USING GRAPHICAL PASSWORD Instead Of TYPED PASSWORD

PRESENTED BY

HAMEED MUTLAG FARHAN

MASTER : ECE

STD_NO : 163103474

Outline

- Introduction
- Overview of the Authentication Methods
- Text Password and drawbacks.
- Graphical Passwords.
- The survey
  - ✓Recall Based Techniques
  - ✓Recognition Based Techniques
- Discussion
  - ✓Advantages
  - ✓disadvantages
- Conclusion

Introduction

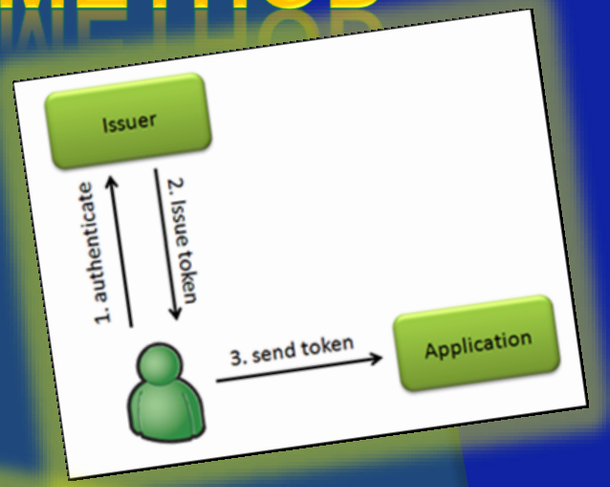
- **What is PASSWORD**

The term **PASSWORD** commonly refers to a secret used for authentication. Passwords are the most commonly used method for identifying users in computer and communication systems.

- **PASSWORDS are used for:**

- ✓ Logging into accounts.
- ✓ Retrieving emails.
- ✓ Accessing applications.
- ✓ Networks.
- ✓ Websites
- ✓ Databases
- ✓ workstations

OVERVIEW OF AUTHENTICATION METHOD



1) Token Based Authentication :

Example : Smart cards , Key cards , ATM

2) Biometrics Based authentication:

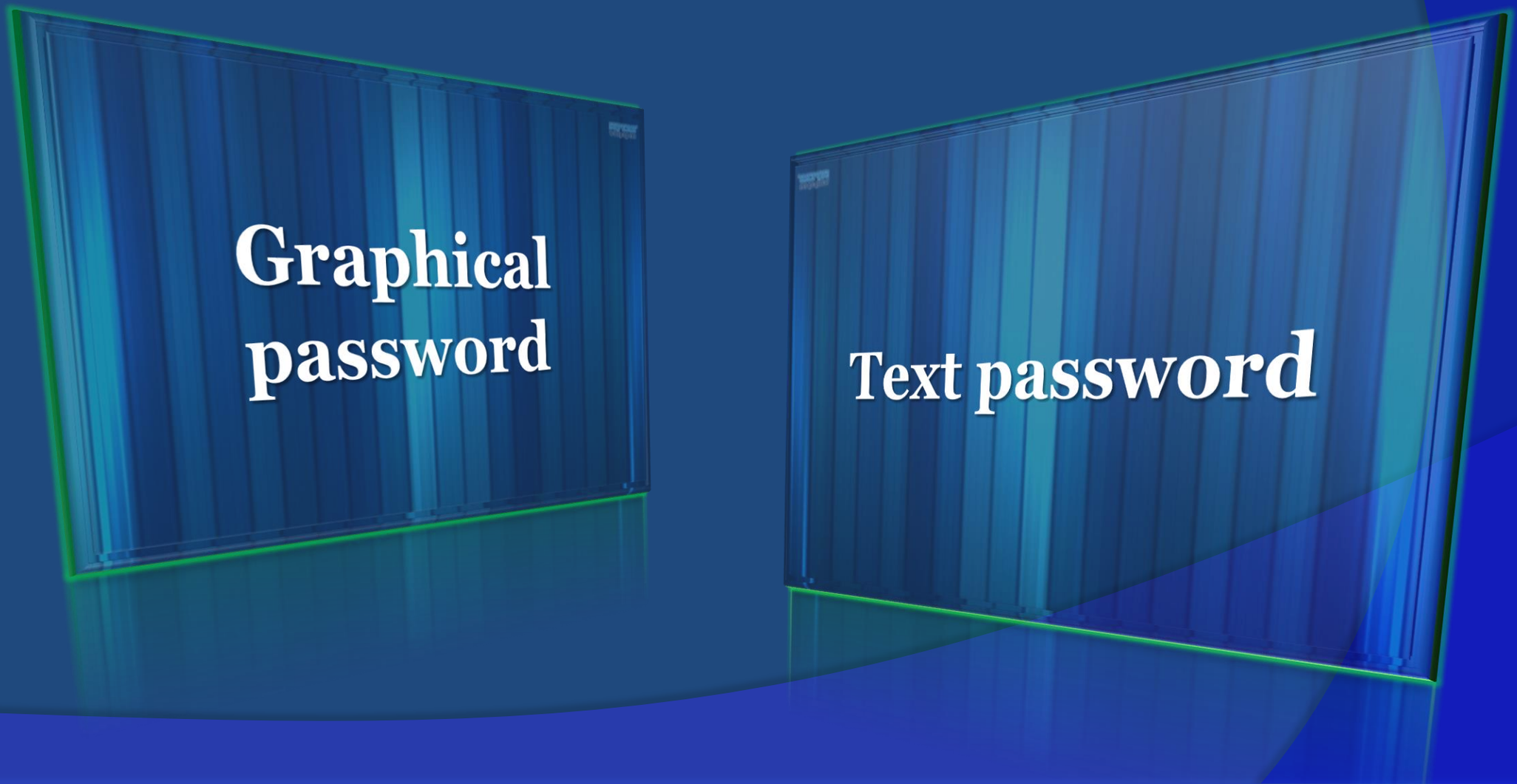
Example: Finger print, Iris scan ,face recognition

3) Knowledge based authentication:

Example: picture based passwords , most widely used authentication techniques.

Types of Password

The are Two Commonly Type Of Password



Text Password

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

Drawback

- Difficulty of remembering passwords.
  - ✓ easy to remember -> easy to guess
  - ✓ hard to guess -> hard to remember
- Vulnerable to attacks like Dictionary attack, Brute force attack .

Many solutions have been proposed. Graphical password is one of the solutions.

Graphical password

- Graphical passwords were originally described by BLONDER in 1996.
- 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 sometimes called graphical user authentication (GUA).

Use of graphical password:

- ✓ Web log-in application.
- ✓ ATM machine.
- ✓ Mobile device.

The Survey: Two Categories

- **Recall Based Techniques**

  A user is asked to reproduce something that he created or selected earlier during the registration stage

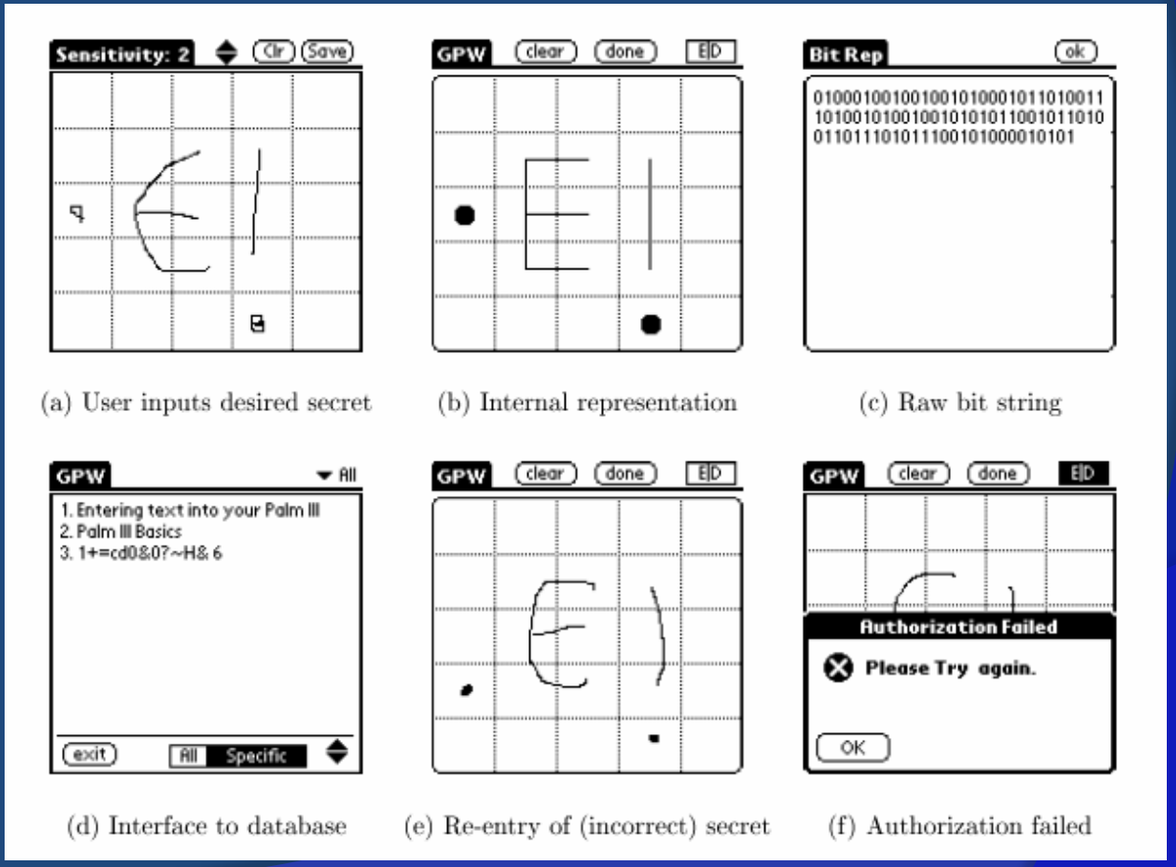
- **Recognition Based Techniques**

  A user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage

Recall based techniques

Draw-A-Secret (DAS) Scheme

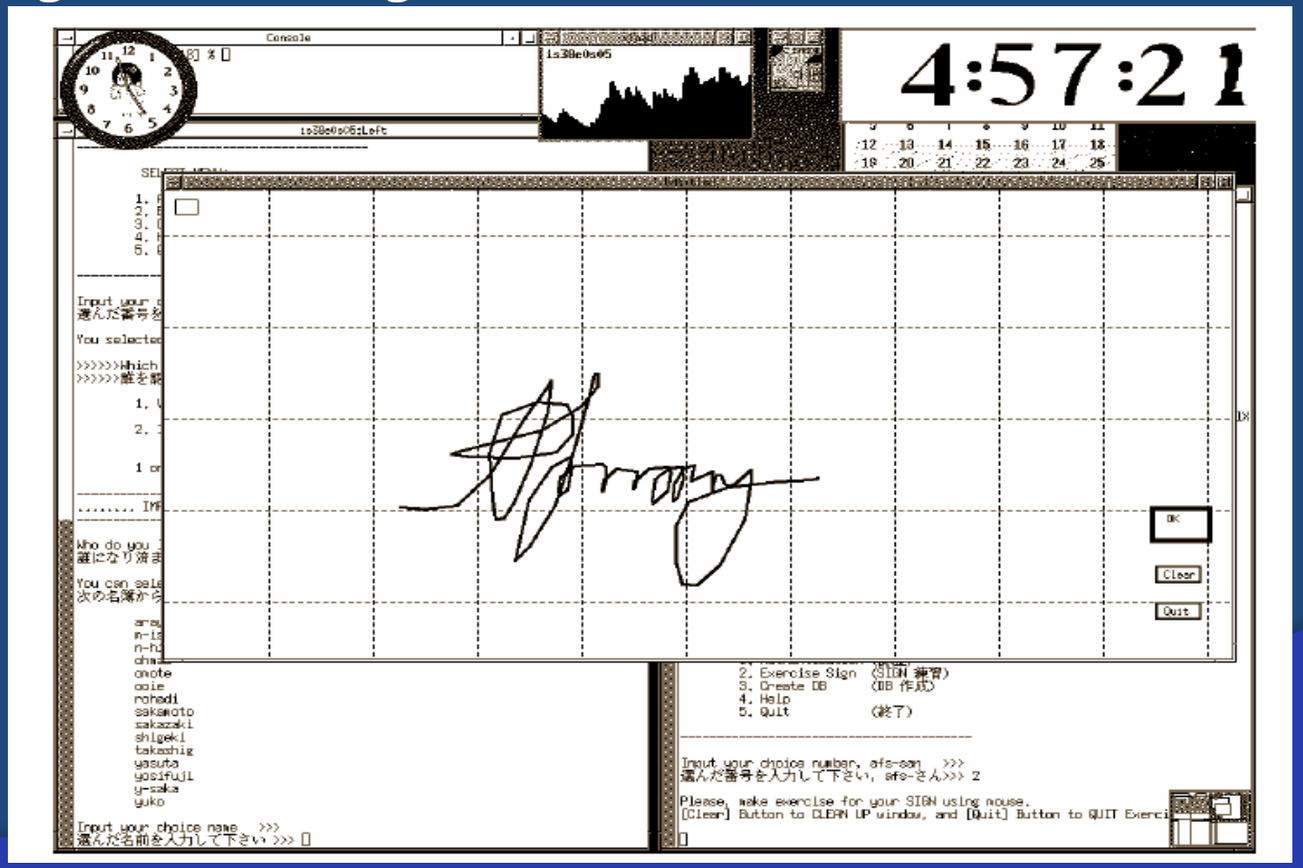
- User draws a simple picture on a 2D grid, the coordinates of the grids occupied by the picture are stored in the order of drawing.
- Redrawing has to touch the same grids in the same sequence in authentication.



Recall based techniques

- **Signature scheme**

  Here authentication is conducted by having the user drawing their signature using a mouse.



Recall based techniques

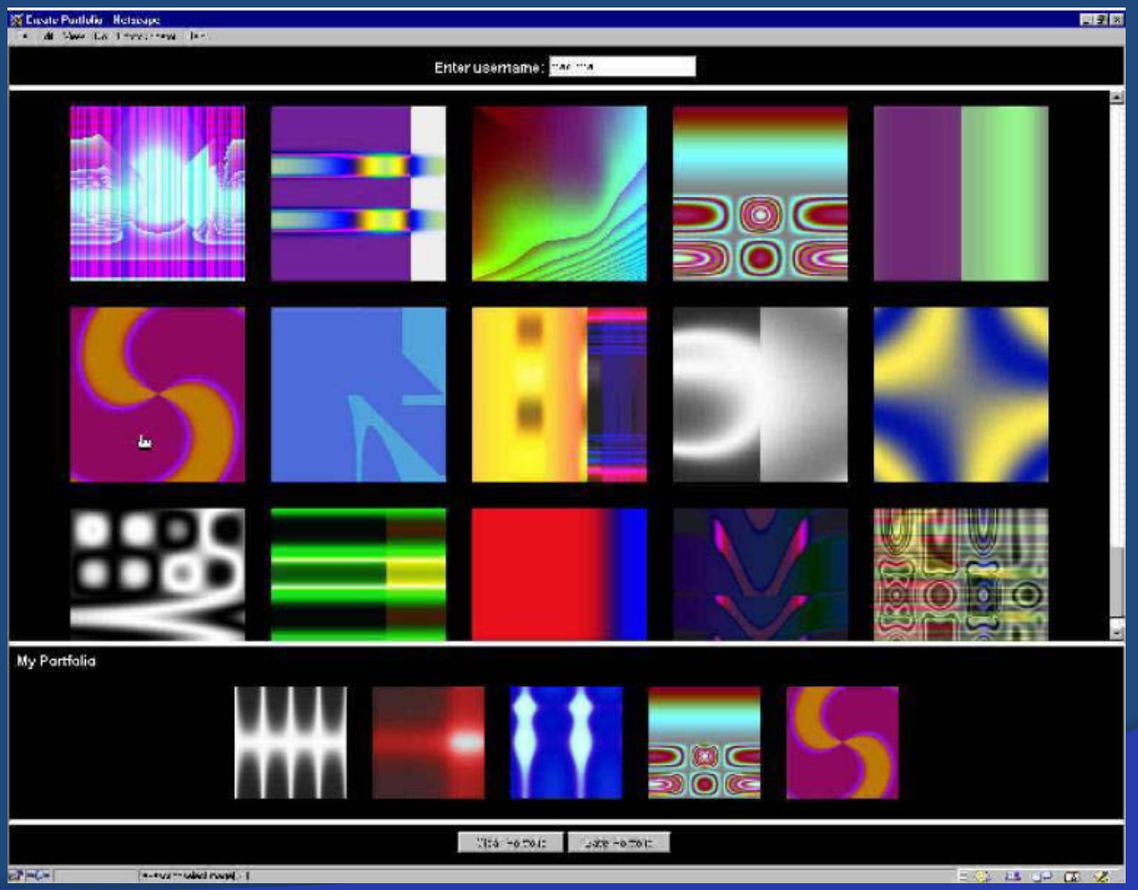
- **Pass Point Scheme**

User click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in the correct sequence.

Recognition based techniques

- **Dhamija and Perrig Scheme**

  Pick several pictures out of many choices, identify them later in authentication.



Recognition based techniques

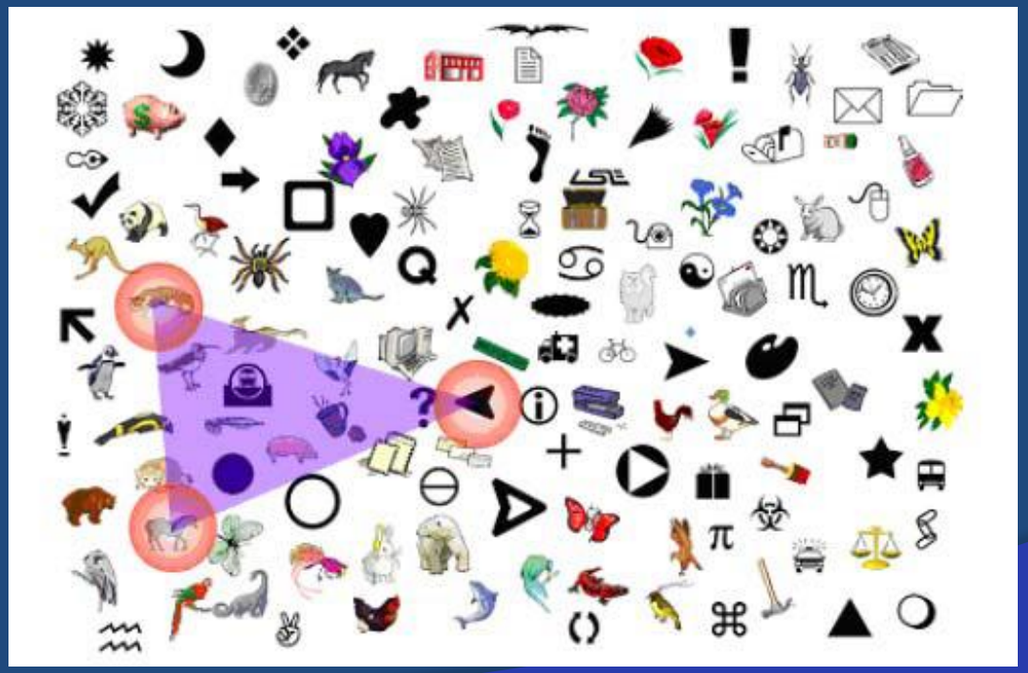
- **Passface scheme:**

In this technique human faces are used as password.

Recognition based techniques

- **Sobrado and Birget Scheme**

  System display a number of pass-objects (pre-selected by user) among many other objects, user click inside the convex hull bounded by pass-objects.



Discussion

- **Advantages of Graphical password**

  - ✓ Graphical password 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.

Discussion

- **Disadvantages of Graphical password**

  - ✓ Password registration and log-in process take too long.
  - ✓ Require much more storage space than text based passwords.
  - ✓ Shoulder Surfing .
    - As the name implies, shoulder surfing is watching over people's shoulders as they process information.

    Examples include observing the keyboard as a person types his or her password, enters a PIN number, or views personal information.

    - Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing.

Conclusion

- Graphical passwords are an alternative to textual alphanumeric password.
- It satisfies both conflicting requirements i.e. it is easy to remember & it is hard to guess.
- By the solution of the shoulder surfing problem, it becomes more secure & easier password scheme.
- Not yet widely used, current graphical password techniques are still immature.


THANK
YOU...
2017