Usable Security and Privacy Application Analysis Paper

Analyzing Method to Resist Shoulder-Surfing

- **Paper Source:**

  https://dl.acm.org/doi/abs/10.1145/1133265.1133303

- **Paper Title:**

Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme.

- **Studied by:** Hanadi Asfour

- **Date:** 20/12/2023

1. Summarize the main goals presented in the paper.

Before entering the main goals of this paper, the reader must know what CHC means (Convex Hull Click Scheme). CHC is a graphical password system that employs challenge-response authentication using a set of pass-icons displayed in a window. To authenticate, the user must recognize and click within the convex hull formed by a subset of pass-icons.
Source: [Page 3, lines 38~49, left-side].

The main goals of the CHC scheme, as presented in the paper, are summarized below:

A. Resisting the problem of shoulder-surfing: The primary goal of CHC is to guard against shoulder-surfing attacks, whether through human observation, video recording, or electronic capture. That is by introducing a challenge-response paradigm that requires users to recognize and interact with pass-icons within a convex hull.
Source: [Page 3, lines 39~41] & [Page 3, lines 46~49, left-side].

B. Implementing usability by optimizing user experience: CHC is designed to be user-friendly and engaging. Moreover, it emphasizes the importance of creating a fun, game-like environment to motivate users to log in quickly and accurately. The goal was to balance security with positive user experiences, fostering a sense of interest and speed during the authentication process.
Source: [Page 3, lines 52~53, left-side] & [Page 4, lines 17~21, right-side].

C. Increasing password security: CHC aims to provide a high level of security by allowing customization of the password space. Moreover, security can be increased by adjusting factors such as the number of icons, pass-icons, and rounds of challenges. This way, brute-force attacks are infeasible as they require far too much memory.
Source: [Page 4, lines 30~34, right-side] & [Page 4, lines 36~42, right-side]

2. Is the topic of this paper relevant in today's digital environment, and why?

Yes, this paper's topic is highly relevant in today's digital world. Because technology is integrated into our daily routines, protecting personal data—whether for banking or chatting online—is very crucial. Moreover, as cyberattacks get smarter, there is a growing realization that traditional passwords have limitations. Exploring new, user-friendly ways to stay secure is necessary. The CHC's approach to solving the shoulder surfing problem is both safe and user-friendly.

For instance, in today's work environments, where individuals often find themselves working in crowded places like coffee shops or co-working spaces, the CHC scheme's graphical password system becomes relevant. In other words, the ability to authenticate securely in such settings, where the risk of shoulder-surfing is higher, aligns with the practical challenges faced in modern work scenarios.

3. Identify and discuss the key challenges mentioned in the paper regarding usable security and privacy.

- Identifying Problems:

	Challenge	Source
1	Longer time to input password	Page 7, line 12, left-side
2	Security risks due to user behaviors	Page 7, line 20, right-side
3	Icon visibility and distinctiveness	Page 7, line 30, right-side
4	Balancing between security and usability	Page 7, line 42, left-side

- Discussion:

1) <u>Longer time to input password:</u>

The time-intensive nature of scanning the window for pass-icons and forming the convex hull causes a delay in the authentication process. This problem is particularly evident in busy environments, such as airports, where users may encounter delays in accessing devices using the CHC scheme.

To address this, one can develop algorithms to optimize the arrangement of icons, making it more intuitive for users to locate and select pass-icons efficiently, which gives faster login times while maintaining the level of security.

2) Security risks due to user behaviors:

Users' insecure behaviors when interacting with the CHC scheme can impose security risks. This is done when one quickly inputs passwords and clicks very near a pass-icon or traces -with their cursor- the convex hull they imagined. These actions could be common among newbies and rushed users.

To prevent this, a user education program can be developed to emphasize security and encourage correct behaviors, in addition to revealing the potential risks associated with poor system interactions.

3) Icon visibility and distinctiveness:

The icons designed for the CHC scheme had a uniform shape and were small (to display it on the screen), which made the pass-icons very hard to distinguish and presented a usability challenge. This becomes an issue in scenarios with poor visibility, such as low-light environments, as users will struggle to distinguish between similar-looking icons, leading to an increase in authentication errors.

Potential solutions include design enhancements to improve icon visibility, such as varying sizes, shapes, and colors. Allowing users to customize icon sets could also contribute to better recognition.

4) Balancing between security and usability:

There are conflicting design goals between enhancing security and providing a positive user experience, one must find the optimal balance in the CHC scheme. Moreover, introducing highly secure measures can be great in terms of security, however, it discourages users from adopting the system due to its complexity.

Finding the balance between usability and security can be done by performing usability studies to gather user feedback. This can help identify the best alternative designs that maintain security without sacrificing its usability.