GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

The journal is indexed in
EBSCO

ISSN 2545-4803 on line
DOI: 10.46763/BJAMI

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI)

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS

YEAR 2024

VOLUME 7, Number 2

AIMS AND SCOPE:
BJAMI publishes original research articles in the areas of applied mathematics and informatics.

Topics:
1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS
(BJAMI), Vol 7

ISSN 2545-4803 on line
Vol. 7, No. 2, Year 2024

EDITORIAL BOARD

CONTENT

Balkan Journal of Applied Mathematics and Informatics Online ISSN 2545-4083
Volume 7 Number 2 Year 2024 UDC:004.382.76.056.523:004.353.2-043.5

MULTI-ACTION GRID AUTHENTICATION: A SECURE AND USABLE AUTHENTICATION SYSTEM FOR SMART TOUCH DEVICES

DARKO CEBOV AND ALEKSANDRA MILEVA

Abstract. In the digital age, securing smart touch devices is of paramount importance to safeguard sensitive information. Traditional graphical password systems, while convenient, remain vulnerable to attacks such as shoulder surfing and smudge tracing. This paper introduces a novel multi-action grid authentication system that enhances security while preserving ease of use. The system allows users to authenticate by performing two actions—tapping and replacing—within a 3x3 grid. Through iterative development and testing, the method shows significant improvements in preventing common security threats while maintaining high user satisfaction. A thorough analysis of password space is also conducted, demonstrating the system's robust resistance to brute-force attacks. Our findings suggest that this multi-action approach offers a secure, efficient alternative to existing graphical password systems.

1. Introduction

The rapid advancement of smart touch devices necessitates increasingly sophisticated methods of user authentication. Traditional password systems, such as alphanumeric and PIN-based authentication, are prone to various vulnerabilities, including dictionary attacks, shoulder surfing, and smudge attacks. Graphical passwords were introduced to address these limitations, as images are often easier for users to remember and more challenging for attackers to guess. However, these systems are not without flaws, particularly in environments where visual privacy cannot be maintained.

This paper introduces a multi-action grid authentication system that aims to mitigate these issues by incorporating two simple yet secure actions: tapping and replacing. By allowing users to perform a sequence of these actions within a 3x3 grid, the system increases the difficulty for attackers to replicate the authentication process through observation or inference. The random positioning of grid points further enhances security, ensuring that each authentication attempt is unique.

In this paper, we describe the development of this system through an iterative design process, incorporating user feedback and security testing at each stage. We also analyze the system's effectiveness in preventing common security attacks, such as shoulder surfing and smudge tracing, and evaluate its usability through user testing. Finally, we calculate the potential password space generated by this method, demonstrating its superior resistance to brute-force attacks compared to traditional systems.

The rest of the paper is structured as follows. Section 2 reviews the related work, while Section 3 is devoted to the description of the proposed authentication system. Section 4 analyzes the size of the password space and security in general, while Section 5 is about usability testing. Discussion is presented in Section 6, and the concluding remarks are made in Section 7.

2. **Related Work**

Graphical authentication methods emerged as an alternative to traditional text-based passwords, leveraging the human ability to recall visual information more effectively. Over the years, several graphical authentication methods have been developed, each aiming to balance security and usability. These methods can be broadly categorized into recognition-based, recall-based, and cued recall methods, as described by Biddle et al. [4].

Recognition-based methods involve users identifying and selecting images or objects previously chosen during registration. One notable example is the technique proposed in [2], where users log in by recognizing a combination of images from a 25-image grid. Each session dynamically rearranges the images, adding a layer of security against attacks like shoulder surfing. However, the system's complexity can hinder usability, especially for infrequent users.

Another hybrid approach is GRA-PIN [1], which combines graphical passwords with PIN-based mechanisms. Users select a secret image, a two-digit number, and an arithmetic operation (addition or subtraction). This method ensures that each login session generates a unique password, making it resistant to shoulder surfing and guessing attacks.

Recall-based methods, such as Draw-A-Secret (DAS) [13], require users to reproduce a pattern on a grid, which is stored as their password. Although DAS offers a large password space, it remains vulnerable to smudge attacks, where attackers infer the password from residue left on touchscreens. Blonder's method [14] further extended this concept by introducing predefined points within an image, forming the basis for future graphical password systems.

Thorpe and van Oorschot [12] introduced graphical dictionaries to improve security, while Davis et al. [11] explored user behavior in selecting graphical passwords, highlighting the importance of user-centered design to ensure both security and memorability.

Pass-Go [6], inspired by the traditional Chinese game Go, introduced a new grid-based graphical password scheme where users select intersections on the grid. This method provides a larger password space and improved usability compared to DAS, with fewer user errors and better resistance to attacks. However, even enhanced systems like Android's Pattern Lock [15] - a popular method for drawing patterns on a 3x3 grid - suffer from vulnerabilities like predictability and susceptibility to shoulder surfing.

Cued recall-based methods offer visual cues to help users remember their passwords. PassPoints [10] is one such system where users select specific points on an image, creating a sequence that serves as their password. Despite its ease of use and relatively high security, PassPoints remain vulnerable to shoulder surfing and smudge attacks.

Chiasson et al. [7] developed Cued Click Points (CCP), which improves security by having users click on points across multiple images in sequence. While CCP makes it harder for attackers to predict the password, it is still susceptible to observation-based attacks. An extension of this, Persuasive Cued Click Points (PCCP) [3], offers suggestions to users for selecting less predictable points, further complicating attack strategies but retaining some vulnerabilities.

Zakaria et al. [5] proposed several enhancements to these methods, introducing techniques like decoy strokes, disappearing strokes, and line snaking to make graphical passwords more resistant to shoulder surfing and smudge attacks. These techniques have been shown to improve security without significantly increasing the cognitive load on users.

The evolution of graphical password systems reflects an ongoing effort to balance security and usability. As highlighted by Owen et al. [8] and Fléchais [9], maintaining this balance is critical for the successful implementation of any authentication system. Systems that focus solely on security often suffer from poor usability, while overly simplistic systems may fail to provide adequate protection.

The proposed multi-action grid system builds on these previous methods by introducing dynamic, randomized elements and allowing for multiple interactions, such as tapping and replacing, within a flexible grid. This approach mitigates the vulnerabilities seen in earlier methods, particularly shoulder surfing and smudge attacks, while preserving ease of use.

3. **Proposed Authentication System**

The multi-action grid authentication system is designed to enhance security while maintaining usability by incorporating two core actions: tapping and replacing. The system operates within a 3x3 grid, providing a flexible yet secure authentication mechanism that mitigates common threats such as shoulder surfing and smudge attacks.

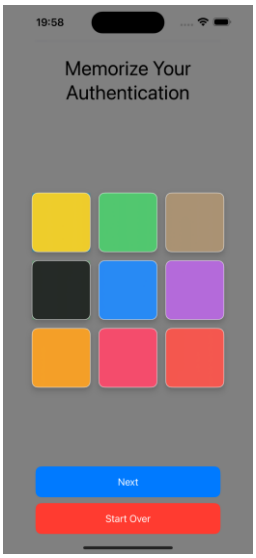

Figure 1. *Screenshot of the multi-action grid application interface during a registration attempt*

3.1. **System Design**. The system presents the user with a 3x3 grid of randomly positioned buttons in different colors during authentication. Each button within the grid represents a possible target for interaction. The user performs a sequence of two actions: tapping on one of the grid points and replacing an object from one grid point to another. The combination of these actions increases the difficulty for attackers to replicate the authentication process.

3.2 **Steps Involved**

1. *Grid Initialization*: At each login attempt, the system initializes the grid with random positions for the colored buttons that users interact with. The randomness of the positioning ensures that the grid configuration changes with every attempt, making it difficult for an observer to memorize the sequence of actions.
2. *User Interaction*:
   - **Tapping**: The user selects a specific button on the grid by tapping on it.
   - **Replacing**: The second action involves replacing a button from one point on the grid to another. This interaction is recorded and added to the authentication sequence.

   The combination of these two actions creates a unique authentication sequence that changes with every login attempt, enhancing security against replay attacks and observational threats (Figure 1).
3. *Authentication Verification*: The system verifies the user's authentication by comparing the sequence of actions (tap and replace) with the predefined sequence stored during registration. If the sequence matches, the user is authenticated successfully (Figure 2).

3.3. **Iterative Development.** The multi-action grid system was developed using an Iterative and Incremental Development (IID) approach, as described by Larman [16]. This methodology allowed continuous refinement based on user feedback and security testing at each stage. The iterative approach ensured that usability improvements were made without compromising the security features of the system.

3.4. **Testing and Feedback**. Extensive usability and security testing was conducted to evaluate the system’s performance. User feedback was collected during each iteration, focusing on ease of use, memorability, and the overall authentication experience. This feedback was critical in optimizing the system’s user interface and ensuring that the complexity of the actions did not hinder the authentication process.

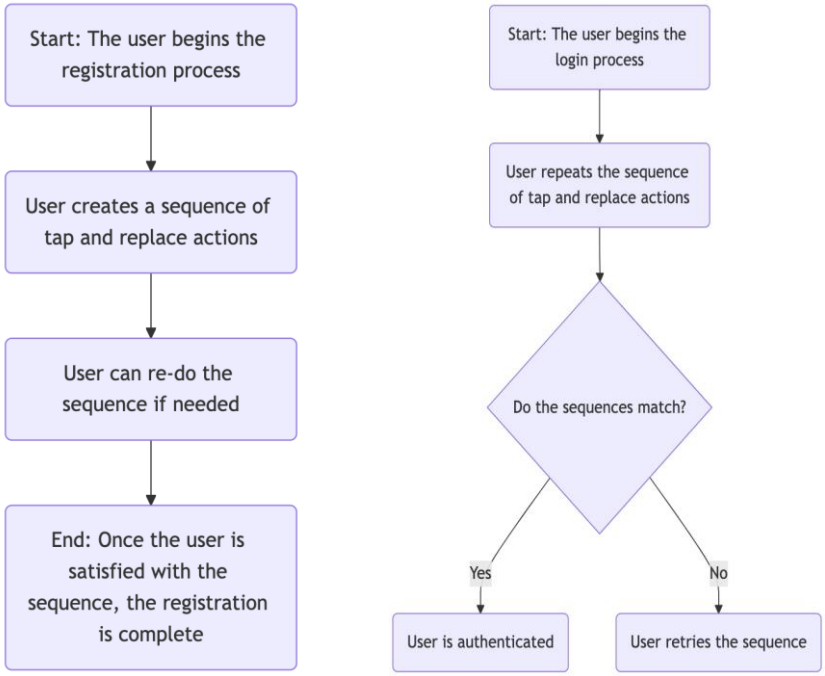

Figure 2. *The registration and login processes for the multi-action grid authentication system*

4. **Security Analysis**

The security of the multi-action grid authentication system is significantly enhanced by the ability to perform different number of taps and replace actions within the 3x3 grid. This flexibility increases the potential password space, making it much harder for attackers to guess or brute-force their way into the system.

At the beginning, because the starting grid appears by random location of 9 colored buttons on 9 place holders, there are 9! starting positions. The user needs to decide in each step if he/she should perform tapping or replacing. For tapping, the user must choose a color, which can be done in 9 different ways, and for replacing, he/she must choose one colored button to replace other colored button, which can be done in 9*8=72 different ways. This means that for one action we have 9+72=81 different ways.

So, the number of possible passwords for a minimum of 4 actions will be:

$$9! \cdot 81^4 = 362880 \cdot 43{,}046{,}721 = 15{,}620{,}794{,}116{,}480 \quad (4.1)$$

while for n actions it is:

$$9! \cdot 81^n \quad (4.2)$$

Since the user is allowed to perform multiple tap/replace actions, the password space grows exponentially with each additional action. For example, after the first replacement, the user may tap another grid point or replace an object again. Each sequence of actions introduces a new set of possibilities, further expanding the total password space.

This exponential growth in password space with each additional action provides substantial security against brute-force attacks. By allowing users to perform multiple actions, the system dramatically increases the number of potential combinations, making it highly resistant to guessing and brute-force attacks.

The password space can be enlarged if, instead of 3x3, we use 4x3 grid. In that case, there are 12! starting positions, 12 choices for taps and 12*11=132 choices for replacements per action, or 144 different ways per action. So, the number of possible passwords for a minimum of 4 actions will be:

$$12! \cdot 144^4 \approx 2.0596 \cdot 10^{17} \tag{4.3}$$

The multi-action grid authentication system is designed to provide robust security against several common attack vectors, including shoulder surfing, smudge attacks, and brute-force attacks (Figure 3). By allowing users to perform multiple tap/replace actions within a dynamic 3x3 grid, the system introduces a high level of complexity that significantly enhances its resistance to these threats.

4.1 **Resistance to Shoulder Surfing.** Shoulder surfing is one of the most common vulnerabilities for graphical password systems. In shoulder surfing attacks, an observer attempts to learn the password by watching the user interact with the system. The multi-action grid system mitigates this risk by using dynamic grid layouts and allowing users to perform multiple actions. The randomness of grid positions during each login session makes it difficult for an observer to memorize the specific sequence of actions.

Additionally, since users can choose how many actions to perform, even if part of the sequence is observed, it would be extremely challenging for an attacker to reconstruct the entire authentication process. The combination of taps and replacements in various locations, along with the flexibility in the number of actions performed, further reduces the likelihood of successfully executing a shoulder surfing attack.

4.2. **Resistance to Smudge Attacks.** Smudge attacks exploit the residue left on touch screens after user interaction to infer the password. Attackers analyze the smudge patterns left by users to recreate the sequence of their inputs. The multi-action grid system reduces the effectiveness of smudge attacks by allowing multiple actions and changing the grid's configuration with each login attempt. The dynamic repositioning of grid elements, coupled with the variety of possible actions, results in a diverse set of smudge patterns, making it difficult for attackers to accurately reconstruct the password sequence based on residue alone.

Additionally, the replace action, which involves moving an object across the grid, further complicates smudge patterns. This movement introduces additional traces that are not as easily interpretable as the static inputs seen in traditional graphical passwords.

4.3. **Resistance to Brute-Force Attacks.** The system's large password space, which grows exponentially with each additional tap/replace action, provides significant resistance to brute-force attacks. As calculated earlier, the more actions a user performs, the larger the number of possible password combinations. For example, with just 4 actions for 3x3 grid, the password space expands to more than $15 \oplus 10^{12}$ combinations, making it highly resistant to brute-force attempts.

Moreover, the system's dynamic grid layout prevents attackers from using common brute-force techniques that rely on static grid patterns or known positions. Each login attempt requires the user to interact with a new configuration, further complicating any brute-force strategy an attacker might employ.

4.4. **Mitigation of Replay Attacks**. Replay attacks occur when an attacker intercepts valid authentication data (such as a recorded sequence of actions) and reuses it to gain unauthorized access. The multi-action grid system mitigates this risk through the dynamic nature of the grid. Each login session generates a new grid layout, making it impossible for attackers to reuse a previously recorded sequence, as the object positions will have changed.

4.5. **Analysis of Edge Cases.** The system was also evaluated against potential edge cases, such as scenarios where users perform minimal actions or where they repeat a predictable pattern. In such cases, the system relies on its dynamic grid configuration and randomization to provide baseline security, even when users choose less complex authentication sequences. However, encouraging users to perform more varied actions can further increase security, and future iterations of the system may include prompts to guide users toward more secure behaviors.

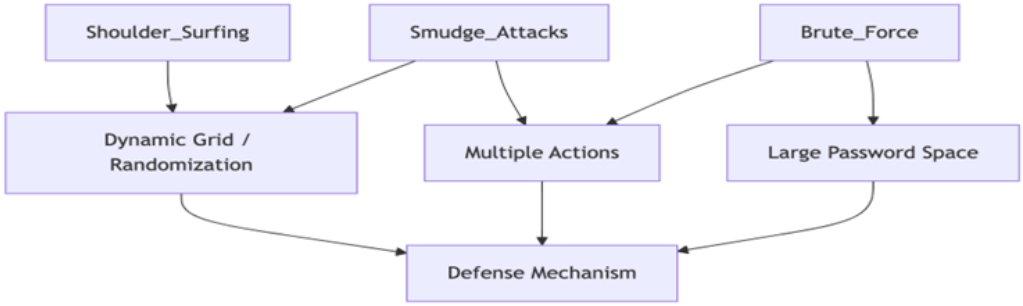

Figure 3. *A security analysis diagram illustrating how various attack vectors - shoulder surfing, smudge attacks, and brute force - are mitigated by the multi-action grid authentication system*

5. Usability Testing

To evaluate the effectiveness and ease of use of the multi-action grid authentication system, usability testing was conducted across a diverse group of participants. The

primary goals of the usability testing were to assess user satisfaction, the learning curve associated with the system, and the balance between security and usability.

The study included 15 participants, ranging from novice to experienced users of touch-based authentication systems. Participants were asked to complete a series of tasks, including registering their authentication sequences and logging in using the system after a period of time.

Participants were first introduced to the multi-action grid authentication system through a brief tutorial. They were then asked to register a sequence of tap and replace actions and were given the option to re-do the sequence if needed. After successfully completing registration, participants were asked to log in multiple times, repeating the sequence of actions they created during registration.

To simulate real-world usage, the participants were asked to perform the login process after a delay of 24 hours and again after a delay of 72 hours. This was intended to test the memorability of the authentication sequence and the likelihood of errors.

The usability testing focused on several key metrics:

- Time to Complete Registration: The amount of time taken by participants to successfully complete the registration process.
- Time to Authenticate: The time taken to log in using the system.
- Error Rate: The number of failed login attempts before successful authentication.
- User Satisfaction: Measured using a post-test questionnaire based on the System Usability Scale (SUS) [17], which rated user experience, ease of use, and overall satisfaction.

5.1 **Results.** The results of the usability testing showed that most participants were able to register and authenticate successfully with minimal difficulty. The average time to complete the registration process was 1 minute and 35 seconds, with most users completing the process after two to three attempts. During the login phase, participants initially took an average of 35 seconds to authenticate after 72 hours, but with repeated use and familiarity, the time reduced to an average of 25 seconds after 24 hours, demonstrating improved efficiency over time.

The error rate was relatively low, with participants averaging 1.2 failed login attempts before successfully authenticating. Users reported a high degree of satisfaction with the system, with an average SUS score of 85, indicating that the system was generally well-received and easy to use.

Participants provided positive feedback regarding the flexibility of the system, particularly the ability to customize the number of actions in the sequence. Users appreciated the dynamic nature of the grid, which added a layer of perceived security while not significantly impacting the ease of use. Some participants suggested that visual cues or hints could be added for users who struggle to recall their sequences, particularly after longer periods of inactivity.

6. **Discussion**

The multi-action grid authentication system successfully addresses several key challenges in graphical password systems, including security vulnerabilities like shoulder surfing, smudge attacks, and brute-force attempts, while maintaining a high degree of usability.

6.1. **Security vs. Usability Trade-off.** The security of the system is greatly enhanced by its use of a dynamic grid and the ability for users to perform multiple tap and replace actions. This introduces a large password space that increases exponentially with each additional action, making it significantly more resistant to brute-force attacks compared to traditional graphical password systems. Additionally, the randomization of grid elements during each authentication session provides effective mitigation against shoulder surfing and smudge attacks.

However, the added complexity raises potential usability concerns. While the system is designed to be flexible and user-friendly, the ability to perform multiple actions in a dynamic grid introduces a learning curve, particularly for less tech-savvy users. Despite this, the usability testing results show that participants quickly adapted to the system, with most users able to register and authenticate with minimal errors after a short period of practice.

6.2. **Memorability.** One of the key advantages of graphical password systems is their memorability, particularly when compared to alphanumeric passwords. The usability tests demonstrated that the multi-action grid system did not significantly impair users' ability to recall their authentication sequences, even after a delay of up to 72 hours. However, it is worth noting that some users expressed concern over their ability to remember more complex sequences after longer periods of inactivity. In future iterations of the system, adding optional memory aids or visual cues could help address this concern.

6.3. **Flexibility and User Control.** The system’s flexibility, allowing users to choose how many actions to perform, was generally well received. Participants appreciated being able to customize the difficulty of their authentication sequences to match their comfort level. This feature also enhances security, as users can create sequences of varying lengths, making it harder for attackers to predict or replicate a pattern.

6.4. **Comparison with Existing Systems.** Compared to the existing graphical password systems, such as PassPoints or DAS, the multi-action grid system offers several advantages. While PassPoints and DAS provide reasonable security, they are vulnerable to smudge attacks and shoulder surfing due to their static nature. By contrast, the dynamic and random elements of the multi-action grid significantly reduce these vulnerabilities. Moreover, the flexibility of the system allows users to create more secure sequences without substantially increasing the cognitive load, a common issue in hybrid systems like GRA-PIN.

6.5. **Limitations and Future Work.** Despite the system's strengths, there are limitations that need to be addressed in future versions. The flexibility of the system, while a key strength, could also lead to inconsistencies in user behavior, with some users opting for overly simple sequences that could compromise security. Introducing a minimum complexity requirement for sequences could help mitigate this risk. Additionally, future

research could explore the use of machine learning to analyze user behavior and provide real-time feedback on the security of their chosen sequence.

Future work should also investigate the system's performance in a wider variety of contexts, including high-risk environments where visual privacy cannot be easily maintained. Further testing with a larger, more diverse user base would provide deeper insights into how the system performs across different demographics and levels of technical expertise.

7. **Conclusion**

The multi-action grid authentication system presents a novel approach to securing touch-based smart devices by combining flexibility, security, and usability. By allowing users to perform multiple tap and replace actions within a dynamic grid, the system enhances resistance to common attack vectors such as shoulder surfing, smudge attacks, and brute-force attempts. The randomization of grid elements during each session further complicates efforts to compromise the system, ensuring a high level of security even in visually exposed environments.

Through usability testing, the system demonstrated a strong balance between security and ease of use. Users quickly adapted to the dynamic nature of the grid and were able to register and authenticate efficiently, with relatively few errors. While some concerns about memorability emerged during testing, particularly for more complex sequences, the overall feedback from participants was positive, with high System Usability Scale (SUS) scores indicating a generally favorable user experience.

This paper contributes to the ongoing evolution of graphical password systems by offering a flexible, user-friendly alternative that significantly increases password space and reduces vulnerability to attacks. While existing graphical systems like PassPoints and DAS offer similar advantages in terms of memorability and ease of use, they fall short in addressing key security concerns that the multi-action grid successfully mitigates.

Moving forward, there are several areas where this system can be improved. Introducing features such as optional memory aids or adaptive guidance for users could help reduce the cognitive load for users who struggle to remember complex sequences after long periods of inactivity. Additionally, further research into more adaptive randomization techniques and AI-driven analysis of user patterns could strengthen the system’s security even further. Another promising area of exploration is extending the system's application to other devices, including wearables and IoT devices, where touch-based authentication is becoming increasingly important.

Overall, the multi-action grid authentication system represents a significant step forward in the development of secure and usable authentication mechanisms for touch-based devices, offering a viable solution for both everyday use and high-security applications.

References

[1] *Almogren, A., Byung-Seo, K., Ali Khan, M., Kausar, N., Ud Din, I.* (2022). GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. Sensors, 22(4), 1349.

[2] *Gokhale, A. S., Waghmare, V. S. (2016).* The Shoulder Surfing Resistant Graphical Password Authentication Technique. Procedia Computer Science, 79, 490-498.

[3] *Chiasson, S., Stobert, E., Forget, A., Biddle, R., Van Oorschot, P. C.* (2012). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Transactions on Dependable and Secure Computing, 9(2), 222-235.

[4] *Biddle, R., Chiasson, S., Van Oorschot, P. C.* (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), Article 19:1-41.

[5] *Zakaria, N. H. Griffiths, D., Brostoff, S. Yan, J.* (2011). Shoulder surfing defence for recall-based graphical passwords. SOUPS '11: Proceedings of the Seventh Symposium on Usable Privacy and Security, July 2011, Article No.: 6, Pages 1 - 1

[6] *Tao, H., Adams, C.* (2008). Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security, 7(2), 273-292.

[7] *Chiasson, C., van Oorschot, P.C., Biddle R.* (2007). Graphical Password Authentication Using Cued Click Points. Carleton University, Technical Report TR-07-13.

[8] *Owen, G. S., Suo, X., Zhu, Y.* (2005). Graphical Passwords: A Survey. Proceedings of the 21st Annual Computer Security Applications Conference, 463-472.

[9] *Fléchais, I.* (2005). Designing Secure and Usable Systems. University of London, Ph.D. Thesis.

[10] *Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.* (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1-2), 102-127.

[11] *Davis, D., Monrose, F., Reiter, M. K.* (2004). On user choice in graphical password schemes. 13th USENIX Security Symposium.

[12] *Thorpe, J., van Oorschot, P. C.* (2004). Graphical Dictionaries and the Memorable Space of Graphical Passwords. Proceedings of the 13th USENIX Security Symposium.

[13] *Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., Rubin, A. D.* (1999). The design and analysis of graphical passwords. Proceedings of the 8th USENIX Security Symposium.

[14] *Blonder, G.* (1996). Graphical Password. US Patent 5559961.

[15] *WooTechy* (2024). All Possible Pattern Lock Combinations for Android. https://www.wootechy.com/unlock-android-phone/all-possible-pattern-lock-combinations/

[16] *Larman, C., Basili, V. R.* (2003). Iterative and Incremental Development: A Brief History. IEEE Computer, 36(6), 47-56.

[17] *Brooke, J.* (1996). SUS: A Quick and Dirty Usability Scale. In P.W. Jordan, B. Thomas, B.A. Weerdmeester, & I.L. McClelland (Eds.) Usability Evaluation in Industry (pp. 189-194). London: Taylor & Francis.

Darko Cebov
Goce Delcev University,
Faculty of Computer Science,
Goce Delcev 89,
Republic of N. Macedonia
E-mail address: darko.210199@student.ugd.edu.mk

Aleksandra Mileva
Goce Delcev University,
Faculty of Computer Science,
Goce Delcev 89,
Republic of N. Macedonia
E-mail address: aleksandra.mileva@ugd.edu.mk