Graphical Password Authentication System

180170116005 - Vishvaa Chhatrara
180170116017 - Rutanshi Khambhatiya
180170116022 - Priya Naika
190173116018 - Harshil Ramanuj

Outline

- Introduction
- Overview of some methods
- Text & Biometrics Drawbacks
- Graphical Passwords and its types
- Drawbacks of current scenario
- Hybrid Technique
- Shoulder surfing resistant techniques.
- Pros of our approach
- Where is it used?
- Conclusion
- References

What is Authentication ?

Authentication is the process of recognizing a user’s identity. It is the mechanism of associating an incoming request with a set of identifying credentials.

Authentication factors :

- The knowledge factors: Something the user knows.
- The ownership factors: Something the user has.
- The inherence factors: Something the user is or does.

Some Password Authentication Methods

- **Knowledge-based authentication**

  includes text-based authentication and picture-based authentication.
- **Token-based authentication**

  includes key cards, bank cards, smart cards, etc.
- **Biometric authentication**

  include fingerprints authentication, iris scan and facial recognition.

Drawbacks of current Systems

- **Text password**

  Text password is a secret word of string of character that is that is used for authentication to prove his identity and gain access to resources.

- **Drawbacks**
  - Difficulty of remembering passwords
  - Vulnerable to attack like Dictionary attack, Brute force attack.

Drawbacks of current Systems

Biometric authentication Drawbacks:

- Costs : Significant investment needed in biometrics for security
- Data breaches : Biometric databases can still be hacked
- Tracking and data : Biometric devices like facial recognition systems can limit privacy for users
- False positives, bias and inaccuracy : False rejects and false accepts can still occur preventing select users from accessing systems

Graphical Passwords

- Graphical password can be used as an alternative to text based (alphanumeric) password in which users click on images to set their passwords.
- Images are generally easier to be remembered than text and in Graphical password; user can set images as their password.
- Where it can be applied:
  - Workstations
  - Web login applications
  - Mobile Devices
  - ATM and Banking Transaction Apps.
- Categories:
  - Recognition Based Techniques
  - Recall Based Techniques
  - Cued Recall Based Techniques

Recognition based Authentication:

- A user is given a set of images and he has to identify the image he selected during registration.

- For example, Passfaces 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 pre-selected 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 Passpoint 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 PassPoints technique.

- In CCP, users click one point on each image rather than on five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

Some known attacks

- Brute force search
- Dictionary attack
- Guessing
- Spyware
- Shoulder Surfing
- Social Engineering

Drawbacks of current scenario..

- It requires more storage space because of images.
- Registration and login process take too long time
- **Less resistant to shoulder surfing.**

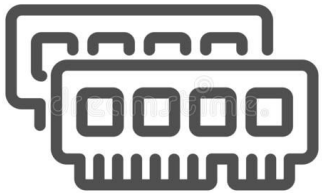
Hybrid Technique

- This technique is the combination of Recognition and recall based techniques.
- It is more usable than other password authentication techniques
- As password space is very large it provides the security against brute force attack. It is easy to use.
- Randomization in both the authentication steps provides security against shoulder surfing.
- Resistant to all other possible attacks also.
- This system can be used for highly secure systems.

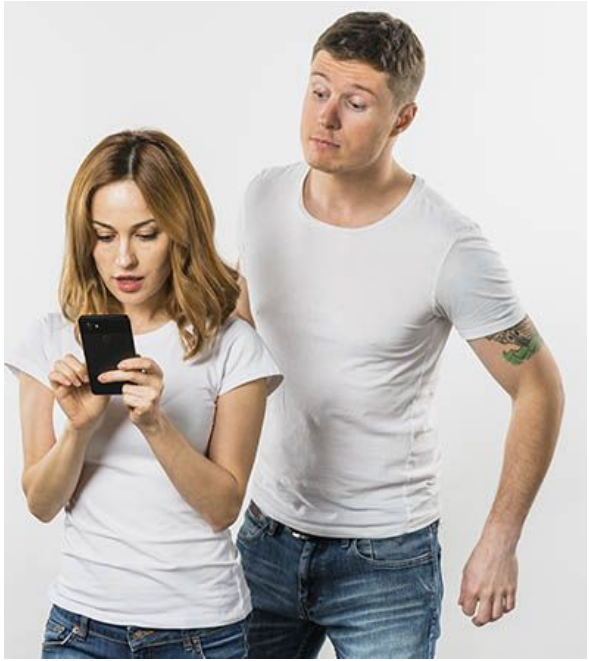
Primary Goal of the project

The proposed system should be -

- Time efficient
- Space / Memory efficient
- **Security towards shoulder surfing problem**
- User Friendly navigation



What is shoulder surfing



- Our approach is mainly to overcome the shoulder surfing attacks.
- Shoulder surfing means watching over the person’s shoulder to get the password.
- When user enters password using keyboard, mouse, touch screen or any other traditional input device, a malicious observer may be able to acquire the user’s password credentials.

Our approach

- **Technique 1: Enter opposites**
  - At the time of registration user is asked to select the 3 categories out of given 8 categories of images(i.e. Cars, Pets, Fruits etc.)
  - At the login time user has to recall which categories he had selected. And Do NOT select that from given set of images having mixture of all categories.
  - This approach can confuse the shoulder surfer and would decrease the chances of success in attack.

- **Technique 2: Same colour illusion**
  - In this technique, at registration phase, user has to choose minimum of 3 and maximum of any number of images from the display screen.
  - Here the display screen will contain an iconic images of selected (specific) objects randomly but repeatedly having different background colours.
  - At login time user need to enter the correct colour of correct object in correct sequence to get authenticated.

- **Technique 3: Hide from Hacker**
  - In this approach, the big idea is that user will enter large number of images (around 10) at the registration phase.
  - At login time, instead of displaying all the images of user to the screen, only some (3 to 4) number of images will be displayed in the cluster of 9 to 12 other (not of user) images.
  - Here, every time when the user comes to login, those 3 to images can be anyone from the user's registered images and will not get repeated consequently.
  - Here shoulder surfer do not get the idea of the images which are not displayed on the screen and cannot differentiate unknown images.

Pros...

- Provides a way of making more human friendly passwords
- Dictionary attacks and brute force search are infeasible.
- It provides higher security than other traditional password schemes.
- CCP makes attacks based on hotspot analysis more challenging.
- **Increased Success rate in resistance to Shoulder surfing and Social engineering attacks.**

Where is it useful?

- Applications or the environment where privacy is a concern and the data leakage can cause the issue to the user and the company both, These techniques of authentication are the best to apply.
- Here more login time taken is even not create a big issue as Security is must.

- The systems where people have to login frequently but there are no such chances of getting hacked because the systems do not contain any confidential or important details of the user, this techniques “ideally” should not be used.
- The reason is that these are time consuming.

Conclusion

- The past decade has seen a growing interest in understanding and implementing graphical password as an alternative to the traditional text-based passwords.
- The main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords.
- Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware.

References:

- http://www.jsoftware.us/vol8/jsw0807-16.pdf
- https://www.researchgate.net/publication/221046286_Graphical_Passwords_A_Survey
- https://www.irjet.net/archives/V5/i3/IRJET-V5I3805.pdf
- https://github.com/sdevkota007/Graphical-Password-Authentication-Using-Persuasive-Cued-Clickpoints-With-File-Encryption
- https://www.sciencedirect.com/science/article/pii/S1877050916001940
- http://www.diva-portal.org/smash/get/diva2:1108259/FULLTEXT01.pdf

Thank You