नमस्ते

வணக்கம்

Greetings

Arunesh Gour

22MCI0005

Shailesh Goswami

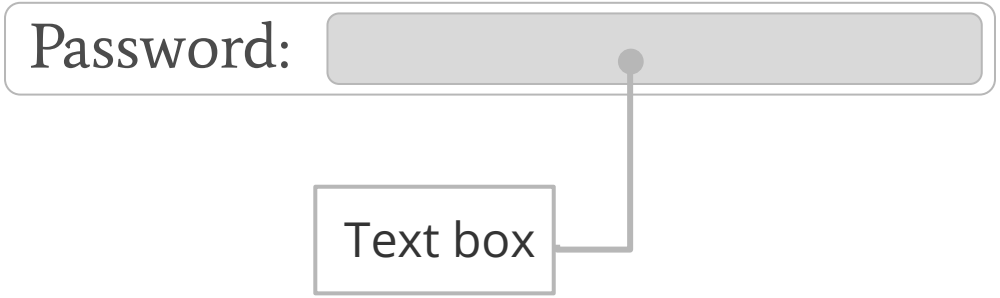
22MCI0007

Cyber Security Domain

Passwords & authentication

Graphical Password Authentication

Passwords


Password:
Text box

Password:

Password: Pa

Password: ****w

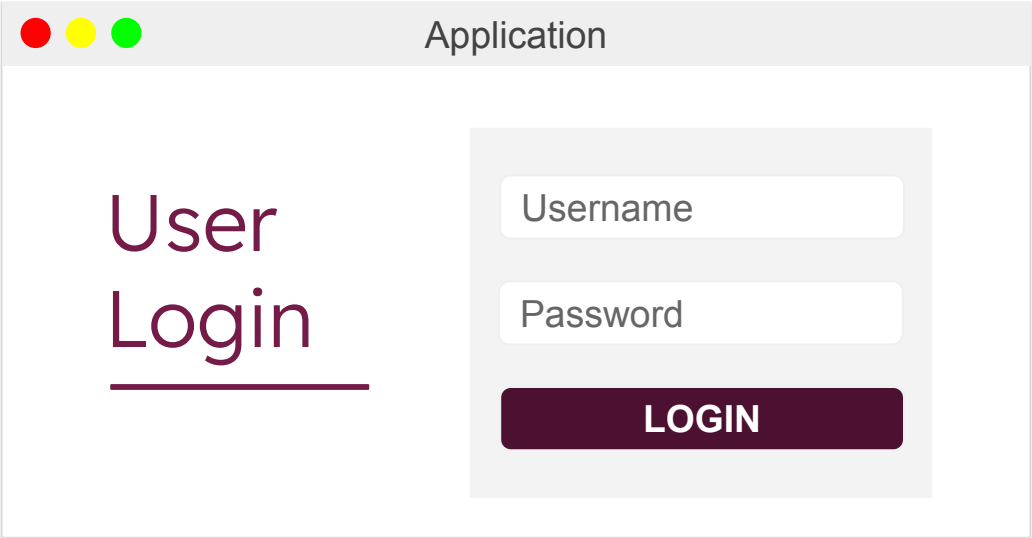
Password: ******r

Password: ********

Advantages

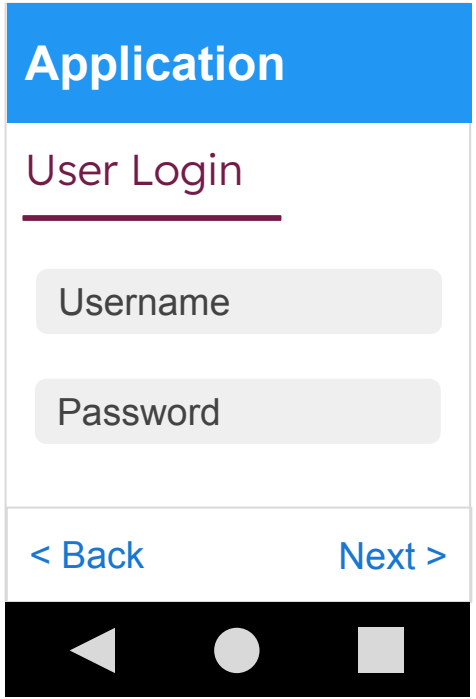
Websites

- Universal



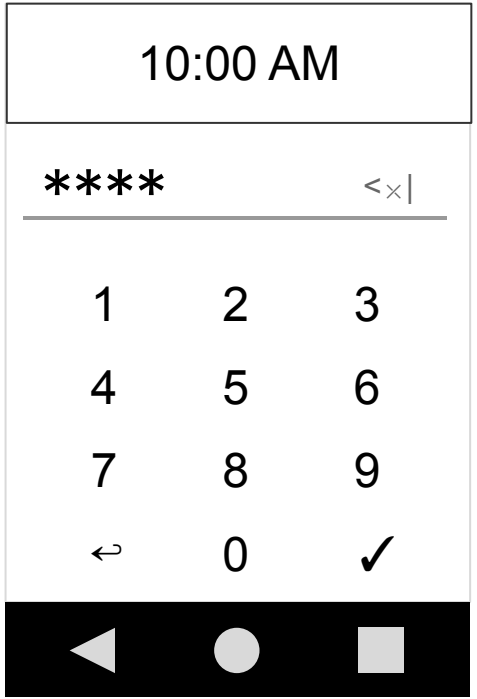
Desktop Applications

- Universal



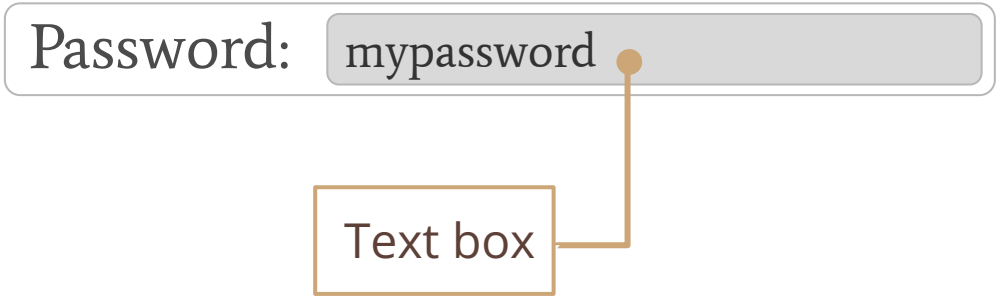
Mobile Apps

- Universal



Device Logins

- Universal



- Easy to use

Password: mypassword

Password: mypassword

- Easy to copy

- Easier to copy

Password: ********

Password: password

- Dictionary attack

Password: ********

A	Z	0	!	#	*	~
a	z	9	@	$	%	.

Password: p@$sw0rd

- Easier to crack

m y P @ s $ w 0 r d !

- Memorization

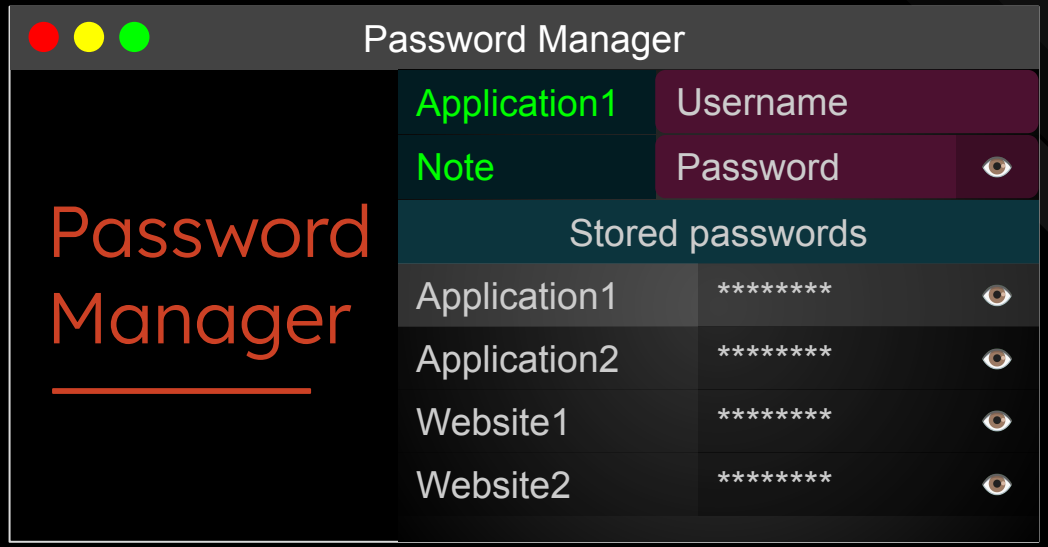
4 5 3 X @ m . s i T E

- Memorization

A	4	#	2	5	p	~	t	1	L	x
4	5	d	E	z	#	5	0	$	%	0

- Memorization

Password Manager



- Tools / Utilities

Text Editor

```
Application1:
    Username
    Password

Application2:
    Username
    Password
```

- Tools / Utilities

- Tools / Utilities

Disadvantages

But, can you …

- Identify your pen

- Identify your pen

- Identify your pen

- Find your shoes

- Find your shoes

Graphical Password Authentication

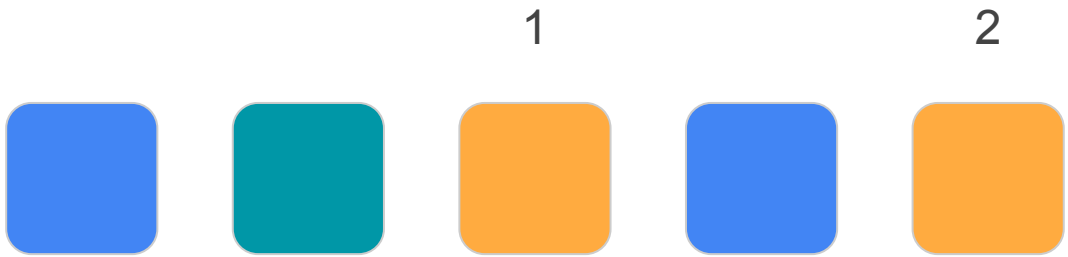
A new and better way to authenticate -)

- Graphics

- Position

- Presence

- Absence



- Count

- Arrangement

Advantages

- Memorization

1 2 5

- Memorization - position

1

2

- Memorization - count

- Shoulder smurfs

- Shoulder smurfs

Colors

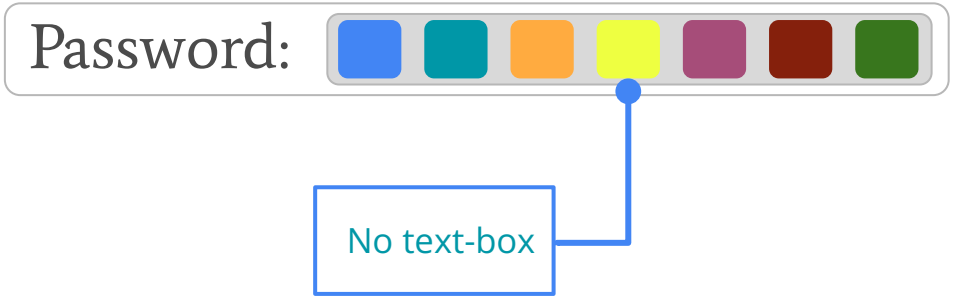
Million +

Shapes

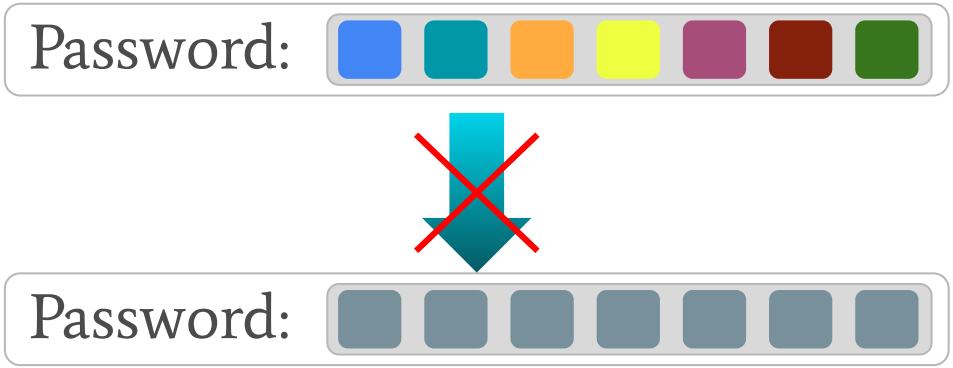
100 +

- Infinite combinations

Limitations

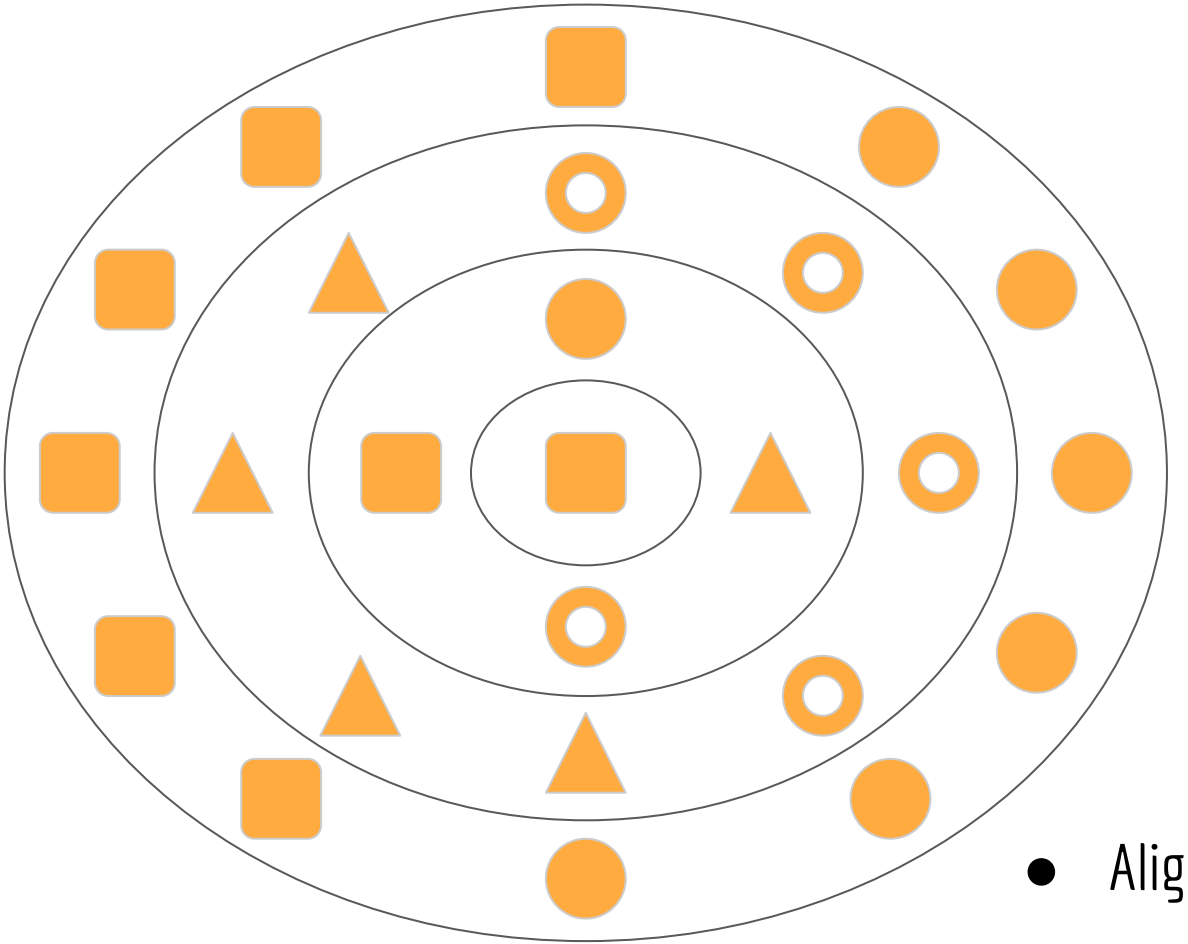


- Complex UI

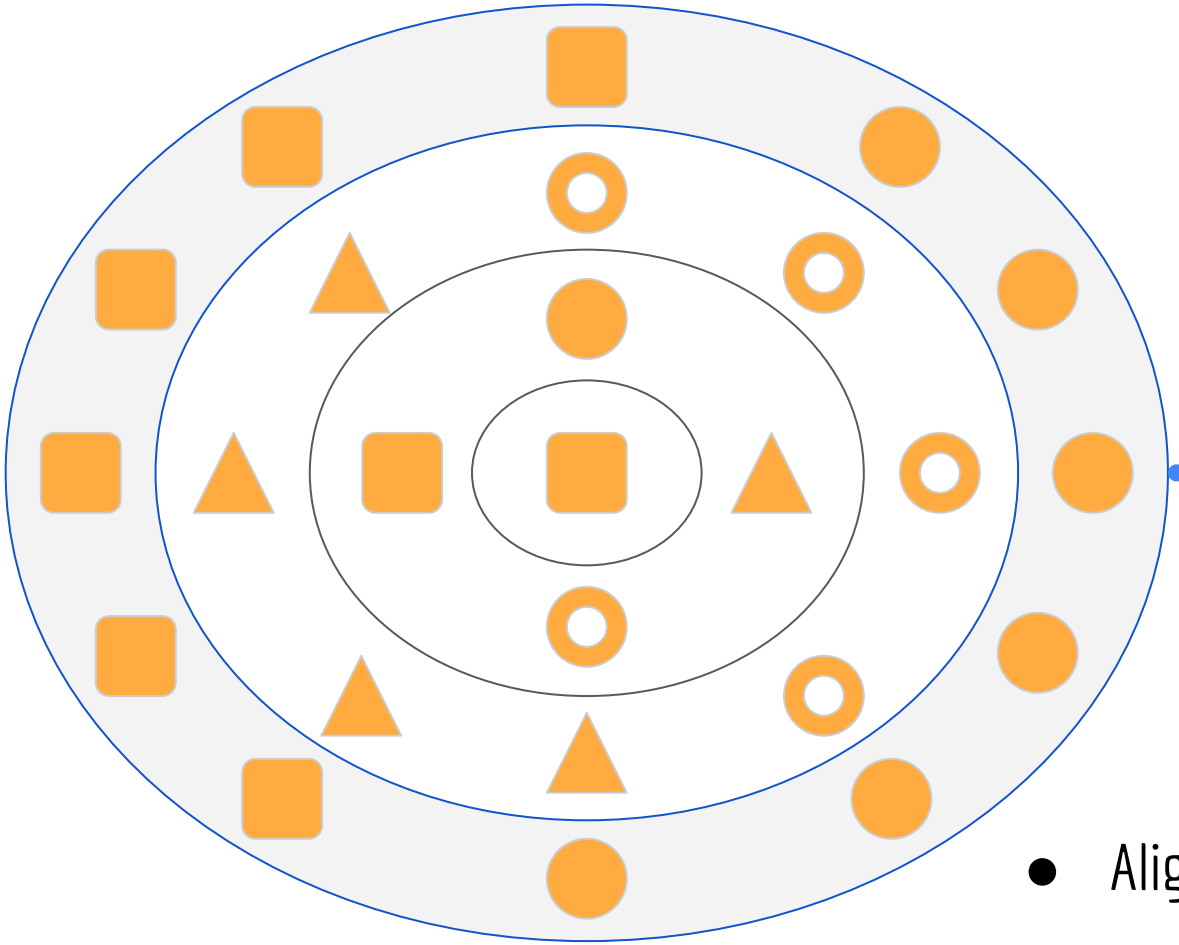


- No copy-paste

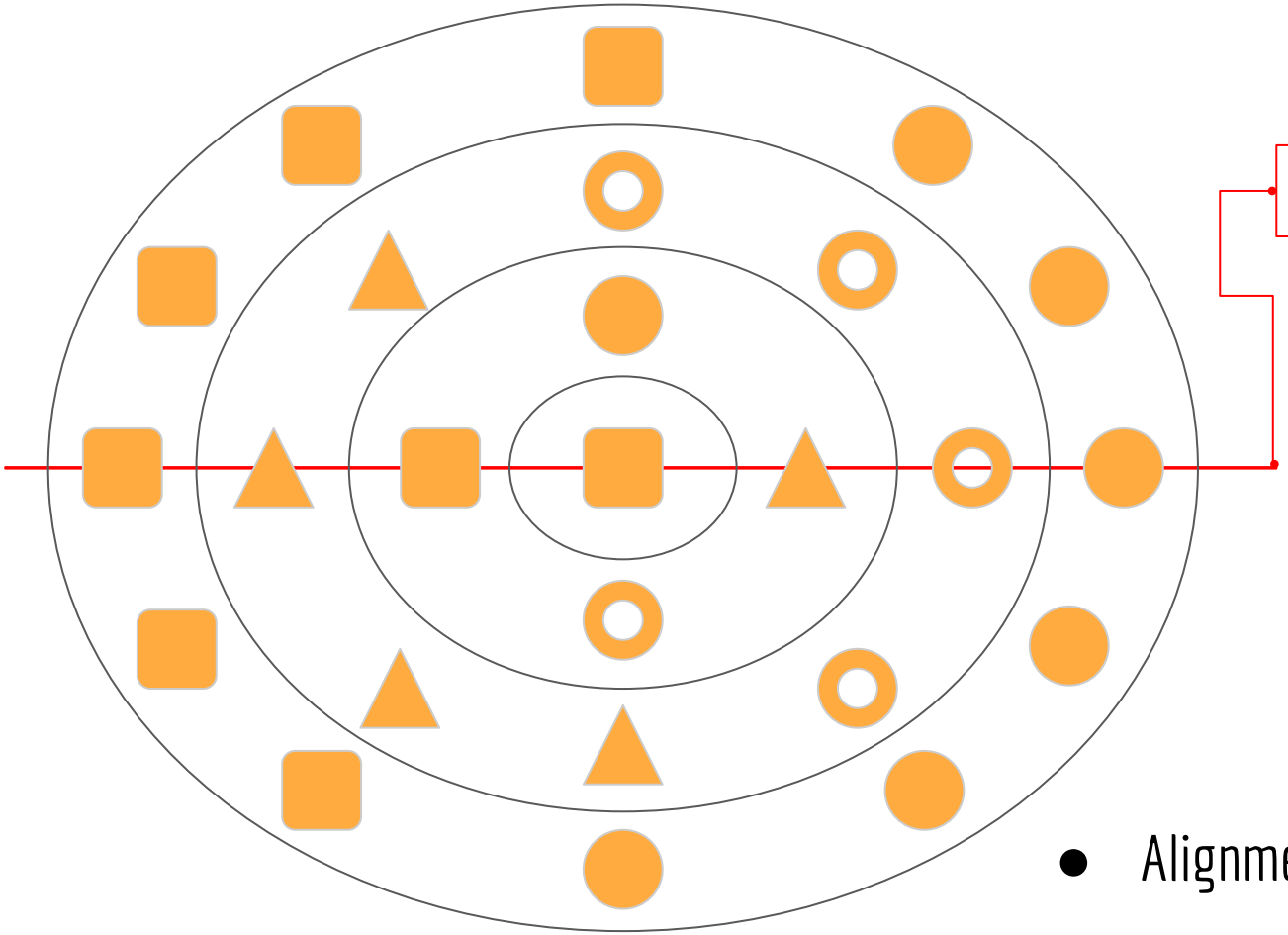
Existing Researches



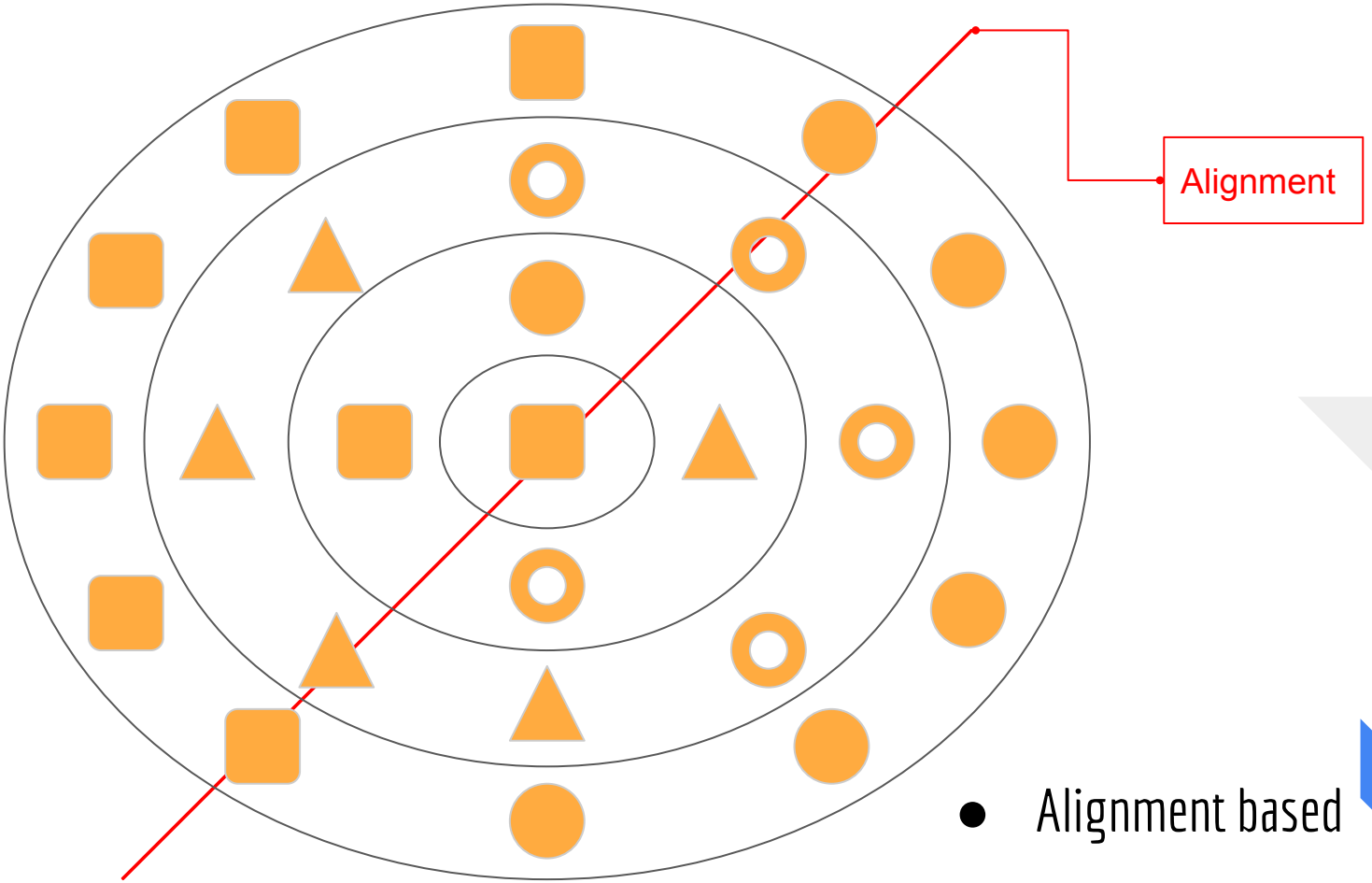
- Alignment based



- Alignment based



- Alignment based



- Alignment based

Level 1

- Presence based

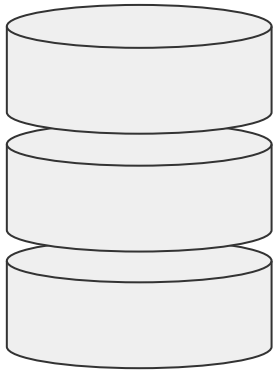
Level 2

- Presence based

Level 3

- Presence based

UI
(User Interface)



DB
(Data Base)

UI
(User Interface)

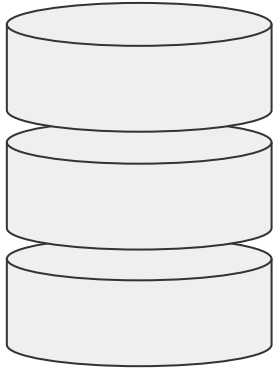
- HTML
- CSS
- JS

- New approach = replace entire UI.
- Linkage errors.
- Change in DB = update UI.

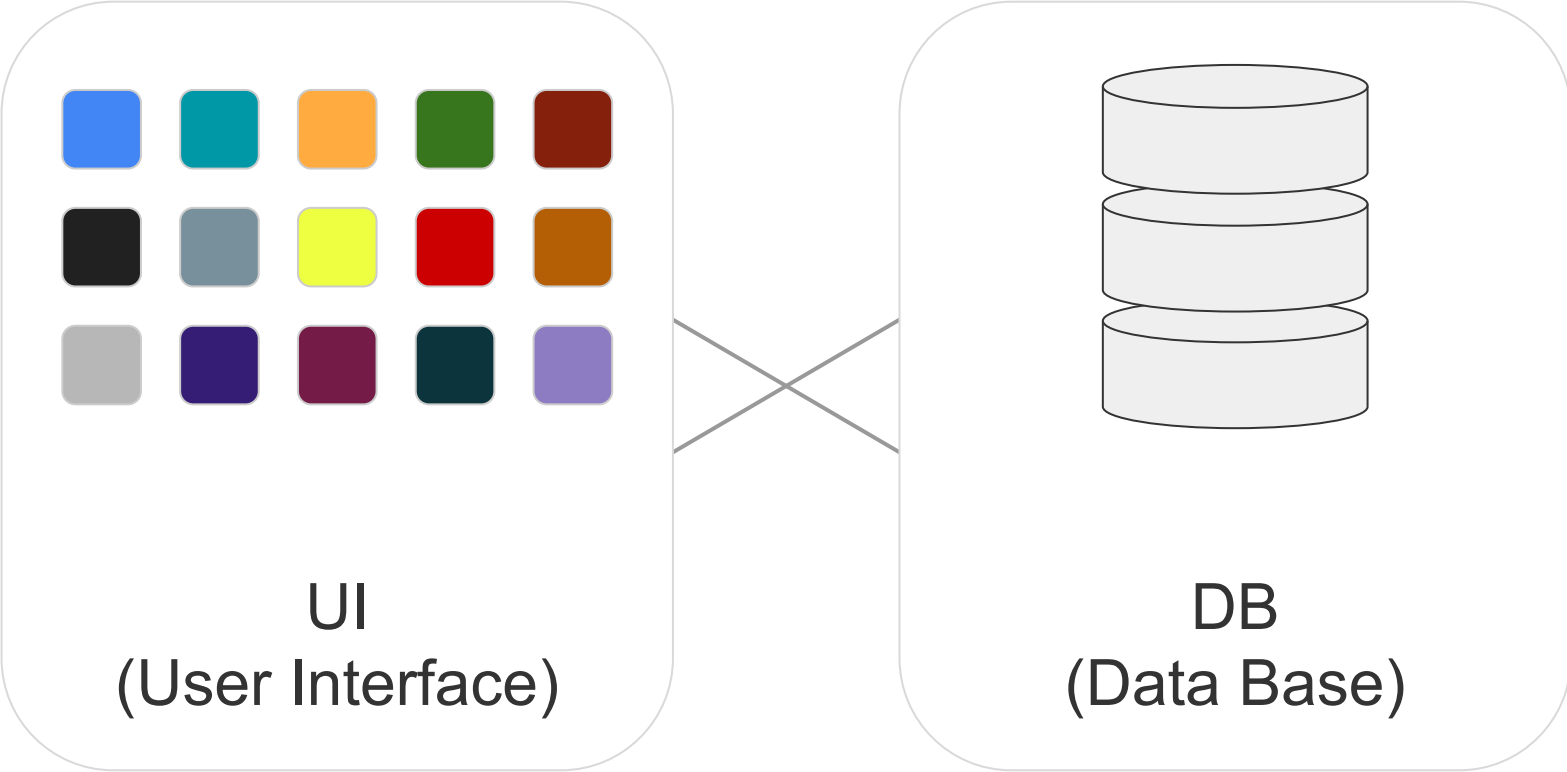
- Python
- Java

- SQL

- Storage formats.
- Authenticating.
- New approach = replace entire backend, DB or both.



DB
(Data Base)


UI
(User Interface)
DB
(Data Base)

Complex UI

User Interface (UI)

<u>is</u>

IMPORTANT !

What if . . .

Abstract

Passwords are universal. They are used in almost all authentication systems. Generally, password refers to text based passwords which are very common. They have their pros and cons. We use passwords almost everytime we want to log in to websites, apps, services, etc. Though this seems very easy and simple task, but for many, this is not. Generally people from non-technical background, life – experienced, mentally challenged and many others find it difficult and complex to use this authentication, be it due to the increasing length and complexity of passwords, inability to remember them, multiple sites requiring password, each one having different rules and policies for password or unable to operate the UI due to complex procedures, so on and so forth. To address such issues, numerous researches have been conducted to replace text – based passwords with graphic based so as to solve this issue. These researches brought numerous designs on the table to make passwords less complex, allowing people to memorize them easily. But in the process, they increased the complexity of the input (or using) to a level that though the concept and benefits are worth it but the UI became a challenge instead. To solve the issue, this paper tries to find and implement a basic, viable and practical mechanism by analysing some of the existing researches.

Introduction

Passwords are a basic yet powerful method for various authentication systems. These are used for various purposes like authenticating a user to a website, application, or service, providing one – time tokens for accessing certain services, securing a database, encryption, cryptography, etc.

Generally, when we talk about passwords, we assume it to be simply text – based, but passwords come in variety depending upon their user interfaces (UI). These are:

- Text – based (something you know).
- Biometric (something you are).
- Physical key (security key) based (something you have).
- Graphic – based (something you know).

Text based passwords

Text – based passwords are universal and most common, basic form of authentication.

These are used everywhere, be it on websites, applications, mobile devices, laptops, old devices, web services, web tokens, etc.

These take input using a text box from frontend and are ready to use directly at the backend.

Biometric passwords

These require the use of special hardware to take user input. User input is in the form of biometric – fingerprint, iris scan, or any other form where the frontend captures user input as a special data, sends it to the backend which processes the input and stores it in another format, and uses different technique to authenticate users.

These are very limited in use owing to the fact that each of these require use of special hardware which itself is expensive based on the requirements.

Security Key

This is a physical key based password where the password is the physical drive itself.

Here, the frontend is the physical interface where the drive mounts to the device which then communicates to the backend of authentication mechanism to prove its identity automatically. Here, the frontend and backend automatically manages the authentication.

But since these keys are very expensive, they are rarely used by general public, even though they are more secure and user friendly.

Graphic based passwords

These are the type of passwords where the user input is taken using images, shapes, or in general graphics. Here, the user picks up images, draws patterns, arranges items, etc based on the mechanism implemented.

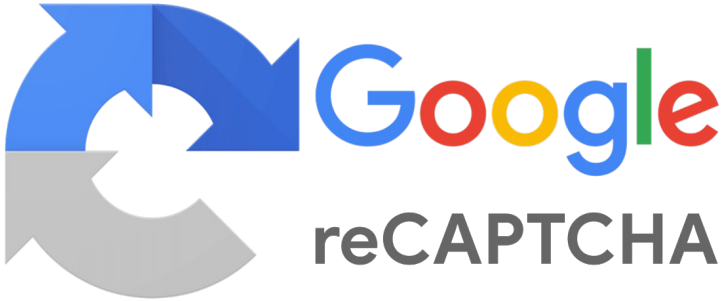
This type of password is easy to remember, shoulder smurf proof, brute force proof, dictionary attack proof, etc, but can be defeated in terms of usability due to its complex user interface.

And so on . . .

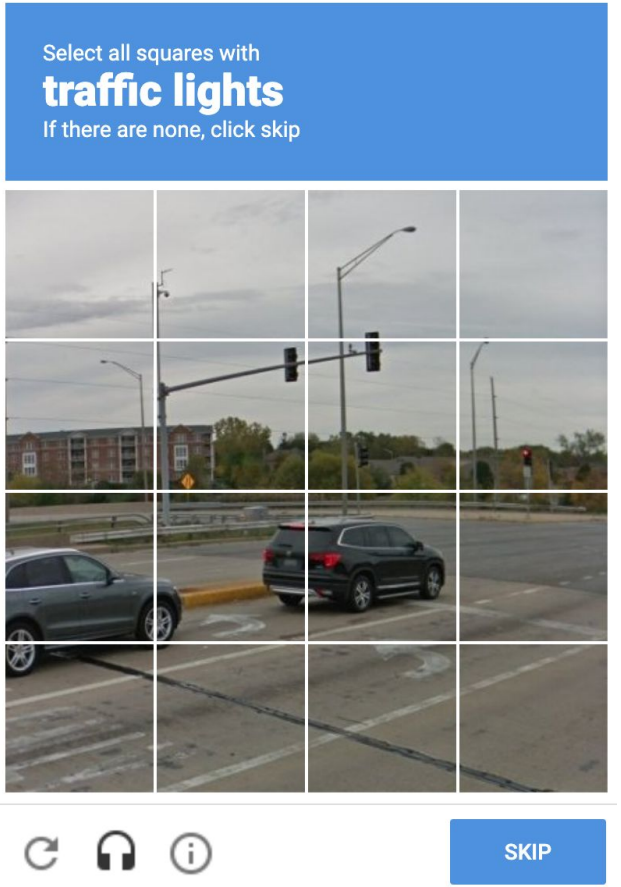
It wasn’t that bad !

Seems good, right ?

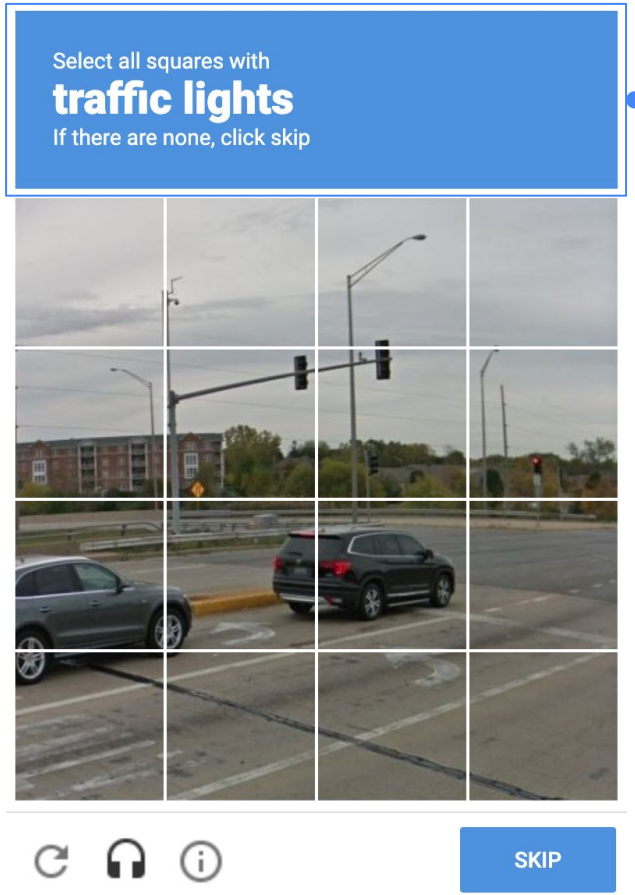
Case study



- reCaptcha

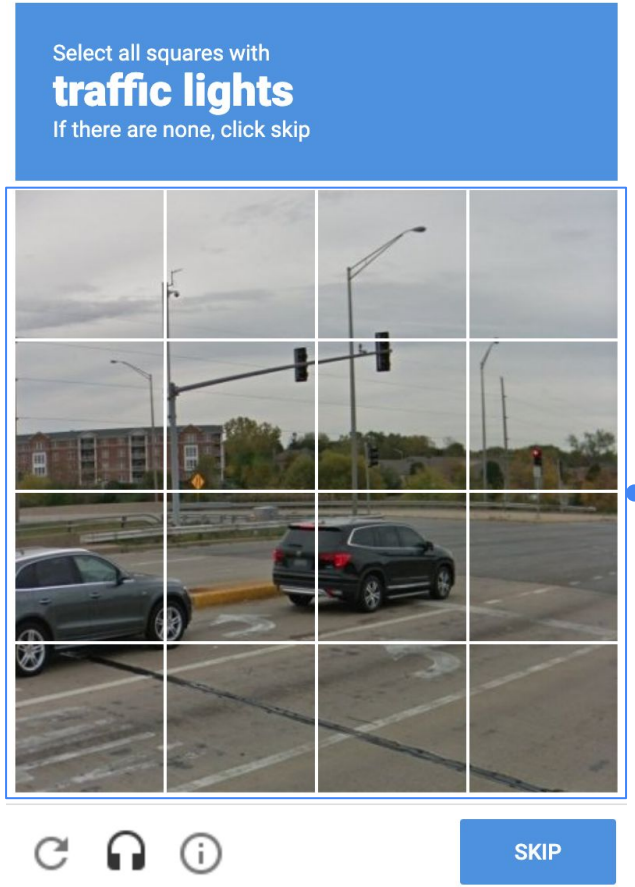

Select all squares with
traffic lights
If there are none, click skip
SKIP

- UI



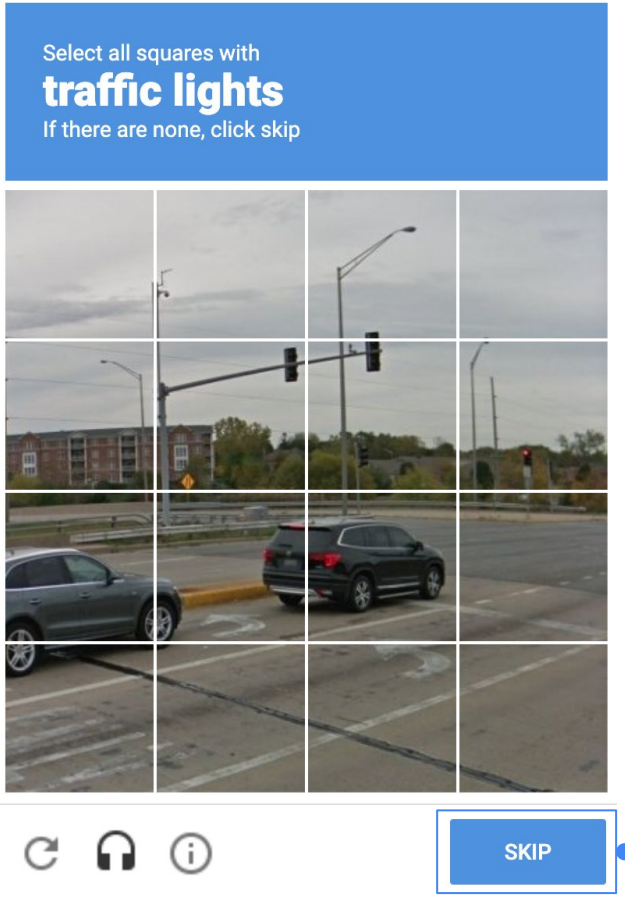
Task / Assignment

- UI



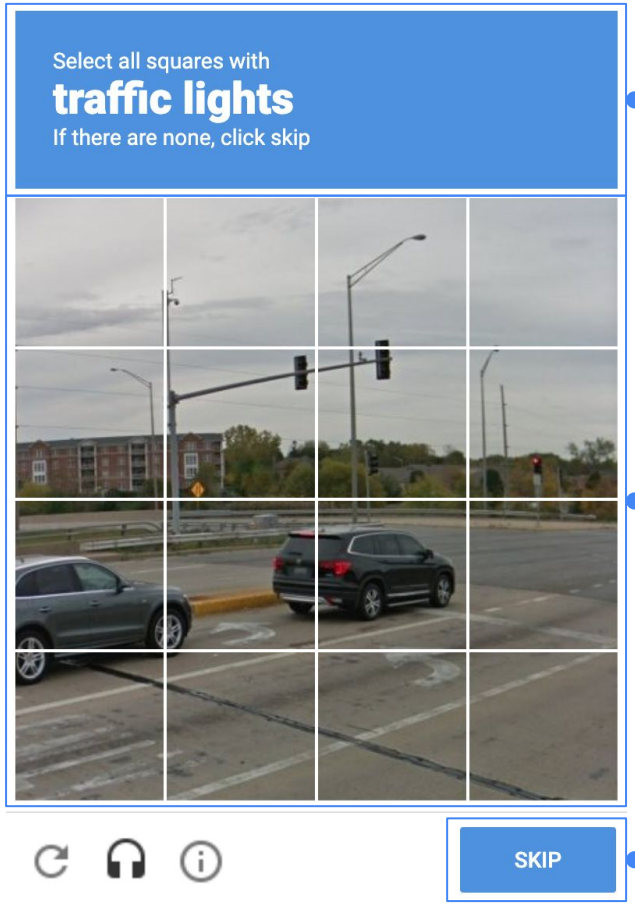
Graphic selector

- UI



Check button

- UI



Task / Assignment

Graphic selector

Check button

- UI

That is it !

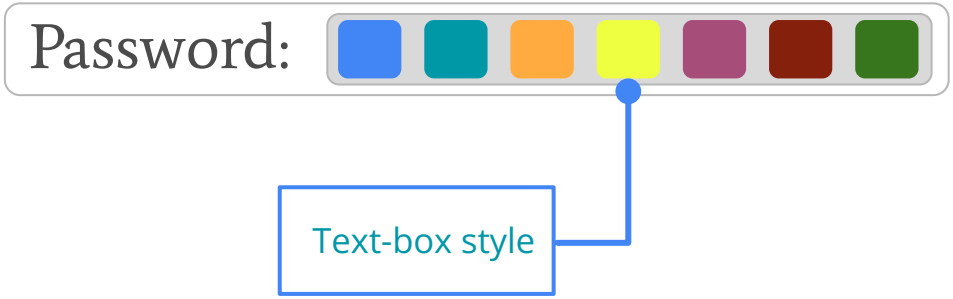
There is no other UI of matching scale in active use today !

We have a

Solution

Introducing

GPA Box

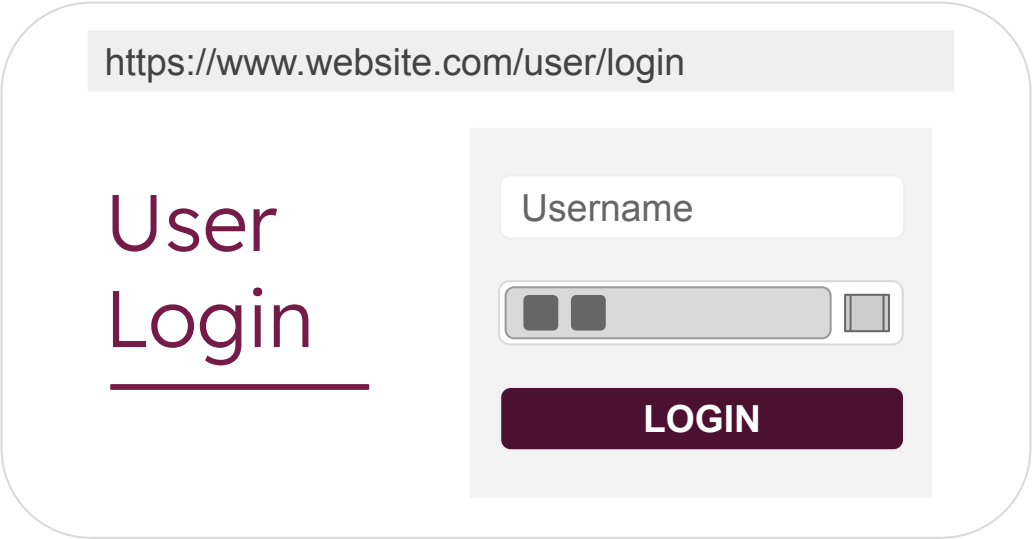


- Simple UI

- Input - Graphics

- Input - Text

- Input - Both



Clutter free UI

- End users

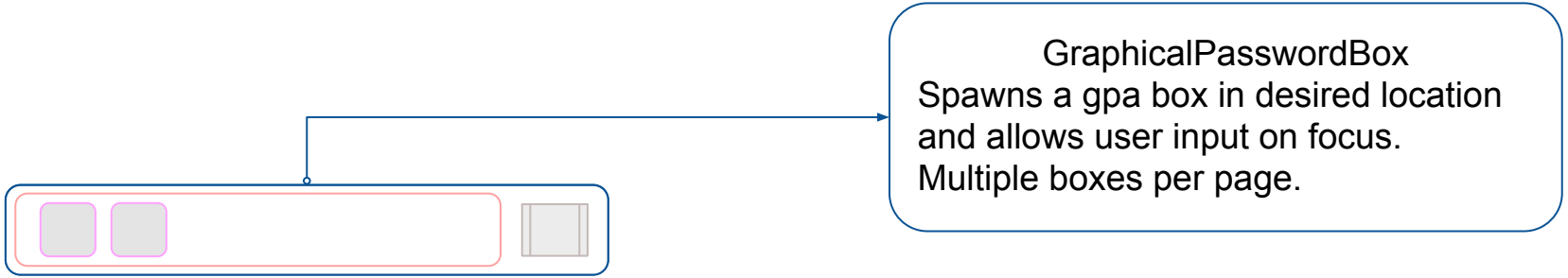
Text Editor

```
1.  # Replace:
2.
3.  <input type="text" />
4.
5.  # with:
6.
7.  <div class="gpa gpa-box"></div>
```

Easy to Implement

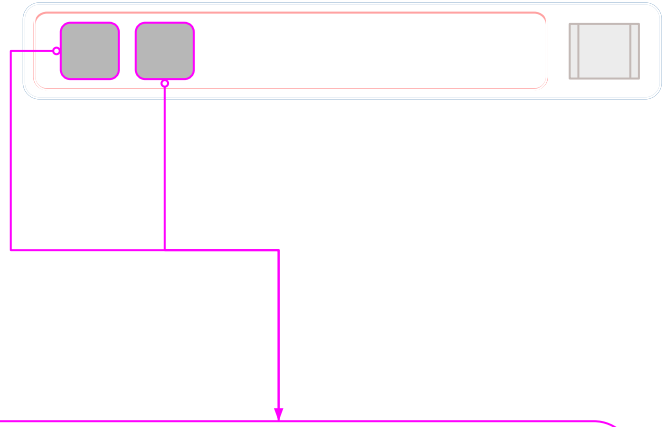
- Developers

Technical details

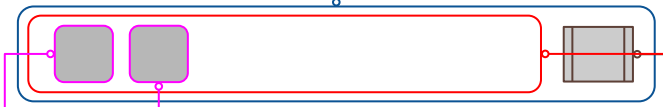

GraphicalPasswordBox
Spawns a gpa box in desired location
and allows user input on focus.
Multiple boxes per page.

GraphicPicker
Spawns a virtual tablet allowing user to choose input for selected gpa box.
Only 1 picker per page.

GPADisplayArea
Designated area in gpa box to display current state of graphical password. One per gpa box.



StateObject
State objects inside GPADisplay area
to show one entry per object.
Multiple objects in GPADisplay area.

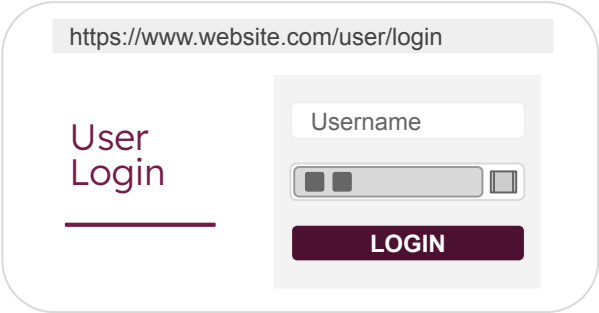


GraphicalPasswordBox
Spawns a gpa box in desired location and allows user input on focus.
Multiple boxes per page.

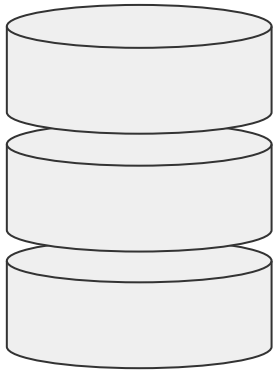
GraphicPicker
Spawns a virtual tablet allowing user to choose input for selected gpa box.
Only 1 picker per page.

StateObject
State objects inside GPADisplay area to show one entry per object.
Multiple objects in GPADisplay area.

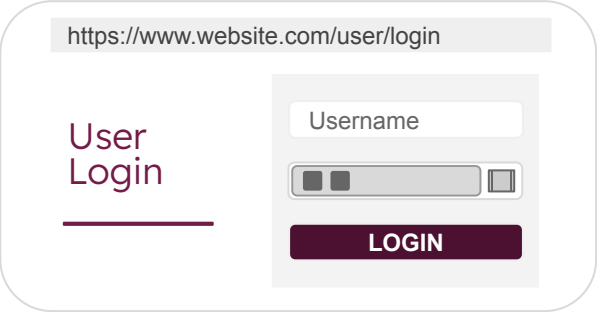
GPADisplayArea
Designated area in gpa box to display current state of graphical password.
One per gpa box.



UI
(User Interface)



DB
(Data Base)



UI
(User Interface)

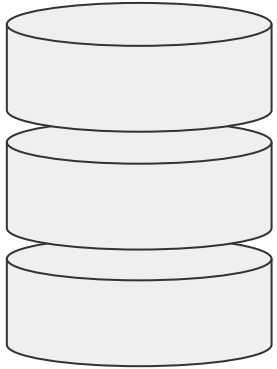
- JS
- CSS
- HTML

- JS API
  - GetPassword
  - SetVisible
  - SetInvisible
  - AddPassword

- Any interface as extension.

- No restrictions !

- Normal passwords.
- Regular Expressions.
- Any algorithm:
  - Alignment.
  - Presence.
  - Absence.
  - Count.



DB
(Data Base)

- Bootstrap 5
- jQuery v3.6

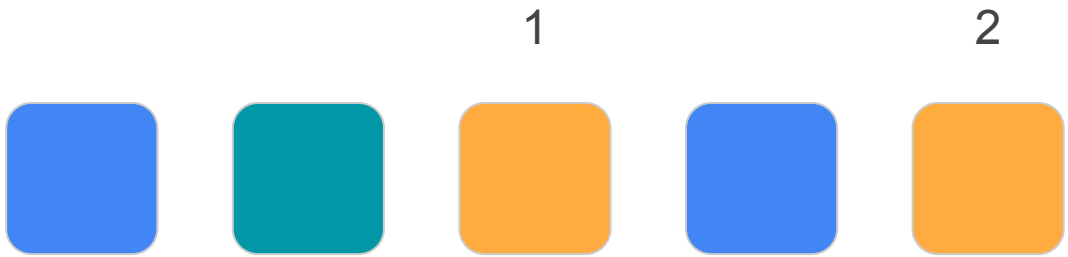
- JavaScript
- CSS 3

Future work

- Position

- Presence

- Absence



- Count

- Arrangement

And lot more as extensions !

Graphical Password Authentication

Thank You