CSMSS CHH.Shahu College of Engineering
Department of Computer Science & Engineering
Year 2022-23
SEM I

Project Title

Group Id :BT_12

Group Member :
Nilima Sanjay Pattekar(CS4169)
Samrudhi Sunil Deshpande(CS4157)
Rohinee Ashok Chaudhari(CS4102)
Manasi Ashok Kamble(CS4166)

Guide name:A.R.Katkar Sir

Outline

1. Project Title
2. Domain
3. Problem Definition
4. Abstract
5. Scope
6. Software-hardware requirements
7. Literature Review of Conference/Journal Papers supporting Project idea(minimum 5 papers)
8. Plan of Project Execution

Project Title

- Graphical Password Authentication

Domain

- Cybersecurity
- Python

Problem Defination

- Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login o the system. Summary: Remembering numerous passwords from various different sites can be difficult for a user. So to provide some flexibility we can provide users a graphical password authentication system where instead of creating a password a user has to select graphical objects in a particular order to keep it as their password. Objective: : In this method, the user is required to select some images (let's say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which is in turn followed by KitKat and so on). Next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially. Every time the user will have to use the same sequence while the images are placed in different ways. This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and provide better results to this process.

Abstract

- A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is called graphical user authentication (GUA). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant disadvantages. For e.g, users tend to choose passwords that can be easily guessed. On the other hand, if a password is difficult to guess, then it is often difficult to remember. To overcome this problem of low security, Authentication methods are developed by researchers that use images as password. In this research paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own. Graphical password schemes have been proposed as a possible alternative to text-based schemes, by the fact that humans can remember pictures better than text; Pictures are generally easier to be remembered or recognized than text.

Scope

- Enhance security
- user-friendly system
- Dictionary attacks are infeasible.
- GUA makes attacks based on hotspot analysis more challenging.

Software Hardware Requirement

- Linux
- Django
- Python

Plan of Project Execution

- The proposed system was implemented using Python Django.
  This Graphical Password can be implemented in authenticating several systems and websites.
- The implementation has few focuses:

• Password: Contain image as reference & encryption algorithm.
• Grids: Contains unique grid values and grid clicking related methods.
• Login: Contains username, images, Graphical password and related methods.
• SSR shield: Contains shield for Shoulder surfing.

As shown in the figure below researchers are trying to stabilize the goal in text based system. However, the text based approach is not able to achieve the goal because as the password strength increases usability

. ADVANTAGES:

-
  - Graphical passwords schemes provide a way of making more human friendly passwords.
  - Here the security of the system is very high.
  - Dictionary attacks and brute force search are infeasible

Flow Graph

Fig.2: Usability VS Security