Explore-a-Nation: Combining Graphical and Alphanumeric Authentication

Lauren N. Tiller(✉), Catherine A. Angelini, Sarah C. Leibner, and Jeremiah D. Still

Department of Psychology, Old Dominion University, Norfolk, VA, USA
{LTill002, CAnge001, SSort001, JStill}@odu.edu

Abstract. Graphical authentication has been a proposed solution to the usability and memorability issues seen with traditional alphanumeric passwords. However, graphical authentication schemes are often criticized for their susceptibility to Over-the-Shoulder Attacks (OSAs). This research proposes and evaluates Explore-a-Nation (EaN), a unique hybrid authentication scheme that attempts to bridge the gap between graphical authentication passcodes and strong alphanumeric passwords. EaN takes advantage of the known security and efficiency associated with passwords along with the enhanced recognition benefit of graphical schemes. The EaN scheme provides users with a static image consisting of a map wherein an icon passcode path is hidden amongst other distractor icons. Following the icon path allows users to generate their strong password. This study compared our EaN prototype to alphanumeric password standards and to Use Your Illusion (UYI) across the dimensions of efficiency, accuracy, OSA resistance, and subjective usability. User login times for both EaN and UYI met the efficiency usability standards established by alphanumeric passwords. Results for UYI (99%) login accuracy were significantly better than EaN (91%). And, UYI obtained a significantly higher Subjective Usability Survey score than EaN, with both schemes exceeding our usability requirement. Notably, EaN was shown to be resistant to OSAs while UYI was not. We suggest EaN might prove to be an effective next-generation authentication scheme for both frequent and intermittent users.

Keywords: Cybersecurity · Graphical authentication · Alphanumeric authentication · Over-the-Shoulder Attack

1 Introduction

Authentication is performed by a computing system in an attempt to verify a user's identity. The intent is to protect a user's valuable information (e.g., banking information, medical records). The most common form of authentication is the knowledge-based alphanumeric password [1]. However, to be effective, passwords must meet an array of requirements. Strong passwords ought to be long, contain numbers and symbols, and not use common dictionary words. Further, they should be different for every account, changed often, and not written down [2]. However, security requirements often make passwords hard to remember. This often leads to users employing workarounds and creating weak passwords. It has been suggested that the competition

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 81–95, 2019.
https://doi.org/10.1007/978-3-030-22351-9_6

between usability and security can be resolved by using innovate authentication schemes [3]. For example, graphical authentication passcodes are easy to remember by taking advantage of humans' affinity for encoding and recognizing visual objects (e.g., picture superiority effect). Unlike letters and numbers, images are encoded both visually and semantically into long-term memory [4]. Research has shown that pictures are easier to encode into long-term memory than an alphanumeric string [5]. Graphical authentication takes advantage of the fact that the user can make more meaningful associations with novel images compared with novel character strings. Graphical encoding allows the user to formulate context around the image and the richer this contextual information, the more strongly the image will be encoded in long term memory [6]. The increased strength of encoding images leads to a decrease in the decay of memory over time when compared to a less meaningful alphanumeric password. Clearly, the graphical authentication literature has demonstrated the memorability benefits of employing visual objects over alphanumeric characters. Though, developers are still searching for ways to overcome security concerns like Over-the-Shoulder Attacks (OSAs).

Cyber attacks are an issue for any authentication system. Alphanumeric passwords must beware of brute force attacks, which occur when an attacker inputs multiple password combinations until they gain access [7]. Conversely, graphical authentication schemes have often been criticized for their vulnerability to OSAs. This occurs when a casual attacker looks over the shoulder of someone employing a graphical authentication scheme in a shared space. And, both alphanumeric and graphical passcodes are vulnerable to a social engineering attack. If users create their own passcode, an attacker could produce an educated guess by learning more about a user (e.g., exploring social media posts to determine a pet's name or visual appearance). But, clearly, the most common criticism of graphical authentication schemes is their susceptibility to OSAs.

To defend against OSAs, researchers tend to use one of four strategies: grouping targets among distractors, disguising targets, using gaze-based input, or translating targets to another location [8]. For instance, the graphical authentication scheme, Passpoints, implements a grouping targets among distractors OSA defense strategy by allowing users to click on specific points within a picture [9]. The Use Your Illusion (UYI) graphical scheme, involves users recognizing a distorted target image from a set of distorted distractor images; this disguising targets technique interferes with the attacker's perception of the passcode [8, 10]. Other graphical schemes use gazed based input requiring users to select passcode targets using their eyes, thus making passcode observation difficult [11]. To further bolster security, some graphical schemes require users to translate target information to another location after the passcode target is recognized (WYSWYE) [12].

Again, graphical authentication employment of visual objects increases a user's ability to easily remember a passcode. Beyond the picture superiority effect, users only have to recognize their graphical passcode amongst a set of icons (c.f., multiple choice question) and not produce them like in an alphanumeric scheme (c.f., essay exam question). But, this benefit for easy memory retrieval comes at the cost of login efficiency. Visually searching for icons amongst distractors takes time. However, entering a well-practiced alphanumeric password is effortless and only takes a couple of seconds.

Uniquely, we attempt to take advantage of the memorability of graphical authentication schemes and the known efficiency of alphanumeric passwords. We proposed a new graphical authentication scheme Explore-a-Nation (EaN) that bridges the gap between graphical authentication passcodes and alphanumeric passwords. The EaN scheme uses the translating targets to another location OSA defense strategy. EaN provides users with a static image consisting of a map with context themed icons wherein an icon passcode path is hidden amongst other distractor icons. To improve memorability, the information provided by the passcode path icons is leveraged as clues that translate to a strong alphanumeric password. The user types the password that corresponds to the icons along their passcode path. The typed alphanumeric password consists of the first two letters of the target icon waypoints along the user's

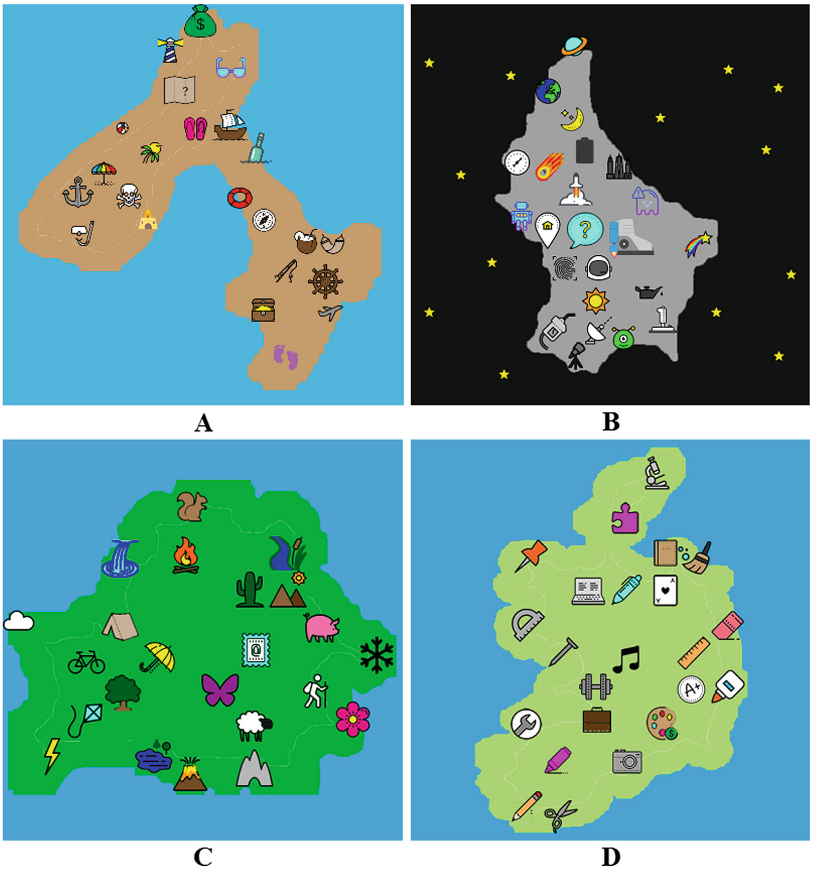


Fig. 1. (A) Blaze Map Passcode: treasure, feet, airplane, wheel, coconut, ? (Password: trfeaiwhco?). (B) Martian Map Passcode: gas, telescope, boot, !, rocket, home (Password: gatebo!roho). (C) Serendipity Map Passcode: @, pig, flower, sheep, umbrella, tent (Password: @piflshumte). (D) School Extravaganza Map Passcode: broom, eraser, ruler, dumbbell, camera, $ (Password: brerruduca$).

passcode path, except for one target icon that serves as a hint to the special character (see Fig. 1). As noted by Al Ameen [13], the cognitive abilities for both encoding and retrieval stages of memory are leveraged when users can view targets. Notably, if the user knows their password, it can simply be entered. The slower graphical scheme interactions only serve as a memory aid and are not a requirement of authentication. Therefore, the proposed EaN scheme ought to facilitate efficiency with sufficient practice.

The current study compared EaN to UYI a popular graphical scheme that disguises targets to prevent OSAs [10]. The purpose of our research was to assess the security requirements and usability of the EaN scheme across the dimensions of efficiency, accuracy, and subjective usability.

1.1 Usability and Security: Recognizing Standards and Creating Requirements

Login Efficiency. According to Still, Cain, and Schuster [3], authentication systems must allow for quick access in order to be efficient. Research conducted by Braz and Robert [14], revealed that the standard for alphanumeric password entry should be performed with login times that range from 7–20 s. Previous research has shown that graphical authentication passcode schemes tend to have longer login times than alphanumeric passwords [9]. Ideal alphanumeric alternative solutions should have shorter login times than those of some previously proposed graphical authentication schemes. More importantly, login times should be comparable to those established for alphanumeric passwords. To meet the standard usability requirement for efficiency, participants needed to be able to consistently enter their password as quickly as traditional alphanumeric passwords. Since EaN authentication requires users to type 11 characters and UYI only requires users to select three targets, we expected that UYI would reflect quicker login times given users are entering a novel passcode.

Accuracy. For a graphical authentication system to be usable, intensive training should not be required, and appropriate actions should be apparent for a wide range of users to ensure successful logins [3]. Previous research has shown that UYI consistently meets the usability requirement for accuracy [8, 10]. Additionally, a PIN entry graphical authentication scheme, that requires interactions similar to UYI, found login accuracy rates of 91% [15]. Perkovic and colleagues [16] found that their translating targets to another location graphical authentication scheme had login times of 8 s and 93% accuracy. A recent study compared the failure rates of graphical passcodes to alphanumeric passwords and yielded results for login inaccuracy rates that ranged from 11.59% to 13.01% [17]. We reasoned that participant login attempts for both the EaN and UYI graphical schemes would reflect average success rates of 90% to meet the standard usability requirements for accuracy. Since UYI needs users to select only three correct targets, while EaN requires users to correctly type 11 characters, we expected that accuracy would be higher for UYI login.

Subjective Usability. The Subjective Usability Scale (SUS) was used as a subjective measure of participant's usability experience [18]. If a login system is perceived as less usable, it may deter a user from using a website or program that employs that login method. Cain and Still [8] found that when users experience UYI for the first time they rated their experience with a SUS score of 65. We predicted EaN and UYI would follow the user requirement standards of ‘OK’ (e.g., SUS score of 51) or ‘Good’ (e.g., SUS score of 71) [19]. Since UYI uses a more familiar interaction metaphor, PIN entry, it would be rated as more usable.

OSA Resistance. Previous research suggests that the relative OSA resistance of a given graphical scheme can vary depending on the type of OSA defense strategy being implemented [8]. UYI disguises targets using image distortion in order to prevent OSAs [8]. Previous research proposes that images distorted at the optimal distortion level will simultaneously help users maintain recognition of targets and make the scheme more resistant to OSAs [20]. However, UYI has been shown to be vulnerable to OSAs when an attacker is permitted three or more viewings [8]. Research examining graphical schemes using a translating targets to another location OSA defense often find that when participants are asked to take the role of an attacker, they are unsuccessful at stealing a given passcode [21, 22]. We predicted the security of EaN will provide users with the same OSA resistance. Therefore, attackers will have 0% success in stealing an EaN password when given an unlimited number of views.

2 Method

2.1 Participants

Twenty-five undergraduate students (13 females, 2 left-handed, 24 reported English as their native language) were recruited from introductory psychology courses and were compensated with class research credit for their participation. Participants’ daily computing device usage ranged from 2 to 15 h (M = 5.54, SD = 2.94). Ages ranged from 18 to 25 years (M = 19.24, SD = 1.81). Twenty-three students indicated that they would accept additional authentication entry effort in order to prevent an OSA.

2.2 Materials Stimuli and Apparatus

Explore-a-Nation Map Prototype. The EaN prototype consisted of four different themed maps that were created using Adobe Photoshop and flat icons (retrieved from https://icons8.com/icon/set/map/all). Each map theme was comprised of a unique set of icons that pertained to a fictitious website’s theme: Blaze (beach), Martian (outer space), School Extravaganza, and Serendipity (outdoors) (see Fig. 1). Each map consisted of 23 unique icons matching the website’s novel theme, 17 distractor and 6 target icons. Two of the 23 icons contained an embedded special character. During EaN map creation, a temporary grid was placed on each map wherein each grid square was assigned a number. The icons were placed using the grid and a random number generator. After all icons were placed, the passcodes for each map were developed using the same grid and random number generator method. The passcodes consisted of a start and end icon with four icon waypoints in between, one of which contained an embedded special symbol. All passcode icons served as a reference to the associated alphanumeric password. The alphanumeric passwords consisted of the first two letters of each icon waypoint along the user's passcode path, except for one waypoint which served as a special character clue (see Fig. 1). Each strong password had 11 characters, contained no dictionary words, and had a special character (e.g., @piflshumte).

The EaN prototype authentication instructions were created for each map theme. Participants were shown both the targets and distractors on the map with an arrow highlighting the passcode path. The instructions went step by step for each passcode icon waypoint, informing users about the target icon and what characters should be translated into the typed password field (see Fig. 2). Participants were encouraged not to point to their passcode icons on the screen. Participants were informed that an image of the map would always be visible during login. Finally, they were given the complete alphanumeric password and instructed to type the password into the password field during login.

E-Prime 2 software was used to create the EaN authentication prototypes (see Fig. 3). The prototype was programmed to display asterisks during password entry. The prototype provided participants with feedback after they typed a password by displaying either "correct" or "incorrect". The E-Prime 2 software recorded login times in milliseconds from the start of password entry to submission and recorded user accuracy.

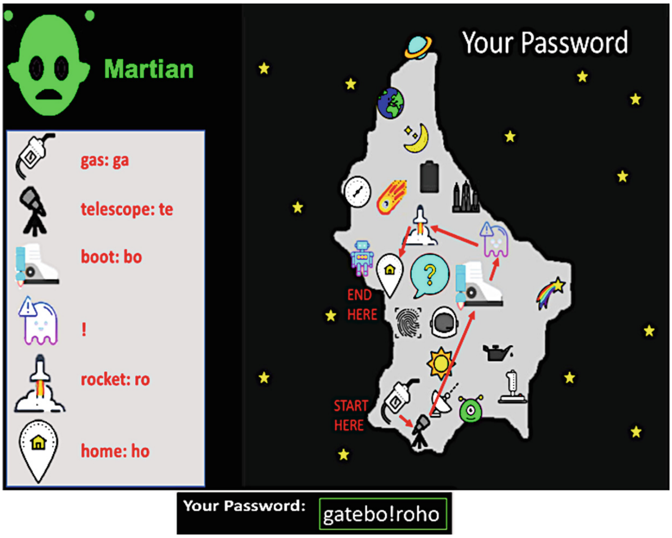
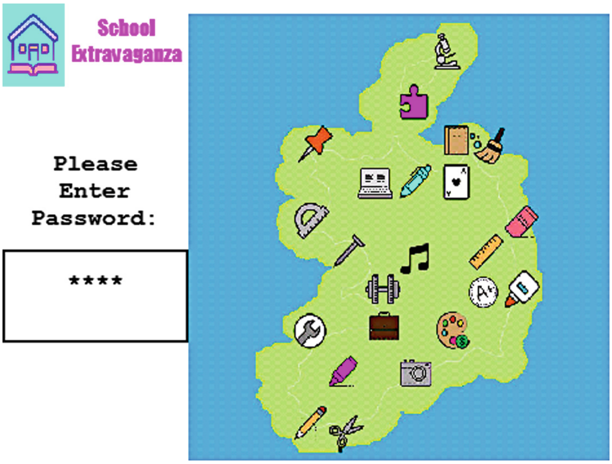


Fig. 2. A summarized representation of the Martian's website authentication instructions provided to participants in Microsoft PowerPoint.



Please Enter Password:

****

Fig. 3. A screenshot of the School Extravaganza EaN website authentication prototype implemented in the E-Prime experimental software.

Explore-a-Nation Over-the-Shoulder Attack Video. To test resistance against OSAs, a video of a researcher logging in to a fictitious food website, Craveology, was created and displayed to participants (see Fig. 4). The video was recorded with an iPhone 7 and captured the computer screen, the keyboard, and researcher's hands. The Craveology website was created using E-prime 2 software and followed the same creation procedure that was used when creating the EaN experimental prototype. A picture of the Craveology login screen was printed out and given to participants to refer to while viewing the video (see Fig. 4). The video was shown to participants in full-screen mode.

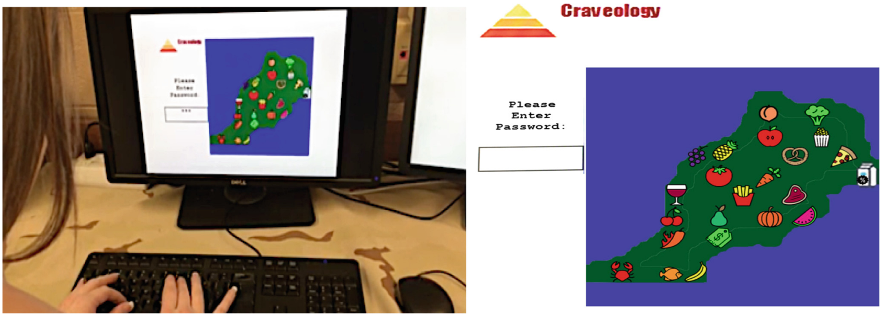


Fig. 4. The left image is a screenshot of the EaN OSA video which displays computer monitor and keyboard. The right image depicts the sheet printed and provided to participants while watching the video.

Use Your Illusion Prototype. Four fictitious websites were created using Paradigm software: Knitted Frog, Bean, GreenTech, and Hoppy Easter. Each website used UYI to authenticate. Each UYI website prototype was created with 27 images (24 distractors and 3 targets). Each website contained an independent set of 27 images. During login, participants were presented with the website information and given the passcode. The instruction depicted both the undistorted and distorted versions of the passcode images (see Fig. 5). Participants viewed three consecutive 3 × 3 grids. Each 3 × 3 grid contained one target and eight distractor images (see Fig. 5). All images were placed on the grid using a random number generator. The passcode targets were also selected using a random number generator. The Paradigm software recorded login times in milliseconds as well as participant input. The researchers verbally informed participants whether or not they successfully input the correct passcode.

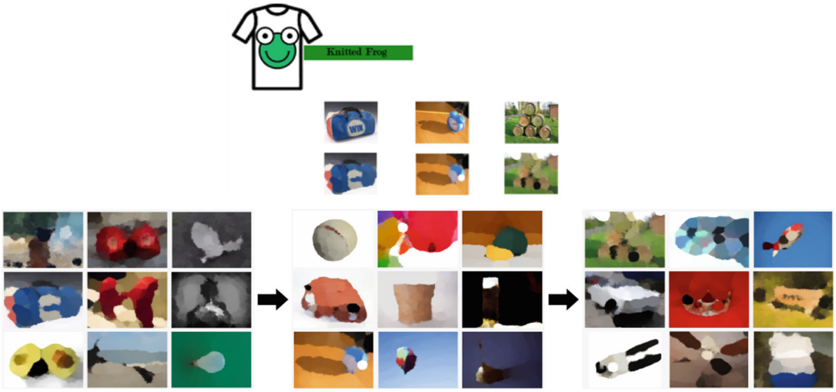


Fig. 5. The top image depicts a general version of what the instruction screen looked like for a given website theme. The bottom three images depict an example of the three 3 × 3 consecutive UYI prototype grids that would be shown during authentication.

Use Your Illusion Over-the-Shoulder Attack Video. To evaluate UYI OSA resistance, a video of a researcher logging in using the UYI system was created. Since a visible mouse cursor is used to select UYI passcode targets, the video was created using Tiny Take's screen recording feature on a computer monitor. The video captured the mouse clicking on the targets within the 3 consecutive 3 × 3 grids. The UYI prototype for the video was created using the same random placement method as the UYI experimental prototype. The set of 27 images used for the UYI OSA video was unique. A picture of all 27 images used in the UYI OSA video was printed on a single piece of paper and given to participants to refer to while viewing the video. The video was shown to participants in full-screen mode.

Usability Satisfaction Survey. Participant's subjective usability satisfaction was measured using the SUS after authenticating with both the EaN and UYI prototypes. The SUS is comprised of 10 items, and each question was scored using a Likert scale from 1 to 5 [18]. The SUS has been shown to have high reliability [23], and good correlation with performance measures [24].

2.3 Experimental Design and Procedure

Participants filled out an informed consent document and a demographics questionnaire. A fully within-subjects experimental design was used to compare the EaN and UYI. The experiment required participants to interact with the four different EaN website maps (Blaze, Martian, Serendipity, and School Extravaganza) and four different UYI websites (Knitted Frog, GreenTech, Bean, and Hoppy Easter). In addition, participants completed the associated SUS ratings and attempted to determine passwords from watching the OSA videos.

When participants interacted with EaN and UYI, they always assumed the role of the user first. To begin, they were shown a website's authentication screen and provided instructions. Participants informed the researchers when they had confidently memorized a password. Participants logged-in using a map 10 times for practice, followed by 10 logins that were recorded. These steps were repeated for all the maps for each prototype in the same presentation sequence. Participants rated their satisfaction of an EaN and UYI authentication experience by completing the SUS questionnaire.

Participants then assumed the role of an over-the-shoulder attacker. Participants were instructed to view the OSA video of an individual logging in to a website using the EaN authentication scheme. They were given the printed sheet of the website screen seen in the video and were informed they could view the video as many times as they desired. Participants informed the researcher when they were ready to guess the password. The researcher recorded the number of times the video was viewed and the participants' password guess.

3 Results

3.1 Authentication Login Efficiency

The data were cleaned by evaluating the EaN login efficiency data to determine if the different EaN website themes (e.g., Blaze, Martian, Serendipity, and School Extravaganza) had an effect on participant login time. The UYI login efficiency data were also cleaned by determining if the different website themes (e.g., Knitted Frog, Bean, GreenTech, and Hoppy Easter) affected participant login time. Boxplots were used to assess outliers and data discrepancies. Data cleaning resulted in removing data for three participants because their login data indicated times exceeding two standard deviations of the mean for the first EaN Blaze map. Additionally, an error in the EaN program allowed individuals to press ENTER without entering a password. This led to two trials where participants had login times of 100 ms. This accounted for less than 1% of the trials. Missing reaction times for these trials were replaced with the average reaction time for that participant on that map.

The researchers evaluated the login efficiency data to determine if the EaN and UYI authentication schemes had an effect on participant login time measured in seconds. The results indicated login speeds for EaN (M = 8.09, SD = 2.75) were significantly longer than the login speeds for UYI (M = 3.56, SD = 0.52), $t(24) = 8.33$, $p < .001$, $d = 1.67$. Longer login times for EaN were expected due to users having to type 11 characters versus only selecting 3 images for UYI. Overall, both authentication schemes obtained login times that met the usability standards for login efficiency (see Fig. 6).

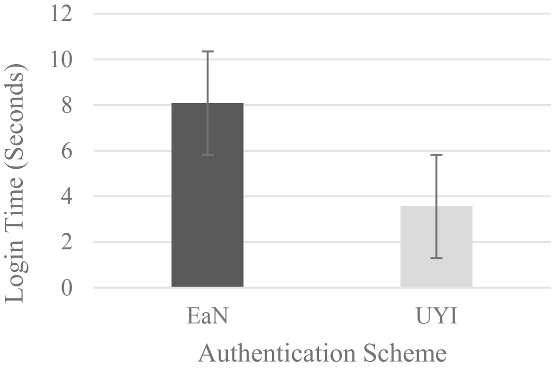


Fig. 6. Mean login times for EaN and UYI. Error bars represent standard error of the mean.

3.2 Authentication Accuracy

The data were cleaned by evaluating the login accuracy data to determine if the different themes affected authentication success. Boxplots were used to assess data discrepancies and outliers. There were outliers; however, excluding them did not significantly affect analyses. A one-way repeated measures ANOVA comparing accuracy for the four different maps indicated there was no difference in accuracy for the different EaN maps, $F(3, 72) = 0.45$, $p = .718$, partial $\eta^2 = .05$.

The researchers evaluated the login accuracy data to determine if the EaN and UYI authentication schemes affected accuracy. Users achieved significantly more accurate

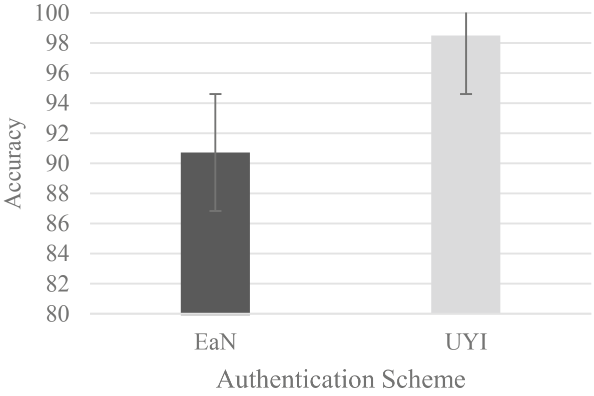


Fig. 7. Mean login accuracy for EaN and UYI. Error bars represent standard error of the mean.

logins using UYI logins (*M* = 99%, *SD* = 6%), when compared to the accuracy of EaN logins (*M* = 91%, *SD* = 9.7%), *t*(24) = 3.44, *p* = .002, *d* = .69. Overall, both authentication schemes obtained high authentication success rates that exceeded our 90% login accuracy usability requirement (see Fig. 7).

3.3 Casual Over-the-Shoulder Attacker Role

The researchers evaluated OSA data to determine if the EaN and UYI authentication schemes affected attacker success. Boxplots were used to assess data discrepancies and outliers. EaN was uniformly distributed at 0% success, while UYI was uniformly distributed at 100% success with a few, expected outliers when participants did not succeed in guessing the password. Excluding the UYI outliers did not significantly affect analyses. A paired-samples *t*-test revealed that OSA attempts were significantly more successful for UYI (*M* = 80%, *SD* = 41%) when compared to EaN attacker success (*M* = 0%, *SD* = 0%), *t*(24) = 9.80, *p* < .001, *d* = 1.96.

When participants attempted OSAs, they viewed the EaN login video (*M* = 7.60, *SD* = 3.95) significantly more times than the UYI video (*M* = 3.16, *SD* = 1.03), *t* (24) = 5.50, *p* < .001, *d* = 1.10. Overall, OSA attempts resulted in 0 accurate guesses for EaN despite more than twice as many average views compared to UYI (see Fig. 8).

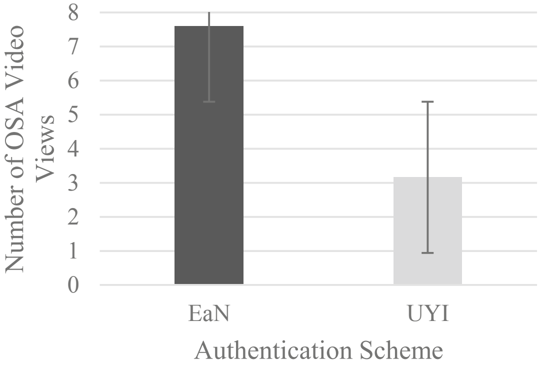


Fig. 8. Mean number of OSA video views of EaN and UYI authentication. Error bars represent standard error of the mean.

3.4 Subjective Usability Satisfaction

The researchers evaluated the SUS data to determine if the EaN and UYI authentication schemes affected satisfaction. Boxplots were used to assess data discrepancies and outliers. There were no outliers in the SUS data. A paired-samples *t*-test revealed that SUS scores for UYI (*M* = 81.90, *SD* = 10.78) were significantly higher than EaN (*M* = 69.60, *SD* = 16.56), *t*(24) = 4.692, *p* = .010, *d* = .92. Overall, both authentication schemes obtained SUS scores that surpassed our usability requirement (see Fig. 9).

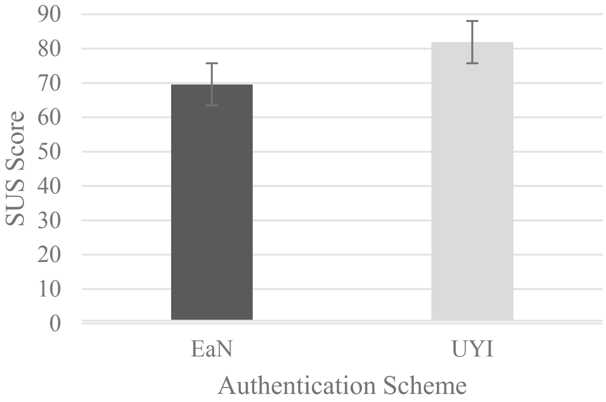


Fig. 9. Mean SUS scores for EaN and UYI. Error bars represent standard error of the mean.

4 Discussions

We proposed and evaluated EaN, a hybrid authentication scheme that combines a conventional strong password with a graphical authentication scheme. The EaN graphical scheme displays a map populated with icons which provides the user with clues for entering their strong password. We evaluated the usability and security of the proposed EaN graphical scheme by comparing it to the popular UYI scheme and to traditional alphanumeric password standards. We determined relative usability by evaluating user performance across the dimensions of efficiency, accuracy, and subjective satisfaction. Authentication security was measured by evaluating a schemes OSA resistance.

We found that both EaN and UYI allowed for quick authentication and met the usability standard for efficiency with login times falling between 7 and 20 s [14]. The login times for both EaN and UYI revealed users needed a maximum of 10 s to authenticate successfully. When compared to graphical schemes that use a translating targets to another location OSA defense, we determined EaN allowed more efficient account access than other schemes (c.f. WYSWYE and SSSL) [12, 16]. Our results for UYI were inconsistent with previous literature. We found that users needed between 2.9 and 5.3 s to login. Hayashi and colleagues found authentication UYI times between 11.5 and 24.7 s [10].

The accuracy usability requirement was determined by evaluating the rate of successful user authentication. To successfully authenticate, EaN login required users to type 11 characters correctly. On the other hand, UYI login only required users to select 3 targets correctly. As expected, we found that users were significantly more accurate when authenticating with UYI. EaN results indicated users achieved 91% accuracy rates on average. EaN accuracy met our usability requirement of 90%. However, UYI demonstrated near ceiling performance. It is important to acknowledge that UYI interactions can be mapped onto PIN entry authentication making its use more intuitive compared to our novel scheme [25].

Both EaN and UYI achieved SUS scores that exceed our usability requirement. Future EaN research should also look at other methods for collecting subjective data beyond the SUS. For example, interview questions could help pinpoint the aspects of the EaN authentication process where users felt improvements were needed.

To reach the authentication security requirements, we determined that casual attackers in the laboratory ought to ideally have 0% success performing an OSA when given one guess and unlimited views. And, indeed, the EaN resisted OSAs successfully. Results indicated the number of EaN OSA video views ranged from 2 to 19, regardless, 0% of participants playing the role of an attacker were able to guess the correct EaN password. These findings were consistent with results reported for schemes that also deploy translation to another location OSA defense strategies [21, 22]. However, the UYI scheme prevented OSAs only 20% of the time. UYI results indicated when participants view the UYI OSA video 1 to 5 times, they would successfully perform an OSA 80% of the time. These findings were consistent with previous literature that indicated UYI fails to prevent OSAs when attackers are given 3 or more OSA viewings [8].

Uniquely, the EaN scheme can equally provide a good usability experience for both frequent and intermittent users. In this study, authentication performance reflected first-time users who were required to learn how to use new schemes for authentication. According to Shneiderman and Plaisant [26], first-time users know the given task concept but lack the abilities resulting from extended practice. Typical graphical authentication requires users to complete a visual search. The targets being searched for are randomly placed within a display. This requires users to always complete a visual search, which takes effort and time. Requiring a few extra seconds to authenticate compared with alphanumeric is not a practical cost given the increase in memorability for intermittent users (e.g., accessing infrequent services: taxes, concert tickets). However, frequent users might be authenticating hundreds of times a week making efficiency a critical usability concern (e.g., accessing your laptop). Those users authenticating with their EaN password regularly, can transfer the password to procedural memory allowing for rapid and effortless logins. They simply enter their password without completing an inefficient visual search, but if they forget their strong password the map provides the necessary clues for recognition.

5 Conclusions

Over the past decade, numerous researchers have proposed various graphical authentication schemes, even though most prevent OSAs, they have failed to gain widespread implementation. We propose EaN might be capable of bridging the gap between strong passwords and graphical passcodes. Password authentication is facilitated by providing users with a static map image with an embedded icon passcode path, which helps users remember their strong password. Importantly, the EaN passwords generated from the passcode paths fulfill the recommendations for a strong password [2].

Results indicated the EaN authentication scheme surpassed the security requirements. And, participants (92%) indicated they would be willing to put forth additional authentication entry effort in order to prevent OSAs. In this case, learning the new EaN authentication scheme could be viewed as an acceptable effort, if they perceive an increase in security. Thus, the proposed hybrid EaN scheme is a promising authentication alternative that incorporates the benefits associated with graphical passcodes and the critical security aspects associated with strong alphanumeric passwords.

References

1. Zyiran, M., Haga, W.J.: Password security: an empirical study. J. Manage. Inf. Syst. **15**(4), 161–185 (1999)
2. Barton, B.F., Barton, M.S.: User-friendly password methods for computer-mediated information systems. Comput. Secur. **3**(3), 186–195 (1984)
3. Still, J.D., Cain, A.A., Schuster, D.: Human-centered authentication guidelines. Inf. Comput. Secur. **25**(4), 437–453 (2017)
4. Paivio, A.: Imagery and Verbal Processes. Psychology Press, New York (2013)
5. Madigan, S.: Picture memory. In: Yuille, J.C. (edn.) Imagery, Memory and Cognition: Essays in Honor of Allan Paivio, pp. 65–89 (1983)
6. Suo, X., Zhu, Y., Owen, G.S.: Graphical passwords: a survey. In: Proceedings of the 21st Annual Computer Security Applications Conference, pp. 463–472, December 2005
7. English, R., Poet, R.: The effectiveness of intersection attack countermeasures for graphical passwords. In: Proceedings of 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1–8. IEEE (2012)
8. Cain, A.A., Still, J.D.: Usability comparison of over-the-shoulder attack resistant authentication schemes. J. Usability Stud. **13**, 196–219 (2018)
9. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum.-Comput. Stud. **63**(1), 102–127 (2005)
10. Hayashi, E., Dhamija, R., Christin, N., Perrig, A.: Use your illusion: secure authentication usable anywhere. In: Proceedings of the 4th Symposium on Usable Privacy and Security, pp. 35–45 (2008)
11. De Luca, A., Denzel, M., Hussmann, H.: Look into my eyes! Can you guess my password? In: Proceedings of the 5th Symposium on Usable Privacy and Security. AMC (2009)
12. Khot, R.A., Kumaraguru, P., Srinathan, K.: WYSWYE: shoulder surfing defense for recognition based graphical passwords. In: Proceedings of the 24th Australian Computer-Human Interaction Conference, pp. 285–294 (2012)
13. Al Ameen, M.N.: The impact of cues and user interaction on the memorability of system-assigned random passwords (Doctoral dissertation) (2016)
14. Braz, C., Robert, J.M.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conference of the Association Francophone Interaction Homme- Machine, pp. 199–203. ACM (2006)
15. Brostoff, S., Inglesant, P., Sasse, M.A.: Evaluating the usability and security of a graphical one-time PIN system. In: Proceedings of the 24th BCS Interaction Specialist Group Conference, pp. 88–97, September2010
16. Perkovic, T., Cagalj, M., Rakic, N.: SSSL: shoulder surfing safe login. In: 17th International Conference on Software, Telecommunications & Computer Networks (SoftCOM), pp. 270–275 (2009)
17. Belk, M., Fidas, C., Germanakos, P., Samaras, G.: The interplay between humans, technology and user authentication: a cognitive processing perspective. Comput. Hum. Behav. **76**, 184–200 (2017)

18. Brooke, J.: SUS-A quick and dirty usability scale. Usability Eval. Ind. **189**(194), 4–7 (1996)
19. Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: adding an adjective rating scale. J. usability Stud. **4**(3), 114–123 (2009)
20. Tiller, L.N., Cain, A.A., Potter, L.N., Still, J.D.: Graphical authentication schemes: balancing amount of image distortion. In: Ahram, T., Nicholson, D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing, vol. 782, pp. 88–98. Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_9
21. Sun, H.M., Chen, S.T., Yeh, J.H., Cheng, C.Y.: A shoulder surfing resistant graphical authentication system. IEEE Trans. Dependable Secure Comput. **99**, 1–14 (2016)
22. Zangooei, T., Mansoori, M., Welch, I.: A hybrid recognition and recall based approach in graphical passwords. In: Proceedings of the 24th Australian Computer-Human Interaction Conference, pp. 665–673 (2012)
23. Bangor, A., Kortum, P.T., Miller, J.T.: An empirical evaluation of the system usability scale. Int. J. Hum.-Comput. Interact. **24**, 574–594 (2008)
24. Peres, S.C., Pham, T., Phillips, R.: Validation of the system usability scale (SUS): SUS in the wild. In: The Proceedings of the Human Factors and Ergonomics Society, vol. 57(1), pp. 192–196 (2013)
25. Still, J.D., Still, M.L., Grgic, J.: Designing intuitive interactions: exploring performance and reflection measures. Interact. Comput. **27**, 271–286 (2015)
26. Shneiderman, B., Plaisant, C.: Designing the User Interface: Strategies for Effective Human-Computer Interaction, 5th edn. Addison-Wesley Publishers, New York (2010, 2005)