Journal of the Nigerian Association of Mathematical Physics
Volume 65, (October 2022– August 2023 Issue), pp191 – 198

TOWARDS A FRAMEWORK ESTABLISHING SECURITY CRITERIA FOR RECOGNITION-BASED GRAPHICAL PASSWORD SCHEMES

Babatunde J. Odetayo and Binitie Amaka Patience

Department of Computer Science, Faculty of Physical Sciences,
University of Benin, PMB 1154, Benin City, Nigeria.
Computer Science Department, Federal College of Education (T) Asaba.

Abstract

The aesthetic and functional abilities of artforms have played significant role in different fields of study including securing standalone or networked computer systems and handheld devices. Though some studies have centered on humans as the weakest link in the security chain, recent assertions from literatures have shown that the choice of artforms in graphical password models and allowing users to choose their own artforms or click point within an artform during authentication have a direct effect on a system's security level. This research therefore establishes the feasibility of developing a security framework for mitigating the effects of cyberattacks in Recognition-based Graphical Password Schemes.

1. Introduction

Implementation of access control policies, standards often involve the identification of appropriate authentication mechanism, and the adopted access control mechanism are directly related to the criticality of the system being protected [1]. Current authentication techniques are divided into three main areas: *knowledge-based, token-based* and *biometric based* authentication. They can also be based on single factor models, two-factor models or multifactor models. It can also be classified based on where the user is located (location-based authentication) [2]. For some decades, authentication via the textual password model is being widely incorporated as part of access control for most systems. Textual or alphanumeric password falls under the domain of knowledge-based authenticating systems. In recent decades, the pervasive nature of the conventional textual passwords, which involves a combination of username and password (or PIN), has been declining because of security challenges [3]. These alphanumeric passwords, which are based on pure recall are a real challenge for users, for recognition memory is better than unaided recall [4].

To address security issues in computing systems, artforms have been used extensively as authenticated proofs and identities [5]. Sasse et al affirmed that users' choices of good or bad passwords are based on the useful information available to aid their understanding. They believed that the existing password system models have not done enough in this aspect to assist the users in choosing strong passwords [6, 7]. They faulted an opinion of users' inability to know and remember good password and indifferent concern about security when using artforms in Recognition-based Graphical Password Schemes as factors responsible for users choosing bad passwords. More so, research has found that users do not have a good understanding of the difference between a strong password and a weak password [7, 8].

Over many years, to address the password requirements, so many Recognition-based Graphical Password Schemes and studies with diverse objectives have been proffered, yet it has been proved that not all artforms generated could improve the security of the system [9, 10]. Also, implementation problems in Graphical Password Models are due to the difficulty in design of the password artforms that are memorable and secure, and in providing a large enough password space [9]. These findings show the importance and levels of security in Recognition-Based Graphical Password Schemes. The security of Recognition-Based Graphical Password Schemes depends to a large extent on the artforms the users are exposed to.

2. Related Works

Over the years, different appraisals have been conducted on Recognition-Based Graphical Password Schemes. Some researches focus on usability and security studies [11, 12, 13, 14] or exclusively on security [15] while some on reliability, usability and security studies [16][17][18]. Some evaluated existing models, building prototypes and carrying out user studies [19, 20, 21]. The following are the review of the some of the studies.

Davis et al designed Recognition-based Password Scheme called Face [13]. The Authentication Model makes use of people faces as password images. A study was carried out on the scheme to evaluate the strength of graphical passwords chosen by the users and its impacts on the security of Graphical Password System. The lab study consists of dataset collected during a semester from a set of students in which each student was randomly assigned to either of two Graphical Password Schemes (Face or Story) to access their grades, homework, homework solutions, and course reading materials. At the end of the semester, the students were asked to complete an

Corresponding Author**:** Babatunde J.O., Email: babatunde.odetayo@uniben.edu, Tel: +2347035901508

exit survey in which they were to state why they chose the faces they did or their chosen stories and provide some demographic information about themselves. The analysis of the results of the experiments indicates that the faces chosen by users in the Face scheme is highly biased by the race of the user, and that the gender and appealingness of the faces also exert influences on the password choices. Both male and female participants selected female faces far more often than male faces, and then picked attractive ones more often than not. It could be deduced that hotspots or biased arts in an artform used in Recognition-based Graphical Authentication Scheme can influence users' choices of password. This poses serious like Guessing attack to the security of Authentication Systems. It was suggested that measures should be put in place to prevent such hotspot-prone cyberattacks. Suggested alternatives for mitigating this threat includes prohibiting or limiting user choice of passwords and educating users on better approaches to select passwords, or to select artforms less prone to these types of biases.

Another Recognition-Based Graphical Password Schemes known as Passpoint was developed and tested in a lab with Eighty-three computer-compliant students [14, 22]. Two issues were considered in this experiment: the effect of tolerance, or margin of error, in clicking on the password points and the effect of the password interface used in the authentication system. The students authenticated using Passpoint Graphical Password Model with tolerance (20 x 20 pixels). They were provided with four different artforms. Results in the tolerance study shows that the participants were quite successful using tolerance 20 x 20 pixels but accurate memory for the password was strongly reduced when using a smaller tolerance (10 x 10 pixels) around the user's password points. They attributed this effect to users' inability to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time. Furthermore, the results of users' performance on four everyday artforms showed that users performed relatively well in some artforms than the others. This indicated that there are possibilities for some password images to perform poorly than the others and this can jeopardize the security of the system. The findings established the fact that password images (artforms) used in Graphical Authentication Systems have an enormous impact on the memorability, usability and thus, the security of the system. It suggested the likes of artforms that should be avoided in the implementation of Graphical Authentication System. It includes users' personal choice of artforms which users are fond of and attackers could identify.

Another study showed how password interface can affect the security of the authentication system by using different password interfaces presented by three click-based graphical password schemes, namely PassPoints, Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) passwords [12, 23]. One of the findings of the experiment reveals that the design of the password interface in Recognition-Based Graphical Password Schemes can influence users' selection of passwords in predictable patterns. Therefore, they theorized that the design choice of password artforms, affects the security of Graphical Authentication system. Moreso, they noted that design choices, which subtly alter user selection of passwords, can not be made naively because they may weaken security. These design choices may lead users to employ coping mechanisms and pave ways to making insecure choices, or make the insecure option most logical or most convenient from a user's perspective. It was concluded that the design of the password interfaces of authentication systems influences users' choices of passwords and may encourage either secure or insecure behaviour.

Jackson reviewed related works on Graphical Password Schemes, and further designed a prototype that could be used to test the possibility of artform-based authentication system which he considered as the main security method of the future [24]. The prototype consists of three password interfaces which are; a picture-based, a facial picture-based and a story-based. He conducted five different experiments to test the memorability, usability and security of the prototype. The results of the experiments indicated that the levels of the memorability of the three interfaces were slightly below 90% of the total participants involved in the experiments. The best memorable interfaces among the three were the Story-Based and Picture-Based interfaces. 89% of forty-five registered password were recalled successfully after a week of registration. He asserted that the Story-based was the best among the three interfaces in term of memorability. He justified this outcome based on the fewer number of passwords to be recalled in Story-based interface compared to other interfaces. Though, in Picture-based interface, some subjects with lesser number of passwords still had difficulty in remembering them. He attributed the success of high memorability in Story-based to methodology users adopt to create passwords appealing to themselves. He noted that Facial picture-based interface scored the least among the three in term of memorability but yet the most secure. He affirmed that the Picture-based interface is a sensible middle ground between the usability and security. With the prevailing threat of Brute force Attacks on Story-based interface, he noted that more works are needed to be done on the security of Artform-based Password System.

[25] improved on the model of [26] and showed how it relates to user-selected Recognition-based Graphical Password Schemes. The experiment was centered purely on automated techniques for guessing attacks. They evaluated various methods of the automated attacks on Recognition-based Graphical Password Systems based on click-order-patterns. It aimed at identifying attractive points (hotspot) users are likely to select by using artform processing method. The automated technique combines click-order-patterns with visual attention models. They considered two approaches: DIAG and LINE. While DIAG click-point-pattern captures arcs that are consistent in both horizontal and vertical directions LINE captures only horizontal and vertical lines. The outcome was examined using two categories of visual attention models: Bottom-up and Top-down, and Saliency Toolbox implemented in Matlab [27]. For each, two different styles of generating a dictionary for use in a guessing attack was examined. To allow meaningful comparison, the methods were tested by trying to guess users' graphical passwords, using a previous PassPoints user study password database [14, 22]. The results show that automated attacks, which are easier to arrange than human seeded attacks, are more scalable to systems that use multiple artforms and posed a significant threat. Importantly, they noted that the attack results are artform-dependent. This shows the impact of password artform used in the implementation of Recognition-Based Graphical Password Schemes on users' choices of secure or insecure passwords.

Further studies attributed the security breaches in Recognition-Based Graphical Password Schemes to the inability of the system to make a provision for human limitations [10]. Two human limiting factors were: the difficulty people have when comparing meaningless string

and memorizing strong passwords and PINs, were examined. The study made use of random arts for automatic generation of artistic artforms. Results showed that the Graphical Password Schemes need to account for human factors by making adequate provisions for human limitation. The prototype developed complimented human limitation in comparing meaningless string and memorizing strong passwords/PINs by converting them to structured artforms which has been proved to be very good in this aspect (hash visualization). However, in their work, they discovered that not all artforms generated were usable or improve the security of the system [14, 22]. They suggested more works on users' perceptions of generated artforms, and how to generate recognizable and secured artforms.

[28, 29, 30] argued that the security of Recognition-Based Graphical Password Schemes has received little attention. They believed that the issue of the security of Recognition-Based Graphical Password Schemes remains largely unaddressed. They claimed that the effect of hotspots has been downplayed. Thus, they examined the security of Recognition-Based Graphical Password Schemes including the effects of different graphical password interfaces, and strategies for guessing user passwords. They focused on a security analysis of an implementation with the same parameters as used in a recent PassPoints publication [22]. They conducted empirical studies and confirmed the existence of hot-spots and postulated that some artforms are more prone to hot-spotting than others.

English noted that researchers often focus on new schemes, usability studies or propose counter-measures to specific attacks. The author argued that though these focuses are very important, the analysis has been inconsistent. The author based their assertion by citing the work of Hlywa et al which proposed an approach in calculating the password entropy (guessability) of a Recognition-Based Graphical Password Schemes [31] and the work of DeAngeli et al which proposed a different approach to measure guessability [32]. The author arguably pointed out that there is no standardised method of measuring the level of security of a Recognition-Based Graphical Password Schemes. This finding led to their proposal of a metric that allows the security of Recognition-Based Graphical Password Schemes to be measured and compared in terms of resistance to four identified attacks. These attacks include; random guessing, guessing based on category bias (semantic guessing), frequency attacks, and shoulder surfing attacks. The purpose of the authors work was to develop a model by which the security of two Recognition-Based Graphical Password Schemes can be compared based on any of the identified attacks in focus. They implemented the metric model by comparing the security of the PassFaces scheme with the security of the adapted VIP1 scheme. They discovered that PassFaces scheme is more secure in terms of frequency attacks. The adapted VIP1 scheme is more secure against random guessing and marginally more secure against shoulder surfing attacks due to the password interface set size. Both schemes are equally secure against SOGAs since pass-artforms are assigned to users. Also, if shoulder surfing is not a concern then the PassFaces scheme may be a better choice.

3.0 Basic Cyberattacks in Recognition-based Graphical Password Schemes.

From the reviewed studies and other literatures, various basic attacks in Recognition-Based Graphical Password Schemes (RGPS) were identified as shown in Table 1.

Table 1: Cyberattacks in RGPS

S/N	Cyberattacks in RGPS	Literatures Review
1	Dictionary Attack	[10, 15, 21, 25, 27, 28, 29 30,33, 34, 35, 36, 37, 38, 39]
2	Brute Force	
3	Spyware	
4	Shoulder Surfing	
5	Social Engineering	
6	Guessing	
7	Intersection Analysis	

3.1 Dictionary Attack:

Dictionary attack attempts to break through an authentication system by using trial-and-error methods of recognizing pass images with likely possibilities in a systematic way. A possible selected list is used to crack the pass images starting from the priotized entries among the list. Recognition Graphical Password Schemes are less vulnerable to dictionary attacks compare to Textual Password System. The attack activity would require more effort and time in Recognition-Based Graphical Password Schemes than textual passwords or Recall-based Graphical Password Schemes because of the use of mouse input type recognition.

3.2 Brute Force Attack:

While the attacker tries a list of known or commonly used passwords in dictionary attack, In Brute Force Attack the attacker does not use a list of passwords, instead, he aims at trying all possible combinations in the password space. Due to large amount of effort and time these attacks consume, Hackers rely on automated tools such as Aircracking, John the Ripper, Hashcat, Ncrack, DaveGrohl to help in brute force attacks. These tools can be used on various operating system platforms such as Windows, Linux, iOS, Android and Mac OS to breach the security of the system. Comparatively, Graphical Authentication Systems are less susceptible to Brute force attack because of numerous input mouse motions. it is more difficult and complicated to use the automated dictionary method to produce all possibility of a single user click of an image than a text-based attack.

3.3 Guessing

Guessing is a form of both dictionary and bruteforce attacks in which an attacker performs repeated log-on trials by assuming possible values of the authenticator pass images. Password guessing could be offline or online dictionary attacks. Hackers prey on users' personal likes and preferences to predict their passwords. Graphical password entropy tries to determine the probability that the hacker would be able to find the correct password using random prediction. Equation 1 shows the password entropy formula.

Password Entropy = N log2 (|L||O||C|) …….Eq1

Where N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet and C is colour of the alphabet, provided all the passwords are distributed evenly[27].

3.4 Spyware:
This malicious software is secretly installed on a computing device without the end user's knowledge. It aims to record the key or mouse movement of the user when operating the device and relays it to the hackers. These key-logging and listening malwares have not been proven to be effective in Graphical Authentication Systems. Only recorded strokes cannot perform the malicious job without other information such as Window size and position.

3.5 Shoulder-surfing:
As the name implies, means an attacker looking over the user's shoulder to steal vital information [40]. This kind of attack is common in a crowded place such as the banking hall and shop mall. Humans or video recorder can be used to observe users' privacy. Both text-based and graphical passwords are susceptible to shoulder surfing attacks. The best method to prevent shoulder surfing is to be conscious and prevent secret eyes all around. Many Recognition-based Graphical Password Schemes are susceptible to this threat.

3.6 Intersection analysis:
Hackers can use the intersection of two or more sets of images to identify the pass images. Intersection analysis is feasible In Deja vu, where all the password images are part of the challenge sets, and decoy icons are changed in each round. Graphical Authentication Systems that uses multiple images choice as pass objects are also vulnerable to intersection attack.

3.7 Social engineering:
Social engineering is a wide range of fraudulent activities accomplished through human interactions. It uses psychological manipulation to trick users into disclosing their sensitive information, in this case passwords to hackers. While some Graphical passwords (such as random arts) could be difficult to disclose by description, some pass objects with distinctive names can be given away through malicious interactions between the users and the hackers.

4.0 Security Measures in Recognition-based Graphical Password Schemes.
Table 2 shows various security measures identified through literature studies and can be implemented to mitigate the effect of cyberattacks respectively in Recognition-Based Graphical Password Schemes.

Table 2: Security measures against cyberattacks in RGPS

S/N	Attacks	Mouse Input. [25,35,38]	Large Password Space. [25, 33,35, 37, 38,39]	Image variation. [35, 41, 42]	Hash visualization [10, 34, 35, 36,]	Unbiased content. [23,12,13,35,28]	Randomly Assigned Image [43, 35, 41, 37]	Users' Assigned image [33, 35,44, 31]	Repeat Verification [13, 34,35]	Hybrid Method [43,36,42, 18]
1	Dictionary Attack	√	√		√	v	√	√		√
2	Brute Force	√	√					√		√
3	Guessing		√	√	√	√			√	√
4	Spyware	√						√		
5	Shoulder Surfing			√			√	√		√
6	Intersection Analysis		√	√			√		√	
6	Social Engineering					√				√

4.1 Large Password Space (LP):
The theoretical password space of a graphical password scheme is a security strength indicator determined by the total number of possible passwords. As for text passwords, the size of the theoretical password space depends on the number of available characters and the password length. The password space in text-based passwords is shown in Equation 2.

Password Space = (94)^K 2
94= printable number of characters excluding the space and
K= length of password.

Recognition-Based Graphical Password Schemes stand the chance to have larger password space than text-based password. In Recognition-Based Graphical Password Schemes, password space is the relative size of the Graphical Interface that can be used as passwords by users. Recognition-Based Graphical Password Schemes make it possible to adopt a multiple-page authentication system which can invariably increase the password space of the system. The larger the password space, the harder for brute force and guessing to succeed.

To compute the amount of password in Recognition-Based Graphical Password Schemes involves some considerations. The popular technique is based on numbers of images contained in different pages of the selection and gives no consideration to the fact that an image can be selected more than one time. [36, 45] put this exception into consideration in their proposed formula for measuring the size of password space. In equation 3, y is the total number of pictures, z is Password length and x is the maximum password length.

$$Password\ Space = \sum_{z=1}^{x} \left(\frac{y+z-1}{y-1}\right) = \sum_{z=1}^{x} \frac{(y+z-1)!}{z!(y-1)!} \quad 3$$

Large Password Space (LP) is a good security feature to check cyberattacks such as Dictionary attack, Brute force, Guessing and Intersection Analysis. Therefore, this research paper expressed it mathematically as seen in Equation 4. In this equation, Large Password Space (LP) contains the set of attacks it can mitigate their threats.

LP = {DA, BF, G, IA} 4

Where DA = Dictionary Attack,
BF = Brute Force,
G = Guessing and
IA for Intersection Attack.
Similar mathematical expression is used for other cyberattacks.

4.2 Mouse Input (MI):

Technically, GPM uses mouse input type recognition for password selection. This distinctive feature of GPM makes the Graphical Authentication System more formidable to cyberthreats such as dictionary attacks, brute force and spyware attacks. These attacks are well associated with text-based password system. it can be denoted mathematically as shown in Equation 5

MI = {DA, BF, S} 5

Where DA = Dictionary Attack,
BF = Brute Force and
S = Spyware.

4.3 Randomly Assigned Image (RA):

Randomly assigned Image is automatic selection of pass images by the system for authentication. This security feature guarantees more secured passwords as it applies to textual passwords as well. It is certain that system generated passwords is more difficult for attackers to hack than user-generated passwords because all the principles that guides the formation of very strong passwords were observed. This strength comes with a tradeoff in password usability measure. The harder the password, the more difficult it is to remember. Randomly Assigned Password security feature can mitigate the effect of cyberattacks such as Dictionary Attacks, Intersection Analysis and Shoulder-surfing attacks. It is mathematically expressed as seen in Equation 6.

RA = {DA, IA, SS} 6

Where DA = Dictionary Attack,
IA = Intersection Attack and
SS = Shoulder surfing attack.

4.4 Image Variation (IV):

This implies that the same image is displayed in different colors, textures, lines and so on. This technique can discombobulate intruders on valid password, and by this, strengthens the system against cyberattacks such as guessing, shoulder surfing and Intersection Analysis. It is denoted mathematically as seen in Equation 7.

IM = {G, SS, IA,} 7

Where G = Guessing,
SS = Shoulder surfing and
IA = Intersection Attack.

4.5 Hash Visualization (HV):

This technique generates images from strings. It replaces meaningless string with structured images. It can effectively manage security threats associated with Dictionary and Guessing Attacks. It is mathematically expressed in Equation 8.

HV = {DA, G} 8

Where DA = Dictionary Attack and
G = Guessing attack.

4.6 Unbiased Content (UC):

This security feature ensures that hotspots in chosen artforms are eliminated or reduced. It screens out artforms with biased contents that can play on the intelligence of the users to choose vulnerable passwords. Unbiased Content features can fortify the authentication system against cyberattacks such as Dictionary attacks, Guessing and Social Engineering. The set of cyberattacks Unbiased Content (UC) can mitigate can be expressed mathematically as seen in Equation 9.

UC = {DA, G, SE} 9

Where DA = Dictionary Attack,
G = Guessing and
SE = Social Engineering.

4.6.1 Users' Assigned Image (UI):

Users' Assigned Image security feature enables the users to make use of image passwords on carriable peripheral devices such as mobile phones. This is similar to OTP (one Time Password) generated machine usually called hardware token in textual password system. This implies that the user image passwords are situated outside the hardware system. This security technique can fortify the authentication

systems against Dictionary attack, Brute force, Spyware and Shoulder surfing attacks. The set of cyberattacks Users' Assigned Image (UI) can mitigate can be expressed mathematically as seen in Equation 10.

UI = {DA, BF, S, SS} 10

Where DA= Dictionary Attack,
BF = Brute Force, S = Spyware and
SS = Social Engineering.

4.7 Repeat Verification:

Repeat verification feature involves users going through more than one verification process before access is given. Users are provided with multiple pages of password interface through which a certain number of pass-images could be selected per each page at the registration stage. This process is repeated at the verification stage. The password interface could appear serially or randomly at the verification stage. This security feature can mitigate against various forms of guessing and shoulder surfing attacks. It also increases the password space of authentication scheme and thus makes dictionary and brute force attacks more difficult. This expressed in Equation 11 mathematically.

RV = {DA, BF, G, IA} 11

Where DA = Dictionary Attack,
BF = Brute Force,
G = Guessing and
IA = Intersection Attack.

4.8 Hybrid Method:

Hybrid method is the combination of recalling with recognition of passwords. Many Graphical Authentication systems use hybrid method to strengthen the system against multiple cyberattacks. This method comes with a great price of slow verification process. It can mitigate the threat of Shoulder surfing and guessing attacks as it is mathematically expressed in Equation 12.

HM = {SS, G} 12

Where SS = Shoulder surfing and
G = Guessing.

5.0 Discussion.

From our study, we identified the cyberattacks that are connected to Recognition-based Graphical Password Schemes (RGPS). These are a set of Dictionary Attack (DA), Brute Force (BF), Guessing (G), Spyware (S), Shoulder Surfing (SS), and Social Engineering (SE) and are represented mathematically in Equation 13.

Cyberattacks (RGPS) = {DA, BF, G, S, SS, SE} 13

The corresponding security measures to combat all the Cyberattacks discussed in this article, is evaluated in Equation 14.

Security Measures = {MI, LP, IM, RI, HV, UB, UI} 14

From Equation 2 to Equation 10, the minimal security measures which can be implemented in RGPS to safeguard the system against mentioned cyberattacks, is deduced, as represented in Equation 15.

{UC} *U* {UI} = {DA, BF, G, S, SS, SE} 15

The last mathematical expression shows that only the combination of Unbiased Contents (UC) and User Assigned Images (UI) can give the set of all the listed cyberattacks. This invariably means that implementing the security measures of Unbiased Contents (UC) with Users' Assigned Image (UI) in RGPS will fortify the system against all the six attacks evaluated under this study, which are Dictionary Attack (DA), Brute Force (BF), Guessing (G), Spyware (S), Shoulder Surfing (SS), and Social Engineering (SE). Other benefits of this finding are listed below

1. The combination gives a good trade-off between Usability and Security.
2. Easy to implement
3. Saves the server from large pictures storage which makes most RGPS very slow.
4. Highly memorably and user-friendly.
5. Very good resistant to Shoulder surfing attacks that threatening all RGPS.
6. Future RGPS can study and adopt this security framework.

6 Conclusion and Future works

In this study, we reviewed the assertions of security experts on the security features of Recognition-Based Graphical Password Schemes. These findings show that the security of Recognition-Based Graphical Password Schemes depends largely on the nature and form of images available for use as passwords. Furthermore, from the literatures, we identified and examined the common cyberattacks connected to Recognition-Based Graphical Password Schemes which are Dictionary Attack (DA), Brute Force (BF), Guessing (G), Spyware (S), Shoulder Surfing (SS), and Social Engineering (SE). More so, from various recommendations of Graphical Authentication Security experts, we identified and evaluated the corresponding security measures which can be implemented to mitigate the identified security threats. Finally, we discussed the minimal security measures that can be implemented to strengthen the Recognition-Based Graphical Password Scheme against cyberattacks. Our finding revealed the combination of Unbiased Content with Users-Assigned Image security features can mitigate the effects of all the listed cyberattacks. This combination proves to be user-friendly, require less storage facility and easy to implement as well.

In future works, we intend to use the security features discussed in this study to assess and rate some common Recognition-Based Graphical Password Schemes. This will form a useful framework to aid users of RGPS in selecting the Recognition-Based Graphical Password Scheme suitable to their needs.

ABOUT THE AUTHORS

Babatunde John Odetayo is a lecturer in the Department of Computer Science, Faculty of Physical Sciences, University of Benin, Benin City, Nigeria. He holds his M.Sc. degree in Software Engineering and currently undertaking his Ph.D. research on network security from University of Benin, Benin City. His other areas of interest include cybersecurity, E-commerce and Artificial Intelligence.

Amaka P. Benetie is a lecturer in the Department of Computer Science, Federal College of Education Technical Asaba, Delta State, Nigeria. She obtained her M.Sc. degree in Computer Science from Adamawa State University, Gombe State and she is currently undertaking her Ph.D. research on E-commerce security from University of Benin, Benin City. She is a member of Nigeria Computer Society (NCS). Her research interests are in the areas of information and cybersecurity, and Artificial Intelligence.

References

[1] Li N., Wang Q., Qardaji W., Bertino E., Rao R., Lobo J., and Lin D. (2009). Access control policy combining: theory meets practice. *Proceedings of the 14th ACM symposium on Access control models and technologies*, 135-144. doi: http://doi.acm.org/10.1145/1542207.1542229.

[2] Choi, M., Lee, J., Kim, S., Jeong, Y.S., and Park, J.H. (2016). Location based authentication scheme using ble for high performance digital content management system. Neuro computing, 209, 25–38.

[3] Kucken M. and Newell A. (2004). Fingerprint formation. *Journal of Theoretical Biology* 235, 71–83

[4] Norman, D.A. (1988). The design of everyday things, basic books, New York.

[5] Samdanis, M. (2016). The impact of new technology on arts. In book: Art Business Today: 20 key Topics. Lund Humphries Publishers ltd,, 164-172.

[6] Sasse, M. A., Brostoff, S. and Weirich, D. (2001). 'Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security', *BT Technical Journal*, 19, 122-131.

[7] Adams, A., and Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM* 42(12), 40-46.

[8] GehringerE.(2002). Choosing passwords: security and human factors. *ISTAS* 39-373.

[9] Anap A. B., Nibe A. A. and Tamboli V. S. (2016). Secure graphical password requirements. Available at: https://www.ijraset.com/fileserve.php?FID=4053

[10] Perrig, A. and Song, D. (1999). 'Hash visualization: A new technique to improve realworld security', *International Workshop on Cryptographic Techniques and Ecommerce*, 131–138.

[11] Conlan R. M. and Tarasewich P. (2006). Improving Interface Designs to Help Users Choose Better Passwords. Available at: https://www.embracetherandom.com/changePasswordUIStudy/Improving%20Interface% 20Designs%20To%20Help%20Users%20Choose%20Better%20Passwords.pdf

[12] Chiasson S., Forget A., Biddle R. and van Oorschot P. C. (2008). User interface design affects security: Patterns in click-based graphical passwords. Available at: https://cups.cs.cmu.edu/~aforget/Chiasson_IntJInfSecDec2009_Patterns.pdf

[13] Davis, D., Monrose, F. and Reiter, M. K. (2004). On user choice in graphical password schemes. Available at: http://www.usenix.org/events/sec04/tech/full_papers/davis/davis_html/index.html.

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

[15] English R. (2014). Modelling the Security of Recognition-Based Graphical Passwords. Available at: https://pdfs.semanticscholar.org/a17c/8c3c9da41e5541f8b53b57ed233067f74a6f.pdf.

[16] Bianchi A., Oakley I. and Kim H. (2015). PassBYOP: Bring Your Own Picture for Securing Graphical Passwords. Available at: http://alsoplantsfly.com/files/2016/Bianchi_Passbyop_IEEE16.pdf

[17] Tari, F., Ozok, A., and Holden, S. (2006): A comparison of perceived and real shoulder-surfing risks between alphanumeric and image-based passwords. *Proceedings of the Second Symposium on Usable Privacy and Security*, 149, 56 – 66.

[18] Wazir K., Mohammed A. and Yang X. (2011). A Graphical Password Based System for Small Mobile Device. *International Journal of Computer Science* 8 (5) 145-154.

[19] Dirik A. E., Memon N. and Birget J. (2007). Modeling user choice in the PassPoints graphical password scheme. Available at: https://isis.poly.edu/memon/pdf/2007_modeling%20user.pdf

[20] Jackson L. (2006). Analysis of Image-Based Authentication and its Role in Security Systems of the Future. Available at: http://www.soc.napier.ac.uk/~bill/lee2006.pdf.

[21] Salehi-Abari A., Thorpe J., and van Oorschot P. C. (2008). On Purely Automated Attacks and Click-Based Graphical Passwords. Available at: http://www.cs.toronto.edu/~abari/papers/passpoints_acsac08.pdf

[22] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy A., and Memon, N. (2005a): Authentication Using Image-based passwords Effects of Tolerance and Image Choice. Available at: http://portal.acm.org/citation.cfm?id=1073001.1073002

[23] Chiasson S., Biddle R., and van Oorschot P. (2007). "A second look at the usability of click-based graphical passwords," *Proc. 3rd Symp. Usable Privacy Security*, pp. 1–12.

[24] Rao P., Devi G. and Rao S. (2013). A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach. *Journal of Computer Engineering*, 10 (6), 14-20.

[25] Itti L., Koch C. and Niebur E. (1998). A Model of Saliency-Based Visual Attention for Rapid Scene Analysis. *IEEE Trans.* PAMI, 20(11):1254–1259.

[26] Touraj K. and Alizadeh M., Gholizadehb G., Zamanic M. and Darvishid M. (2015). Security Analysis Method of Recognition-based Graphical Password. *Journal of Technology (Sciences & Engineering)*. 72(5), 57–62. DOI: 10.11113/jt. v72.3941

[27] Thorpe J. and van Oorschot P. C. (2004a), 'Graphical dictionaries and the memorable space of image-based passwords', *Proceedings of the 13th USENIX Security Symposium*, 9-13, San Deigo, USA.

[28] Thorpe J. and van Oorschot P. C. (2007). Towards Secure Design Choices for Implementing Image-based passwords. Available: http://www.acsac.org/2004/papers/48.pdf.

[29] Thorpe J. and van Oorschot P. C. (2007). Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. Available at: https://www.ccsl.carleton.ca/paper-archive/usenix07.hotspots.pdf

[30] Hlywa M., Biddle R., and Patrick A. (2011). Facing the facts about image type in recognition basedgraphical passwords. *Proceedings of the 27th Annual Computer Security Applications Conference*, 36, 149–158.

[31] De Angeli, A., Coutts, M., Conventry, L., Cameron, D., Johnson, G.I. and Fisher, M. (2002). 'VIP: A visual approach to user authentication', Proceedings of the Working Conference on Advanced Visual Interfaces (AVI 2002), ACM Press, New York, pp. 316-23.

[32] Binnar P. and Mane V. (2015). Usability and Security of Recognition based Graphical Password Scheme. *International Journal of Computer Applications* (0975 – 8887).

[33] Dhamija, R. (2000). Hash visualization in user authentication. Available at: http://people.ischool.berkeley.edu/~rachna/papers/hash_visualization.pdf.

[34] Hafiz M., Abdullah A., Ithnin N. and Mammi H. (2008). Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. *Second Asia International Conference on Modelling & Simulation.* DOI: 10.1109/AMS.2008.136.

[35] Lashkari A. and Farmand S. (2009). A survey on usability and security features in graphical user authentication algorithms. *International Journal of Computer Science and Network Security*, 9 (.9), 195 – 204.

[36] Nwokedi U., Onyimbo B. and Rad B. (2016). Usability and Security in User Interface Design: A Systematic Literature Review. *Information Technology and Computer Science*, 5, 72-80.

[37] Touraj K., Muzahidul I., Sabariah B., Shozo K. (2016). Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes. *International Journal of Electrical and Computer Engineering* 6 (6), 2939 – 2948.

[38] Towhidi F. and Masrom M. (2009). A Survey on Recognition-Based Graphical User Authentication Algorithms. *International Journal of Computer Science and Information Security*, 6(2). ISSN 1947-5500.

[39] Binitie, A. P., Egbokhare, F., Egwali, A. O., & Innocent, O.S. (2021). Implementing existing authentication models in ussd channel. *2021International Conference on Electrical, Computer and Energy Technologies (ICECET) 9-10 Dec, 2021, Cape Town- South Africa, 1-5*

[40] Karode A., Mistry A. and Chavan S. (2013). Graphical Password Authentication System. International Journal of Engineering Research & Technology (IJERT) 2 (9), ISSN: 2278-0181

[41] Yeung, A.L.C., Wai, B.L.W., Mughal, F., & Iranmanesh, V. (2015). Graphical password: shoulder surfing resistant using falsification. *9th Malaysian Engineering Conference*, 145-148.

[42] Gokhale A. and Waghmare V. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *7th International Conference on Communication, Computing and Virtualization.* Procedia Computer Science 79, 490 – 498.

[43] HayashE.i, Christin N., Dhamija R., and PerrigA."Use Your Illusion:Secure authentication usable anywhere". *In 4th ACM Symposium on Usable Privacy and Security (SOUPS), Pittsburgh*, July 2008.

[44] Suo, X., Y. Zhu, and G. S. Owen. 2006. Analysis and Design of Graphical Password Techniques. *Proceedings of the 2nd International Symposium, Advanced in Vis. Comp., Nov. 6–8, Springer, Berlin Heidelberg*. 4292: 741–749.