The Authentication Game - Secure User Authentication by Gamification?

Frank Ebbers and Philipp Brune(✉)

University of Applied Sciences Neu-Ulm,
Wileystraße 1, 89231 Neu-Ulm, Germany
f.ebbers@yahoo.de,
Philipp.Brune@hs-neu-ulm.de

Abstract. Knowledge-based authentication with username and password still is the predominant authentication method in practice. As the number of online accounts increases, users need to remember more and more passwords, leading to the choice of better memorable but insecure passwords. Therefore, it is important to take into account the users' behavior to improve IT security. While gamification has been proposed as a concept to influence users' behavior in various domains, it has not been applied to user authentication methods so far. Therefore, in this paper an approach for a gamified authentication method is presented. Using a prototype implementation, a qualitative evaluation in an empirical study is performed. Results illustrate the general feasibility of the proposed approach.

Keywords: Information security · User authentication · Graphical passwords · Biometrics · Gamification

1 Introduction

For many years, knowledge-based authentication using username and password is the predominant authentication method in practice [2]. In recent years, also biometric and token-based approaches have become increasingly important, but textual passwords remained frequently used despite their well-known disadvantages [33]. As the number of mobile devices, web services and other online accounts increases, users need to remember more and more passwords. An average US user has 25 password-protected accounts and has to enter a password eight times a day [15]. Therefore, many people choose memorable but insecure passwords, built a mnemonic aid [28], write passwords down or use one password for many different services [17]. This leads to increasing security risks for private and business computing and illustrates the importance of "human factor in security" [39].

Security cannot be achieved by technological solutions alone [34]. It is important to take into account the users' behavior and security awareness regarding password usage. However, existing attempts like security awareness trainings often failed to successfully change users habits [21].

S. Nurcan et al. (Eds.): CAiSE 2016, LNCS 9694, pp. 101–115, 2016.
DOI: 10.1007/978-3-319-39696-5_7

In recent years, gamification has been proposed as a concept to influence peoples behavior in different contexts [49]. It denotes the process of adding game elements to a non-gaming environment [11] to influence users through intrinsic motivation. Although gamification already has been used in various contexts, in particular for educational purposes [42], few attempts have been made to apply it in the domain of IT security so far.

Therefore, in this paper an approach for a gamified authentication method is presented and evaluated. It requires a user to successfully complete a computer game to authenticate to a system. Using a prototype implementation of this authentication game, the approach is qualitatively evaluated in an empirical study. The results indicate the general feasibility of the proposed approach and show its perception by different potential users.

The rest of this paper is organized as follows: In Sect. 2 the related work is discussed in detail and Sect. 3 explains the design and implementation of the proposed authentication game. The design and data collection of the empirical study is described in Sect. 4, while Sect. 5 discusses the obtained results. We conclude with a summary of our findings.

2 Related Work

Traditionally, user authentication to an application or service is performed using a combination of a username and a secret password chosen by the user (the so-called user credentials), mainly since it is cheap and easy to use [19]. However, the weaknesses and risks of this approach have been discussed for many years [37,48]. Passwords may be easily forgotten, stolen or guessed by an attacker, i.e. using dictionary attacks [31,37]. The security of a password increases with its length, which in turn makes it harder to remember. In addition, the number of passwords an average user has to remember strongly increased in the last years [31]. Maintaining their various passwords therefore is an increasing challenge for most users [9,10]. The usability [32] of information security measures, in particular the traditional password-based authentication is being discussed for some years [3,46]. In particular, various alternatives to the standard username/password credentials have been proposed, namely biometrics and graphical passwords.

Graphical passwords are methods of image-based authentication first proposed in 1996 [4], which are based on the fact that humans can remember pictures much better than letters [8]. There exist different variants for graphical passwords, in particular recognition-based authentication [5], recall-based authentication [47] like the Draw-a-Secret (DAS) method [13,25], and pass-point methods [23,26]. Graphical passwords, in particular DAS are commonly used today in practice to protect mobile devices [12,30]. However, despite their better usability compared to using a conventional password, also the graphical password approaches like DAS have some security [44] as well as usability problems (i.e. the difficulty to draw precisely) [36].

"Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person" [24]. Physical and chemical characteristics could be fingerprints, voice, veins, iris prints or even ones DNA [45]. Another method for biometrical authentication is keystroke analysis. It has been demonstrated that human key stroke behavior is unique for a person [6,29]. However, the accuracy of keystroke-based approaches is inferior to other biometric characteristics. On the other hand the keystroke behavior could not be copied or stolen. The human way of pressing and releasing keys on a keyboard is unique and can be captured and replayed only be means of a key logger installed on the system. In the future, a logical continuation of keystroke patterns may be the use of gestures for user authentication [40].

However, in general still better technologies which improve the memorability of a user's credentials while improving the security of the authentication process are required [38]. Gamification may provide a promising approach for that purpose [1].

In recent years, Gamification has been studied by various authors. One major field of research is its application for educational purposes, denoted by terms like Serious Gaming, Edutainment or Learning Games [42]. While first applications of Gamification in the information security domain have been proposed [49], they mainly are related to information security trainings for improving security awareness [1,7,14]. Despite the fact that Gamification may provide a mean to improve IT security enormously [43] and that all existing alternatives to textual passwords like biometrics and graphical passwords have serious security or usability flaws, it has rarely been applied to user authentication so far [16,18].

Therefore, in the present paper the question is addressed how a gamified authentication method with additional keystroke pattern recognition could be designed for improving the security and usability of user authentication simultaneously.

3 Design and Implementation of the Authentication Game

This paper proposes a game-like solution for users to authenticate themselves with any web service or personal computer called the Ariadne PathLogin. Referring to the password management life cycle [9] it uses a holistic approach taking into account all human factors influencing the password generation and maintenance phase by means of Gamification. In addition, since it has been demonstrated that human muscle movements improve the ability to remember the password [9], the approach utilizes also users keystroke patterns as an additional biometric authentication factor.

Therefore, the proposed approach uses a chessboard game-like scenario as illustrated in Fig. 1. After selecting a specific avatar character, the user has to move it on an individual, secret path across the game board. During this movement, the user might also have to perform special actions (i.e. jumping) on certain fields. The specific avatar character and the path including the special actions have been individually selected by the user during the registration phase, therefore serving as part of the secret information identifying the user. The

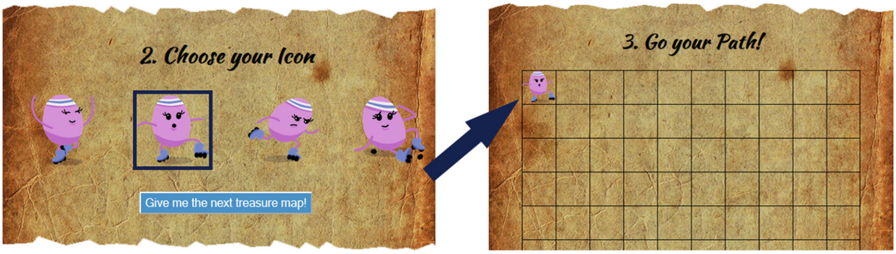


Fig. 1. Design of the avatar character selection and playing field screens in the proposed Ariadne PathLogin game for user authentication. After selecting a specific avatar character as a "playing figure", the user has to move it on an individual, secret path across the game board for authentication using the keyboard's arrow keys.

additional special tasks further support the creation of highly individual and better memorable secrets by the users [9,20].

Ariadne PathLogin uses a board dimensioned to a 10 × 10 fields square (see right part of Fig. 1). Although the board itself thus offers only $10 \times 10 = 100$ fields, the number of selectable paths is theoretically infinite, since at every field the character might move to 4 possible neighboring fields (including fields already visited before) and the number of steps forming a path is also variable and unlimited. The goal of Ariadne PathLogin is to access to the Ariadne Castle at the end of the login process, which is accompanied by a fanfare sound, giving users a feeling of success. In a real-world application this corresponds to being granted access to the system.

Users control the character on the board by the arrow- or space keys on the keyboard. The user's characteristic keystroke pattern while doing so is also captured during the enrollment phase for subsequent comparison in every authentication process as an additional biometric signature.

3.1 Registration Phase

Like any other authentication method each user has to register first. For the Ariadne PathLogin, three different steps are required:

1. Specifying a unique textual username,
2. Selecting a specific "playing figure" or avatar character (called Ariadne),
3. Defining a specific path across the playing board.

The user can only perform one steps at once. In the game, each step is represented by a part of a treasure map (see Fig. 1), which may foster curiosity, learnability and memorability [32]. Furthermore, by displaying only one step at a time the user will not be distracted by too much information and the process is more secure since less information is unveiled.

The user has to select a personal avatar character out of four predefined characters. Choosing a unique character seen as a playing figure is important for creating a personal touch for the user [27]. Ariadne is the character of this game. She is a female character representing different and funny attitudes, designed by the authors. The user can choose between four different variants of the character as illustrated in the left part of Fig. 1. All variants are rather similar in shape and color in order to make character guessing or shoulder-surfing attacks by a third party more unlikely.

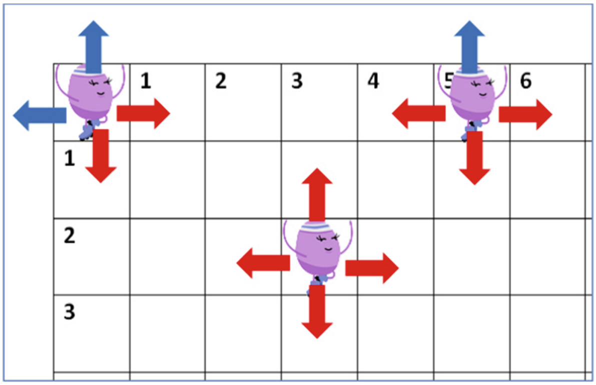


Fig. 2. Possible moves of the Ariadne avatar character during its path across the board. Red arrows indicate visible moves while the blue ones correspond to "hidden" moves to confuse a possible shoulder-surfing attacker. (Color figure online)

Third, the user has to move the avatar character across the chess-like board to define an individual secret path, optionally including special actions like jumping on certain fields. The character's initial position is in the left upper corner of the board. The character can be moved only via the arrow keys. For each keystroke, the actual key and the corresponding time stamp are captured by the system. The user can choose the path freely with the character moving visibly only within the board area. However, if the user types a key sequence corresponding to the character moving outside the playing field, these keystrokes are still captured without moving the character visibly to enable using "hidden" paths for additional security. These different types of move operations are illustrated in Fig. 2. Here, red arrows symbolize visible movements while blue ones refer to invisible movements forming the hidden path.

To capture a characteristic individual keystroke pattern and to ensure that a user memorizes the selected path well, the user has to repeat this path five times. This can be compared to the traditional registration phase using text-based passwords, where any user also has to enter a new password at least twice in order to exclude mistakes. This first path is considered as the basis for the upcoming paths. If the user changes the path or the character in a subsequent iteration, the system will prompt the user by a popup message and cancel the path capture. After the fifth successful iteration, the characteristic keystroke pattern will be calculated and the captured data will be stored in the user database. For obtaining this characteristic keystroke pattern for a user's path, the arithmetic mean values of the time differences (in milliseconds) between subsequent distinctive keystrokes are calculated.

3.2 Authentication Phase

In the authentication phase, a user is authenticated by repeating the same three steps as in the registration phase, now entering the correct username, avatar character and path as previously captured. For comparison with the stored characteristic keystroke pattern, again the time differences between subsequent keystrokes are calculated and compared with the values stored in the database. However, since the measured time differences never will be exactly the same for a human (i.e. due to external factors and personal condition) [9], some tolerance interval needs to be used in the comparison. Previous results suggest a time tolerance interval of about 160ms for biometric keystroke patterns [41], which was adopted for the current implementation of Ariadne PathLogin. If all data are correct, the user is prompted about the successful login.

If the login process fails, the user has to start right from the beginning again. The reason is that in this case either the user name or the character or the path or multiples of these may be wrong. Since an attacker should not be revealed any information which of these are wrong, no clue is given and all data entries have to be repeated.

3.3 Prototype Implementation

For the experimental evaluation of the proposed approach, a prototype of the Ariadne PathLogin game was implemented as a browser-based web application. The purpose of this implementation is not to provide a production-ready solution, but to serve as the basis for evaluation of the concept.

The user interface of the prototype is implemented using HTML5, CSS and JavaScript. This frontend interacts with a server-side backend implemented in the widely used PHP language[1]. All data used within the authentication process are stored in a MySQL database accessed by the PHP code, using the InnoDB storage engine[2].

The users' characteristic keystroke patterns are stored in this database as strings consisting of a sequence of the numerical key codes pressed and the corresponding time passed since the previous keystroke in milliseconds. Since the pupose of the prototype implementation was to evaluate the feasibility of the approach from a user's perspective and not to provide a production-ready solution, implementation-related security issues like of this underlying storage mechanism are not discussed in this paper.

[1] See http://www.php.net.

[2] See http://www.mysql.com.

4 Evaluation

To evaluate the proposed approach, a qualitative, explorative empirical study was performed using the described prototype implementation. The purpose of the evaluation was twofold: First, the proposed approach was evaluated with respect to its effectiveness from a user's perspective regarding its usability and Gamification. This was done using a questionnaire the participants had to fill out. Second, its effectiveness as an authentication scheme needed to be analyzed regarding the reliability of clearly identifying a specific user. Therefore, the participants had to practically use the prototype implementation to register and authenticate themselves at the system.

A convenience sample of 51 participants with different occupation, social background and gender took part in the study. All participants were between 15 and 67 years old, with the majority being between 20 and 30. 41 of these participants (approx. 80 %) were male.

To have comparable results and exclude environmental influences, all participants had to use the Ariadne PathLogin in an identical work environment. A desktop workplace with always the same computer equipment was set up for them in a neutral surrounding. Only one participant was inside the room at a time to avoid mutual influences between participants.

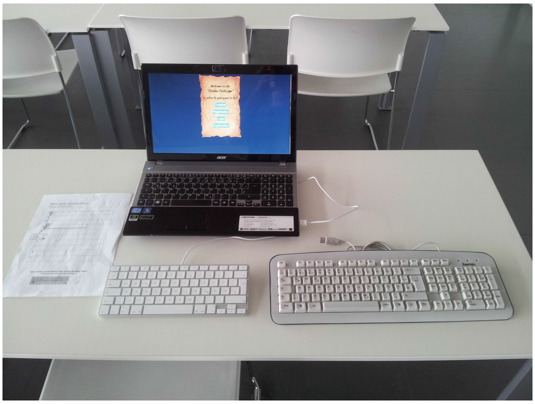
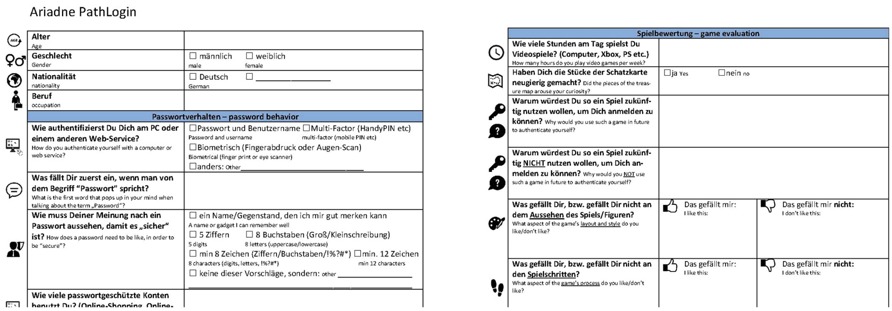


Fig. 3. Setup of the participants' desktop for the empirical evaluation. Two different keyboards have been used to study the influence of the keyboard type on the users' keystroke patterns.

The computer used for the evaluation was a Notebook (Acer Aspire V3-571G with Intel i5-3210M CPU and Seagate Momentus XT 750 GB SSHD solid-state hybrid drive) running with Microsoft Window 8.1 64 Bits, a Firefox web browser 35.0.1 without any add-ons and the Ariadne PathLogin application running within the XAMPP 5.6.3 environment. In order to analyze the possible influence of keyboard types, two (new) USB keyboards were used with strongly



Ariadne PathLogin

Alter Age	
Geschlecht Gender	□ männlich □ weiblich male female
Nationalität nationality	□ Deutsch □ ________________ German
Beruf occupation	
Passwortverhalten – password behavior	
Wie authentifizierst Du Dich am PC oder einem anderen Web-Service? How do you authenticate yourself with a computer or web service?	□Passwort und Benutzername □Multi-Factor (HandyPIN etc) Password and username multi-factor (mobile PIN etc) □Biometrisch (Fingerabdruck oder Augen-Scan) Biometrical (finger print or eye scanner) □anders: Other________________________________
Was fällt Dir zuerst ein, wenn man von dem Begriff "Passwort" spricht? What is the first word that pops up in your mind when talking about the term „Password"?	
Wie muss Deiner Meinung nach ein Passwort aussehen, damit es „sicher" ist? How does a password need to be like, in order to be "secure"?	□ ein Name/Gegenstand, den ich mir gut merken kann A name or gadget I can remember well □ 5 Ziffern □ 8 Buchstaben (Groß/Kleinschreibung) 5 digits 8 letters (uppercase/lowercase) □ min 8 Zeichen (Ziffern/Buchstaben/!%?#*) □min. 12 Zeichen 8 characters (digits, letters, !%?#*) min 12 characters □ keine dieser Vorschläge, sondern: other ________________ ____
Wie viele passwortgeschützte Konten benutzt Du? (Online-Shopping, Online-	

Spielbewertung – game evaluation		
Wie viele Stunden am Tag spielst Du Videospiele? (Computer, Xbox, PS etc.) How many hours do you play video games per week?		
Haben Dich die Stücke der Schatzkarte neugierig gemacht? Did the pieces of the treasure map arouse your curiosity?	□ja Yes □nein no	
Warum würdest Du so ein Spiel zukünftig nutzen wollen, um Dich anmelden zu können? Why would you use such a game in future to authenticate yourself?		
Warum würdest Du so ein Spiel zukünftig NICHT nutzen wollen, um Dich anmelden zu können? Why would you NOT use such a game in future to authenticate yourself?		
Was gefällt Dir, bzw. gefällt Dir nicht an dem Aussehen des Spiels/Figuren? What aspect of the game's layout and style do you like/don't like?	Das gefällt mir: I like this:	Das gefällt mir **nicht:** I don't like this:
Was gefällt Dir, bzw. gefällt Dir nicht an den Spielschritten? What aspect of the game's process do you like/don't like?	Das gefällt mir: I like this:	Das gefällt mir **nicht:** I don't like this:

Fig. 4. Excerpts of the first (left) and second page (right) of the questionnaire handed out to the participants before and after the practical usage of the prototype, respectively. The first page contains questions related to personal data and previous experiences regarding user authentication. The second page is devoted to the actual evaluation of the game. Questions are stated in German and English language.

differing types of keys (rather flat vs. high), namely Hama Basic Keyboard K 210, USB and an Apple Keyboard A1242. The complete described setup for the evaluation environment is displayed in Fig. 3.

In addition to using the tool, the participants had to fill out the two-page questionnaire shown in Fig. 4.

Each participant first was introduced into the topics of authentication, passwords and the purpose of the Ariadne PathLogin. Afterwards he or she had to fill out the first page of the questionnaire. When starting to use the prototype, the web browser was already opened in full-screen mode, displaying the main page of Ariadne PathLogin containing an overview of all functions to ensure an identical starting point for all participants.

Now the participants were asked to do a tutorial first to get familiar with the approach. No data was logged during this step.

After that, the participants should perform the described registration and login steps. In order to collect comparable data, all participants were asked to use the same predefined path, presented to them on a piece of paper. During these steps, the entered data was logged by the system for evaluation.

After the registration phase, users were asked to do the login. They were given the choice to select one of the two different keyboards. It was not necessary to login using both of them. If the user passed the login after a maximum of three tries, the login was considered as successful.

Finally, the users were asked to fill out the second page of the questionnaire.

5 Results

5.1 User Perception

Regarding previous experiences with different authentication methods, username and password are used by all participants, as one would expect. Due to the popularity of smartphones and mobile devices, 20 % also use finger print sensors. Multi-factor authentication has been used by about 22 % of the participants. These numbers are in agreement with previous findings indicating that 27 % of users use multi-factor authentication on their smartphones [35] and 22 % use of biometrical authentication [22].

Almost half of the participants immediately associated the term security with passwords. Despite this fact, nearly one fifth of the participants is annoyed by using text-based passwords, which supports the request for better authentication methods.

Table 1. Participants' opinions of Ariadne PathLogin as a computer game.

Positive	Negative
"Easy and clear to understand"	"Entering a new password (registration step) takes too long"
"Freedom of decision which character and path to choose"	"You can walk a wrong path"
"You can choose the security by yourself by defining a path or secret path"	"The icon's jump is confusing"
"Speed and sounds fit to the game"	"Too little action"
"Easy to reproduce"	

However, only about 50 % of the participants stated that they would be interested or willing to use Ariadne PathLogin in the future. Figure 5 shows a more detailed analysis of the reasons given by the participants for acceptance of the game.

The reasons for refusal of the approach are strongly varying between the different age groups (see Fig. 5). A majority of the 15–50 year-old participants considers it is too time consuming. As one participant formulated it: "I would use it for accounts I do not use very often, but which are very safety-critical like my online banking". The older the participants were, the fewer security doubts they had.

On the other hand, the older participants found the approach increasingly difficult to use.

Regarding their perception of the Ariadne PathLogin as a computer game, the structure and rules seemed clear for the majority of the participants. They liked also the possibility to choose the password strength by adjusting the path. On the negative side, users stated that the process takes too long and there are too few but still confusing actions, e.g. a jump is executed on the same field. The pros and cons of the approach as perceived by the participants are summarized in Table 1.

65 % of the participants claimed that they could remember the graphical path in Ariadne PathLogin better than a complex textual password. Two participants

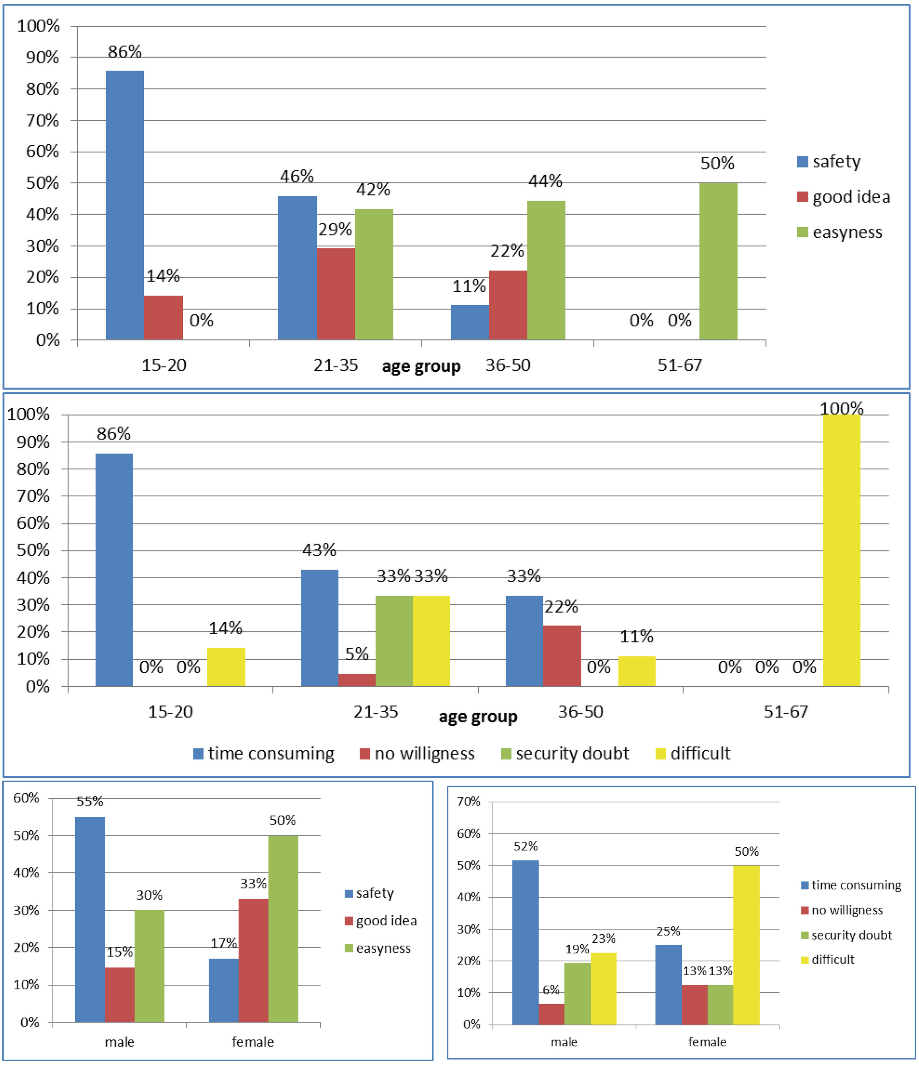


Fig. 5. Participants' reasons for their willingness to use or not use Ariadne PathLogin in the future depending on age (above) and gender (below).

even stated "Hey, that is cool. I can connect the path with a rhythm or beat" and "I would connect this path with my favorite song, that will surely help me".

5.2 Effectiveness of the Authentication Mechanism

Figure 6 shows the number of successful logins of the participants while using the Ariadne PathLogin prototype implementation depending on age and gender.

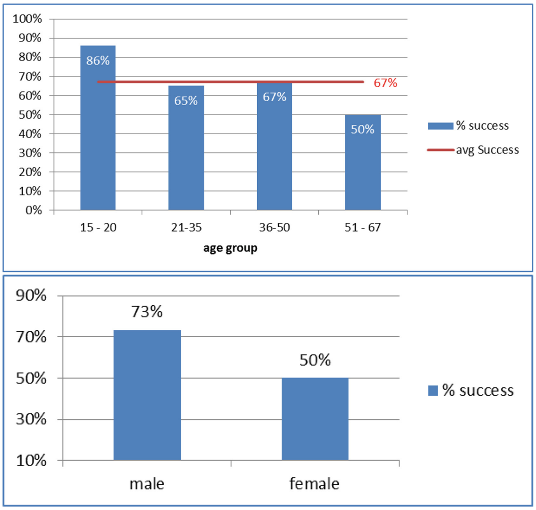


Fig. 6. Number of successful logins by the participants using Ariadne PathLogin depending on age (above) and gender (below).

The authors consider the login success rate as the main indicator for the effectiveness of the proposed approach.

The average success rate was 67 %, with a variance of 2 % and a standard deviation of 15 %. Within the age group of 15 to 20 the rate was sufficiently high (86 %). But even for elderly persons the login was successful in one out of two tries. Generally speaking, no critical difference can be found between age groups, whereas male users succeed almost 25 % more often than female ones.

However, these results for the success rates should be considered critically. First, the number of participants was not equal for age groups and genders, and second users were presented a predefined path for this evaluation. It is likely that the memorability of the path and thus the success rate improves when users have to choose a path by their own.

It was also observed that the login success rate is strongly dependent on the numerical tolerance value used while comparing the keystroke pattern captured during login to the one previously stored in the database. The initial tolerance value used was 160 ms (see above). When increasing it to 250 ms, around 50 % of those who failed before also succeeded. And even 70 % were successful after changing the tolerance to 450 ms. However, increasing the tolerance on the other hand reduces the security of the approach, as it increases the probability of false positive matches.

Regarding the keyboard used, no significant influence was observed. Users typed on average 6 % (25.81 ms) faster on the keyboard with the flat keys than on those with the higher keys. However, this small difference can be neglected.

To evaluate the risk due to false positive matches during the keystroke pattern comparison, the authors also tried to login to the users accounts. Although the authors knew all the credentials information of the users (username, chosen character, the path and the approximate typing speed at least from subjective cognition), they succeeded only in two out of 51 cases. This emphasizes the additional security gained by the biometric keystroke pattern comparison.

6 Conclusion

In conclusion, in the present paper an approach for a gamified authentication method has been presented and evaluated, which requires the user to successfully complete a computer game to authenticate to a system. The authentication mechanism used by the game is a combination of a biometric and a knowledge-based factor. To successfully log in, the user has to possess the secret knowledge of the correct username, avatar character and path across the playing board as well as to control the character with the corresponding personal keystroke pattern.

The feasibility of the proposed approach was evaluated by an empirical study, in which the participants had to use a prototype implementation of the game to log in, as well as to answer a questionnaire to assess the perceived quality of the game. The evaluation results suggest that despite some differences between participants of different ages the approach is feasible in general. However, it was considered rather time-consuming by many participants, so probably its application will remain restricted to scenarios where a higher level of security is required (i.e. online banking or access to mission-critical applications).

However, the validity of these findings is still limited due to the limited number of the participants in the empirical study and its qualitative nature. The evaluation still needs to be extended by further research efforts to verify the obtained results.

References

1. Amorin, J.A., Hendix, M., Andler, S.F., Gustavsson, P.M.: Gamified training for cyber defence: Methods and automated tools for situation and threat assessment (2013)
2. Andress, J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd edn. Elsevier Science, USA (2014)
3. Balfanz, D., Durfee, G., Smetters, D., Grinter, R.: In search of usable security: five lessons from the field. IEEE Secur. Priv. **2**(5), 19–24 (2004)
4. Blonder, G.E.: Graphical password (1996). http://www.google.com/patents/US5559961
5. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. In: McDonald, S., Waern, Y., Cockton, G. (eds.) People and Computers XIV – Usability or Else!, pp. 405–424. Springer, London (2000)
6. Brown, M., Rogers, S.J.: User identification via keystroke characteristics of typed names using neural networks. Int. J. Man Mach. Stud. **39**(6), 999–1014 (1993)
7. Burke, M., Hiltbrand, T.: How gamification will change business intelligence. Bus. Intell. J. **16**(2), 8–16 (2011)

8. Chaki, N.: Computer Networks & Communications (NetCom): Proceedings of the Fourth International Conference on Networks et Communications. Lecture Notes in Electrical Engineering, vol. 131. Springer, New York (2013)
9. Choong, Y.-Y.: A cognitive-behavioral framework of user password management lifecycle. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 127–137. Springer, Heidelberg (2014)
10. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The tangled web of password reuse. In: Symposium on Network and Distributed System Security 2014, Washington, D.C. (2014)
11. Deterding, S., Sicart, M., Nacke, L., O'Hara, K., Dixon, D.: Gamification: using game-design elements in non-gaming contexts. In: Tan, D., Amershi, S., Begole, B., Kellogg, W.A., Tungare, M. (eds.) The 2011 Annual Conference Extended Abstracts, pp. 2425–2428 (2011)
12. Dunphy, P., Heiner, A.P., Asokan, N.: A closer look at recognition-based graphical passwords on mobile devices. In: Cranor, L.F. (ed.) SOUPS 2010. ACM International Conference Proceedings Series, p. 1. ACM, New York (2010). http://dl.acm.org/citation.cfm?id=1837114
13. Dunphy, P., Yan, J.: Do background images improve draw a secret graphical passwords?. In: Ning, P., Capitani, D., di Vimercati, S., Syverson, P., Capitani, D., di Vimercati, S., Syverson, P.F., Evans, D. (eds.) Proceedings of the 14th ACM conference on Computer and Communications Security, pp. 36–47. ACM Digital Library, New York (2007). http://dl.acm.org/citation.cfm?id=1315252
14. Fernandes, J., Duarte, D., Ribeiro, C., Farinha, C., Pereira, J.M., da Silva, M.M.: ithink: A game-based approach towards improving collaboration and participation in requirement elicitation. Procedia Comput. Sci. **15**, 66–77 (2012)
15. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Williamson, C., Zurko, M.E. (eds.) Proceedings of the 16th International Conference on World Wide Web 2007, pp. 657–666. ACM, New York (2007)
16. Forget, A., Chiasson, S., Biddle, R.: Persuasion as education for computer security. In: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, vol. 2007(1), pp. 822–829 (2007)
17. Fortinet: Multiple password tendencies of gen x online users in the united states, as of February 2014: Statista (2014). http://www.statista.com/statistics/305462/generation-x-multiple-internet-account-passwords/
18. Gallego, A., Saxena, N., Voris, J.: Playful security: a computer game for secure wireless device pairing. In: 2011 16th International Conference on Computer Games (CGAMES), pp. 177–184, July 2011
19. Hari, K.K.K., Anbuoli, P., Manikandan, A., Saikishore, E. (eds.): Computer Applications I: Proceedings of the International Conference on Computer Applications, 24–27 December 2010, Pondicherry, India. Research Pub. Services, Singapore (2011)
20. Helkala, K., Svendsen, N.K.: The security and memorability of passwords generated by using an association element and a personal factor. In: Laud, P. (ed.) NordSec 2011. LNCS, vol. 7161, pp. 114–130. Springer, Heidelberg (2012)
21. Herold, R.: Managing an Information Security and Privacy Awareness and Training Program, 2nd edn. CRC Press, Boca Raton (2011)
22. InformationWeeks Analytics: Analytics report: Identity management - saas, mobility add urgency (2011). http://www.exactidentity.com/wp-content/uploads/2012/07/InformationWeek-Identity-Management.pdf
23. Iranna, A., Pankaja, P.: Graphical password authentication using persuasive cued click point. Int. J. Eng. Res. Appl. **2**, 2963–2974 (2013)

24. Jain, A.K., Flynn, P.J., Ross, A.A.: Handbook of Biometrics. Springer, New York (2007)
25. Jermyn, I., Mayer, A.J., Monrose, F., Reiter, M.K., Rubin, A.D., et al.: The design and analysis of graphical passwords. In: Association, U. (ed.) Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA, vol. 8. (1999)
26. Khot, R.A., Srinathan, K., Kumaraguru, P.: Marasim: a novel jigsaw based authentication scheme using tagging. In: Tan, D.S., Fitzpatrick, G., Gutwin, C., Begole, B., Kellogg, W.A. (eds.) CHI 2011, pp. 2605–2614 (2011). http://dl.acm.org/citation.cfm?d=1978942.1979322
27. Kroeze, C., Olivier, M.S.: Gamifying authentication. In: Venter, H.S., Loock, M., Coetzee, M. (eds.) 2012 Information Security for South Africa, pp. 1–8. IEEE, Piscataway (2012)
28. Kuo, C., Romanosky, S., Cranor, L.F.: Human selection of mnemonic phrase-based passwords. In: Cranor, L.F. (ed.) SOUPS 2006: Proceedings of the Second Symposium on Usable Privacy and Security, pp. 67–78. ACM, New York (2006)
29. Loy, C.C., Lai, W.K., Lim, C.P.: Keystroke patterns classification using the artmap-fd neural network. In: Liao, B.Y. (ed.) IIHMSP 2007, pp. 61–64. IEEE Computer Society, Los Alamitos (2007)
30. Luca, A.D., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and i know it's you! implicit authentication based on touch screen patterns. In: Konstan, J.A., Chi, E.H., Höök, K. (eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 987–996. ACM, New York (2012). http://dl.acm.org/citation.cfm?id=2208544
31. Newman, R.: Security and Access Control Using Biometric Technologies. Cengage Learning, New Delhi (2009)
32. Nielsen, J.: Usability Engineering. Morgan Kaufmann Publishers, San Francisco (1994). Updated edn
33. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proc. IEEE **91**(12), 2021–2040 (2003)
34. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: Human factors and information security: Individual, culture and security environment (2010)
35. SafeNet Inc.: Multi-factor authentication: Current usage and trends (2013). http://www2.safenet-inc.com/email/pdf/Multi_Factor_Authentication_WP_EN_A4_v3_3Apr2013_web.pdf
36. Sarohi, H.K., Khan, F.U.: Graphical password authentication schemes: current status and key issues. Int. J. Comput. Sci. Issues (IJCSI) **10**(2), 437 (2013)
37. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley, New York (2011)
38. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley, New York (2000)
39. Schultz, E.: The human factor in security. Comput. Secur. **24**(6), 425–426 (2005)
40. Shahzad, M., Liu, A.X., Samuel, A.: Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking, MobiCom 2013, pp. 39–50. ACM, New York (2013). http://doi.acm.org/10.1145/2500423.2500434
41. Sharif, M., Faiz, T., Raza, M.: Time signatures - an implementation of keystroke and click patterns for practical and secure authentication. In: Third International Conference on Digital Information Management (ICDIM 2008), pp. 559–562. IEEE, Piscataway (2008)

42. Thiebes, S., Lins, S., Basten, D. (eds.): Gamifying information systems - a synthesis of gamification mechanics and dynamics. In: ECIS, Tel Aviv, Israel (2014)
43. Thornton, D., Francia, G.I.: Gamification of information systems and security training: Issues and case studies. Inf. Secur. Edu. J. **1**(1), 19–29 (2014)
44. Uellenbeck, S., Dürmuth, M., Wolf, C., Holz, T.: Quantifying the security of graphical passwords: the case of android unlock patterns. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS 2013, pp. 161–172. ACM, New York (2013). http://doi.acm.org/10.1145/2508859.2516700
45. Wang, P.: Pattern Recognition, Machine Intelligence and Biometrics. Springer, Heidelberg (2012)
46. Yee, K.P.: Aligning security and usability. IEEE Comput. Soc. **2**(5), 48–55 (2004)
47. Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J.: Shoulder surfing defence for recall-based graphical passwords. In: Cranor, L.F. (ed.) Proceedings of the Seventh Symposium on Usable Privacy and Security, vol. 2011, pp. 1–12. ACM, New York (2011)
48. von Zezschwitz, E., De Luca, A., Hussmann, H.: Survival of the shortest: a retrospective analysis of influencing factors on password composition. In: Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., Winckler, M. (eds.) INTERACT 2013, Part III. LNCS, vol. 8119, pp. 460–467. Springer, Heidelberg (2013)
49. Zichermann, G., Cunningham, C.: Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps, 1st edn. O'Reilly Media, Sebastopol (2011)