PALAK KHATRI 20BCP031
SHREYA PANENGADEN 20BCP046

Graphical Authentication System

MENTOR:
Dr. Aashka Raval

WHAT ARE

Graphical Passwords

Graphical passwords are a type of **authentication method** that replaces traditional **text-based** passwords with **visual** elements. Instead of entering a sequence of characters, users interact with images, patterns, or gestures to authenticate themselves. This approach offers several benefits over text-based passwords

WHY DO WE NEED

Graphical Passwords

01 Enhanced Security : difficult for attackers to guess or crack using brute-force methods

02 Memorability : easier to remember visual patterns or images compared to complex strings of characters.

03 Usability : more intuitive and user-friendly

04 Resistance to Shoulder Surfing: where someone observes a user entering their password

05 Innovation: enable novel and creative methods of authentication.

BACKGROUND AND RELATED WORK

- One of the major drawbacks with current passwords, both alphanumeric and graphical, is the threat of "watching" attacks: snapshot, remote monitoring, channel interception and shoulder-surfing.
- A person who gets to observe a few login sessions could, depending on the scheme, eventually figure out the password. For instance one can imagine that during an online bank transfer data might be abused by internal bank staff.
- Another scenario could be external attackers that utilize a flaw in the security strategy from the internal staff to get access to private accounts.

GRAPHICAL PASSWORD DEFENCES

01

Draw a secret

A simple picture drawn on a grid when a user first logs in. The system will record each stroke across the grid and in order to pass the authentication, a user must draw a picture similar to the initial one.

02

PassPoint

an authentication system model proposed by Wiedenbeck where a user clicks on sequential pixels set beforehand to authenticate himself

03

Passfaces

Using human face picture as authentication media, basically takes advantage of the fact that human tend to recognize faces much easier. While authenticating a user needs to click a prespecified face pictures and such process repeats itself several times for security enhancement purpose.

LITERATURE REVIEW

- **Draw a secret**
  - Disadvantages:
    - User's habits largely jeopardize its security. Users are more inclined to choose simple patterns easy to guess and at a more central location.
    - User cannot remember the exact stroke order. If user is not familiar with the input devices(mouse, joystick,etc) then the technique is difficult to use.
- **PassPoint**
  - Disadvantages:
    - Most users tend to choose easily identifiable points such as edges or centres of objects, which favours attackers using behaviour analysis to crack the password.
    - Time Consuming: Difficult to memorize the click points, thus number of trials is required for authentication
- **Passfaces**
  - Disadvantages:
    - The system gives a very limited password space which is pretty unsatisfying from security perspective. The system doesn't escape "watching" attacks.

LITERATURE REVIEW

- **Grid Selection Algorithm**
  - Difficult to memorize the click points, thus number of trials is required for authentication
  - Disadvantages:
    - User cannot remember the exact stroke order.
    - If user is not familiar with the input devices(mouse, joystick,etc) then the technique is difficult to use.
- **PIN Entry Methods**
  - Disadvantages:
    - The problem of shoulder surfing arises when an attacker observes the login PIN directly or by using a recording tool, and later reproduces the PIN
- **Dictionary attacks**
  - If the domain of possible selected passwords is not very large (limited to a dictionary), an adversary has the chance to guess all possible passwords and gain an unauthorized access in a reasonable amount of time.
  - To hinder dictionary attacks and to help users remember their passwords, the graphical password is an alternative in which the user is required to remember picture-based information instead of characters

LITERATURE REVIEW

- **Graphical schemes pruposed by Sobrado and Birget**
- The user is presented with a screen full of hundreds or more graphical objects, randomly distributed each time they are displayed, and must identify the objects that compose the password. To avoid disclosing the password information to an observer, the user does not select the password objects themselves, but instead must click anywhere within the convex hull of the triangle formed by a triplet of objects. Because the number of possible triangles far exceeds the number of objects on the screen, the observer has obtained very little, if any useful information about the actual password just by knowing the clicked location.
- **Disadvantages:**
  - If the number of graphical objects is large, the user will spend a long time searching for the objects that compose the password.
  - If the randomly distributed objects that make up a given password screen are all clustered in a corner of the screen, the convex hull of the triangle will be small and relatively close to the corner of the screen. Additionally, the number of possible triplets associated with that clicked location may be small, which would make it easier to guess the triplet.

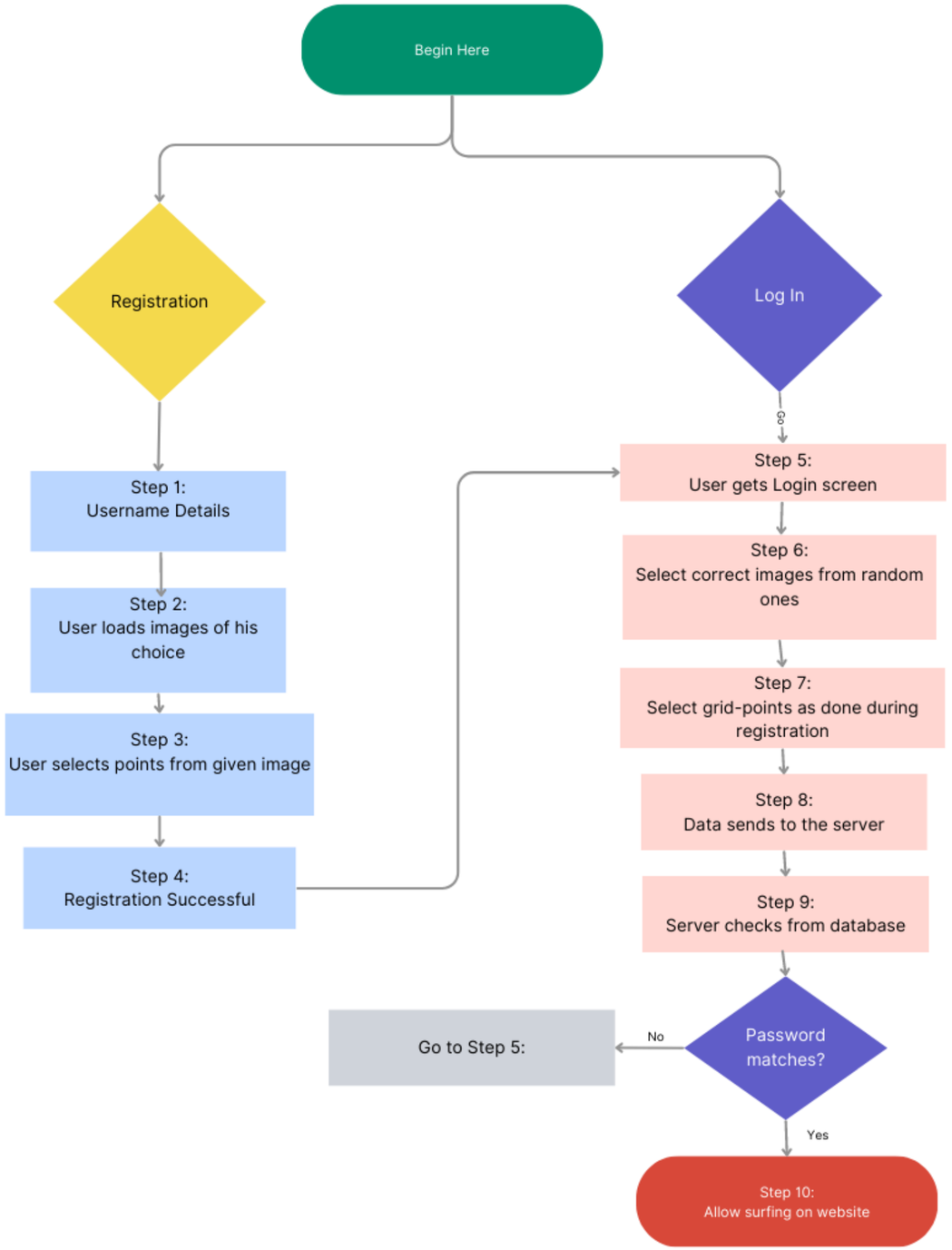
Problem Statement

RESEARCH GOAL

This research seeks to address the challenges faced by graphical password authentication systems and advance the state of the art in this field. By investigating techniques to enhance security against "watching" attacks, optimizing usability, diversifying pattern selection, developing effective user training strategies, and ensuring compatibility, this study aims to contribute to the creation of robust, user-friendly graphical password authentication systems that offer an improved balance between security and user experience. Ultimately, the research endeavors to provide practical solutions that align with evolving cybersecurity needs while meeting user expectations and requirements.

METHODOLOGY

- Dynamic Image Selection Authentication : Images change positions and contents per login attempt.
- Point selection Authentication : Users select three points on a registered image.
- Account Lockout and OTP recovery : Consecutive failed attempts lead to account lockout. also,Users receive OTP via email for account unlock.
- Time Limit Enforcement : time limit contributes to both security and user experience.



ARCHITECTURE

FINDINGS

01 Dynamic image selection approach effectively countered shoulder surfing attacks.

02 After every wrong attempt in the first authentication level, the dynamic image selection options are designed to increase in complexity.
This deliberate increase in difficulty serves as a deterrent to attackers attempting to guess or brute-force their way into the system.

03 Attackers cannot rely on observing a fixed pattern, as the dynamic nature of the image grid makes prediction difficult.

04 Balancing Usability and Security: While enhancing security, we have carefully balanced the usability aspect by ensuring that the complexity increase remains manageable for genuine users.

05 While enhancing security, we carefully balance the usability aspect by ensuring that the complexity increase remains manageable for genuine users.

CONCLUSION

- Balancing Security and Usability
- Enhanced Security Measures
- User Centric-Approach
- Usability and User Satisfacition
- Real world implications

- Our multi-layered authentication system strikes a successful equilibrium between robust security measures and user-friendly experiences.
- The incorporation of dynamic image selection, point selection, and adaptive difficulty mechanisms results in a multi-faceted authentication approach that elevates protection while ensuring user convenience.
- Organizations that choose to embrace this multi-layered authentication approach position themselves at the forefront of user-centric security trends, fostering greater user confidence and trust, ultimately enhancing digital interactions in an ever-evolving digital environment.
- The transformative potential of our authentication system reverberates not only in its direct impact on security but also in its capacity to reshape perceptions of cybersecurity, driving us closer to a safer and more user-centered digital future.

FUTURE RESEARCH

- Refining Adaptation:
  - Fine-tuning adaptive mechanisms based on user behavior patterns.
- Biometrics Integration:
  - Exploring biometric factors like fingerprints to enhance security.
- User Perception Study:
  - Investigating user satisfaction and perceptions of the multi-layered approach.
- Cross-Platform Compatibility:
  - Extending the system's usability across different platforms and interfaces.
- Behavior Analysis with Machine Learning:
  - Utilizing machine learning for deeper insights into user behavior.

REFERENCES

- A Graphical Password Scheme against Snapshot, Remote Monitoring, And Shoulder-surfing with Its Application in One-Time Password - Zuejia Lia
- Comparison of Graphical Password Authentication Techniques - Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle
- Graphical passwords - Leonardo Sobrado and Jean-Camille Birget
- A systematic review of PIN-entry methods resistant to shoulder-surfing attacks - Farid Binbeshr, M.L. Mat Kiaha , Lip Yee Por , * , A.A. Zaidan
- Shoulder surfing: From an experimental study to a comparative framework - Leon Bošnjak, Boštjan Brumen
- Novel shoulder-surfing resistant haptic-based graphical password - M. Orozco, Abdulmotaleb El Saddik
- Screen oriented technique for reducing the incidence of shoulder surfing - Bogdan Hoanca, Kenrick Mock
- Security and User Interface Usability of Graphical Authentication Systems - Hassan Umar Suru , Pietro Murano
- A Survey of User Authentication Based on Mouse Dynamics - Kenneth Revett, Hamid Jahankhani, Sérgio Tenreiro de Magalhães & Henrique M. D. Santos
- BlindLogin: A Graphical Authentication System with Support for Blind and Visually Impaired Users on Smartphones - Yean Li Ho, Bachir Bendrissou, Afizan Azman and Siong Hoe Lau

“

THANK YOU

PRESENTED BY
PALAK KAHTRI - 20BCP031
SHREYA PANENGADEN - 20BCP046