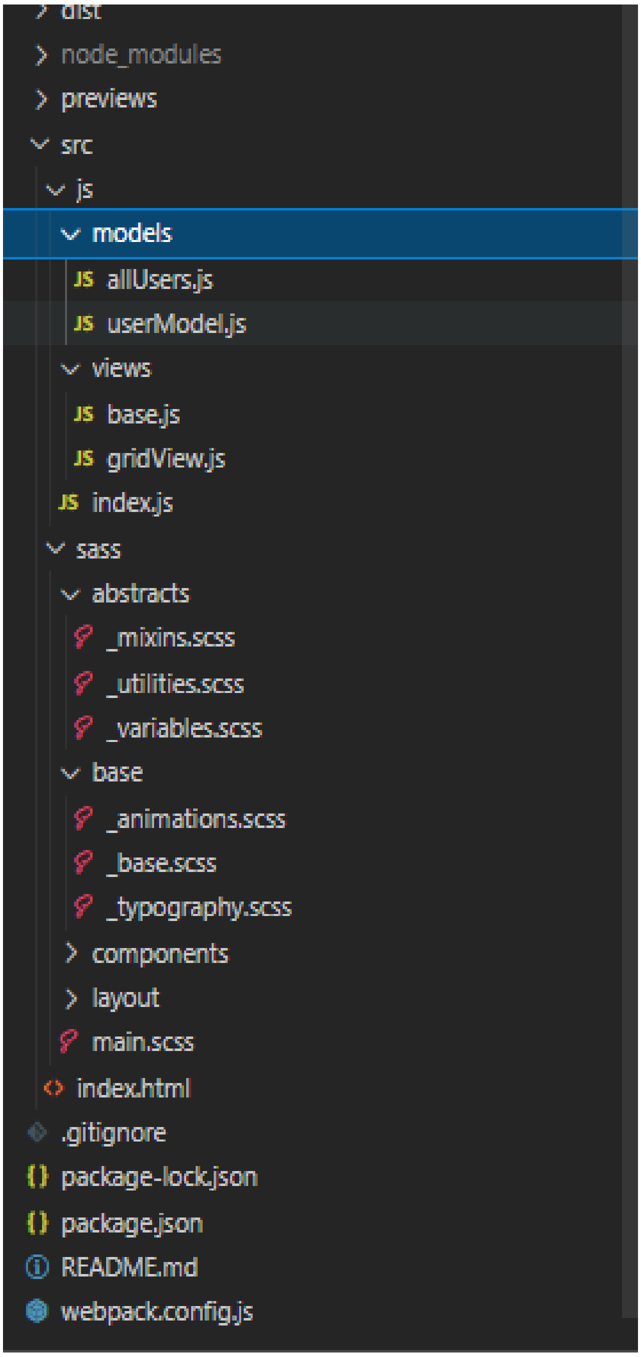
Please choose username and password. Username must be at least 3 characters and password must be at least 6 characters.

demo@gmail.co



Level Three

Please drag and drop the images below to your preferred locations to create a graphical pattern.



```
> dist
> node_modules
> previews
v src
  v js
    v models
        allUsers.js
        userModel.js
    v views
        base.js
        gridView.js
      index.js
  v sass
    v abstracts
        _mixins.scss
        _utilities.scss
        _variables.scss
    v base
        _animations.scss
        _base.scss
        _typography.scss
    > components
    > layout
      main.scss
    index.html
  .gitignore
  package-lock.json
  package.json
  README.md
  webpack.config.js
```

8.Advantages

- It is user-friendly.
- It provides higher security than other traditional password schemes.
- Dictionary attacks are infeasible.
- CCP makes attacks based on hotspot analysis more challenging.

9.Disadvantages

- Registration and login take too long.
- It requires more store space because of images.
- Shoulder surfing(Watching over people's shoulders as they process information).

Webpack.config

```
const path = require('path');

const HtmlWebpackPlugin = require('html-webpack-plugin');


module.exports = {
  entry: './src/js/index.js',
  output: {
    path: path.resolve(__dirname, 'dist'),
    filename: 'js/bundle.js'
  },
  devServer: {
    contentBase: './dist'
  },
  plugins: [
    new HtmlWebpackPlugin({
      filename: 'index.html',
      template: './src/index.html'
    })
  ]
};
```

Packages.json

```
{
  "name": "authentication-system",
  "version": "1.0.0",
  "description": "A graphical password authentication system that uses three levels of authentication",
  "main": "index.js",
  "scripts": {
    "watch:sass": "node-sass src/sass/main.scss dist/css/style.css -w",
    "dev": "webpack --mode development",
    "start": "webpack-dev-server --mode development --open"
  },
  "author": "Graphical Authentication System",
  "license": "ISC",
  "browser": {
    "fs": false,
 "child_process": false
  },
  "devDependencies": {
    "node-sass": "^5.0.0",
    "html-webpack-plugin": "^3.0.7",
    "webpack": "^4.2.0",
    "webpack-cli": "^3.3.12",
    "webpack-dev-server": "^3.1.1"
  },
  "dependencies": {
    "sweetalert": "^2.1.2"
  }
}
```

11.Conclusion :

In this extend we are trying to make our authentication system more user friendly and also we have tried to implement mature & fast Shoulder Surfing Resistant Mechanism. We have considered both methods: text based and graphical based systems and tried to reduce the efforts required by enduser to remember passwords. A look at the advancement in technology over the past few years tells us that the next era will have system security at its core. Thus Graphical Password may be adapted in future as a major authentication system. Our system is a combination of recognition and recall based approach. It is more usable and secure as compare to previous graphical password authentication systems As password space is very large it provides the security against brute force attack. It is easy to use. Passwords can be created and memorized easily Randomization in both the authentication steps provides strong security against shoulder surfing. Overall our system is resistant to all other possible attacks also. This system can be used for highly secure systems. In future, one more addition possible to our system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also. So user can get the system updates although he is offline Thus, in future, our system can be made more secure and easy to access

12.References

➢ https://idoc.pub/download/seminar-report-on-graphical-passwordauthentication-6nq8j11wppnw

➢http://www.geeksforgeeks.com/graphical-password-authentication/

➢https://ieeexplore.ieee.org/document/468240860000

➢https://www.researchgate.net/publication/2210464r4286_Graphical_Passwords_A_Survey

➢https://ieeexplore.ieee.org/abstract/document/5749855000/

➢https://www.ijert.org/web-based-graphical-password-authentication