Proceedings of the Eighth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2014)

Alternative Graphical Authentication for Online Banking Environments

H. Alsaiari[1], M. Papadaki[1], P.S. Dowland[1] and S.M. Furnell[1,2]

[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2]Security Research Institute, Edith Cowan University, Perth, Western Australia
e-mail: info@cscan.org

Abstract

Many financial institutes tend to implement a secure authentication mechanism through the utilization of the One-Time-Password (OTP) technique. The use of a hardware security token to generate the required OTP has been widespread. Despite the fact that this method provides a fairly high level of security, many systems have not taken into consideration the need for a secure alternative login method whenever the hardware token is unavailable. This paper discusses the authentication issues associated with current e-banking login implementations when the hardware security token is unavailable. The study was supported by a user survey to realize the constraints confronting the user while logging in to their online banking system. The result showed that many online banking users had multiple accounts and found carrying around several security tokens is inconvenient. Moreover, high proportion of the users had confidently accepted the concept of one-time graphical password as an alternative means of authentication. Therefore, a potential solution has been introduced along with a conceptual discussion. The proposal aims to consolidate several authentication mechanisms to unite their various advantages into one robust authentication system with consideration of usability. The composite mechanism comprises of a One-Time-Password combined with graphic-based authentication techniques.

Keywords

Alternative authentication, User authentication security, Online banking authentication, Graphical password, One-Time-Password

1. Introduction

Online banking, also known as Internet banking, is a means of delivering banking services electronically to customers. Online banking services include accessing account information, the transfer of funds between different accounts and making electronic payments and settlements (Dube & Gulati, 2005; FFIEC, 2003). The popularity of online banking is growing, but it is now faced with major challenges, one of which is the high risk of data compromise. Thus, in order to minimize the threats to online banking and at the same time increase customer security, confidence and acceptance of this electronic service channel, the online accounts of customers must be securely protected via enhancing user authentication without adversely impacting upon the users' experience (Williamson & Money–America's, 2006).

As reported by Verizon (2013), 37% of breaches in 2013 affected financial organizations, which increased by about 10% compared with the previous year's report. Crime against the finance industry involved various type of common attacks such as tampering (physical), brute force (hacking), and spyware (malware). The target of such breaches was mostly payment cards, credentials, and bank account info. Basically, gaining unauthorized access in an easy and less-detectable way is possible through leveraging other's authorization access. Moreover, an earlier report (2012) showed that about four of every five breaches involving hacking was factored by authentication-based attacks (guessing, cracking, or reusing valid credentials). Authentication credentials theft presented a high value of loss as a result of espionage-related breaches. About 80% of these attacks can be forced to adapt or die whenever the idea of a suitable authentication replacement is collectively accepted.

The critical importance of securing the wide range of banking services being deployed over the Internet is a major concern for both service providers and customers. Thus, extreme caution is always paid to safeguarding the e-banking system as well as customer information. The first line of defence is protecting the authentication system from fraud and identity theft. Currently, the traditional text-based password is the foremost knowledge-based authentication and the primary form of user authentication (De Angeli et al., 2005; Fu et al., 2001) and while there are many techniques to secure passwords (Pinkas & Sander, 2002), most are insufficient in the face of attackers' tools (Chakrabarti & Singbal, 2007; AuthenticationWorld.com, 2012). The deficiencies of the textual password is well-known and affects both aspects of usability and security (Dhamija & Perrig, 2000; Suo, Zhu & Owen, 2005). Therefore, the need for alternative methods has emerged where various alternative knowledge-based techniques have been proposed, such as graphic-based passwords (recognising graphical elements – e.g. images, iconography, grids) (Gyorffy, Tappenden & Miller, 2011; Kuber & Yu, 2010) or associative/cognitive questions (Zhao, Dong & Wang, 2006; Alexander, 2008). Each approach has different aspects of strengths and weaknesses.

In crucial systems such as in financial organizations, robust security is constantly demanded. One of the solutions to meet that goal is the One-Time-Password approach. The idea of OTPs is to encode the password for a single use only; producing a unique password for each login session or transaction. In other words, the user will end up using different dynamic password for each login. Illegitimately obtaining an OTP should be useless and helpless for attackers to generate any further encoded passwords. Thus, managing to record or steal a used OTP would be totally unusable for further login attempts since an OTP loses its validity (expire and discard) after first use. This means that OTP systems are protected against replay attacks (Yampolskiy, 2007; McDonald, Atkinson & Metz, 1995).

This paper aims to point out limitations in some authentication cases within the online banking system and propose a potential solution to securely fill-in this gap using the same web browser without the need for any additional devices. The remainder of the paper proceeds with a brief review of some authentication features provided by leading financial institutes. Section 3 then discusses the authentication

problems in online banking. Section 4 presents the preliminary survey results that investigate the authentication issues in online banking and gauge perceptions towards alternative authentication methods. Section 5 gives a general introduction to our proposed prototype of OTGP and conclusions and future work are addressed in Section 6.

2. The provided authentication by leading banking institutes

We conducted a review of the authentication approaches offered by banking services providers. We assessed the practices of the top four banks as ranked by relbanks.com (relbanks.com, 2012) in the UK and Saudi Arabia on the basis that respondents from these countries would form the basis for later survey data collection. The purpose was to gain tangible results from a field review that investigate and compare different authentication experiences within the electronic banking domain.

The comparison data was collected by visiting each online banking service of these banks to explore the provided authentication features. The services were compared on the basis of the following factors:

- **Authentication options**: when more than one authentication method is available for the user to choose from (e.g. OTP hardware-token or subset digits of textual password). Combining more than one form of authentication mechanism is called **Two-factor authentication**.
- **Static password**: The conventional password approach.
- **Subset digits of password**: challenges the user by requesting to submit different digit locations of the full password (e.g. 2^{nd}, 4^{th}, 7^{th} digit of your password).
- **Memorable information**: a type of personal questions that can be easy and short to answer by legitimate user.
- **OTP (SMS)**: a One Time Password sent to mobile phones through carrier short messages.
- **OTP (Soft-Token)**: a type of One Time Password that is generated by software application usually installed on smart phones.
- **OTP (Hard-Token)**: a special hardware device that directly generates a One Time Password.
- **PIN-dependent token**: an additional feature to the hard-token device where a PIN is needed to generate One Time Password.
- **Card-dependent token**: Another additional feature to the hard-token device where a smart-card is required to generate One Time Password.
- **Authorization site image**: a feature that allows the selection of a picture that will indicate a correct access to the official online banking website at every login time (and not a phishing website).
- **Authorization personal image**: allows uploading a personal picture that will be shown at every login to ensure accessing the official online banking website.

- **Designation of safe computer**: a computer that typically being used to access online banking accounts can be designated to be recognised as a Trusted Computer, any access from any other PCs will be denied.

	Bank	Authentication features										
		Authentication options	**Two-factor authentication**	**Static password**	**Subset digits of password**	**Memorable information**	**OTP (SMS)**	**OTP (Soft-Token)**	**OTP (Hard-Token)**	**Token needs PIN**	**Token needs Card**	**Other**
UK Banks	HSBC	×	✓	×	×	✓	×	×	✓	✓	×	
	Barclays	✓	✓	×	✓	×	×	×	✓	✓	✓	
	Royal Bank of Scotland	×	×	×	✓	×	×	×	×	×	×	
	Lloyds	×	×	✓	✓	✓	×	×	×	×	×	
Saudi Arabian Banks	National Commercial Bank	✓	✓	✓	×	×	✓	✓	✓	×	×	-Authorization Site Image
	Al-Rajhi Bank	✓	✓	✓	×	×	✓	✓	✓	✓	×	
	Samba Financial	✓	✓	✓	×	×	✓	×	✓	×	×	-Authorization personal Image -Designation of safe computer
	Riyad Bank	✓	✓	✓	×	✓	✓	×	✓	×	×	

Table 1: Authentication technologies used by leading banking institutes

The comparative Table 1 reveals that various authentication techniques to secure access to the systems have been applied. The text-based password is still the most common method used, appearing in different forms, such as static password, subset digits or memorable information. Usually, text passwords are used in conjunction with other authentication methods such as One-Time-Password (OTP) which also forms a two-factor authentication. In addition, the majority of banking systems have fortified their systems by implementing two-factor authentication instead of relying on a single factor. A number of banking systems have offered a variety of One-Time-Password (OTP) implementation methods using hardware tokens, short messages (SMS) or software tokens with the support of some additional security features.

Furthermore, it can be inferred that some authentication features are applied in one country but not the other. For instance, while some UK online banking systems utilise subset digits of password and memorable information, Saudi Arabian banks mostly do not. Whereas, soft-token OTP is implemented in Saudi Arabia but not commonly used in the UK. Notably, this part of the study was focused solely on the login authentication service which means that it does not cover any further authentication like transaction-based authentication or adding a new payee.

3. Limitations of online banking authentication

Giving the option for the user to choose the appropriate authentication method is a fundamental usability feature that adds flexibility to the system. Despite the fact that this feature does exist in some current systems, it is realized that the available options depend mainly on phone banking services providing the required access or on giving the customer the choice of selecting between the use of a hardware token or SMS. That means that there is still potential for encountering some of the usability problems, such as that of being reliant on hardware devices like mobile phones or OTP tokens, which are vulnerable to theft and loss or in the case of mobile phones may suffer an interruption in the service coverage (Weir et al., 2010). In addition, other systems may offer the traditional passcode option or allow authentication via a series of Q&A challenges in case the user is unwilling/unable to use the recommended secure authentication options which potentially fall back into the weaknesses of the traditional textual password. However, none of the discussed authentication options other than the text-based password offer in-session authentication which uses the web browser to process any extra login task. That in turn emphasizes the dependence on an additional out-of-band means (e.g. token/mobile) to secure the authentication task.

More recently, many banks have adopted OTP authentication using hardware tokens that are supplied to each client as part of a multi-factor authentication scheme. Although this method is effective, it has a fundamental downside due to the reliance of the applied OTP authentication being mostly on a single OTP delivery method. Thus, many online banking systems are not equipped with a supplementary authentication method to back up the primary hardware-based OTP authentication. In other words, lost/stolen/forgotten/damaged hardware tokens will prevent clients from gaining access to the online banking system due to the absence of an operative alternative means of logging in under such critical circumstances. However, some online banking systems utilize an out-of-band method, such as mobile SMS messaging, as a parallel means of obtaining the OTP. Still, this service can encounter several problems, such as message delivery delay, weak signalling, roaming availability and charges (Weir et al., 2010; RBS, 2014). Therefore, the need for a secure, usable secondary authentication method to play an alternative role alongside the primary hardware-based OTP scheme has emerged in cases where the hardware token is unavailable.

Graphic-based authentication is among the promising alternative proposals, which occupies an important position within user authentication research area (Ray, 2012).

According to classic cognitive science experiments, humans have a vast, almost limitless memory especially for pictures (Dhamija & Perrig, 2000). Thus, authentication types that depends on graphics are likely to tackle the memorability problems that negatively affect text-based authentication since remembering complex passwords as well as multiple passwords for different systems are claimed to be a difficult task (Furnell, 2005; Furnell & Zekri, 2006), while at the same time, humans find it easier to recognise images even after a period of time (Anderson, 2001).

4. Research survey

A structured online questionnaire was designed and delivered to investigate the authentication issues associated with online banking in addition to gauging the participants' perceptions and attitudes towards alternative authentication methods for online banking. The main purpose of the survey was to find answers for some research-related questions such as whether users manage multiple online accounts, are using security tokens for that purpose, the user perception regarding carrying around several tokens, have they ever encountered login problems when using these tokens, and finally their acceptance of alternative authentication methods. The survey was comprised of a total of twenty nine questions encompassing demographic information, experiences of user authentication schemes and security-related techniques, usage of the banking system, experiences of authentication within the online banking system and lastly the users' opinions and acceptance level of the alternative authentication mechanisms.

4.1. Results interpretation and analysis

A total of 250 respondents participated in this online survey over a period of 3 weeks. All participants were volunteers, participants were recruited from students and staff in the authors' university, and colleagues/friends of the author who were invited via email and text messages. Two thirds of the respondents were males and the remaining third were females. The age group between 30 and 39 years comprised the majority of the sample and represented 43% of the total number of participants. The residential location shows that almost 90% of the respondents resided either in the UK (46%) or Saudi Arabia (44%). Regarding the educational background, the highest percentage of participants (44%) had studied at Higher education level, while 39% were Postgraduates. As for the employment status, the highest percentage of participants (67%) were employed followed by 24% being students. Regarding the level of computer experience, most participants (48%) considered themselves to be at advanced level followed closely by 47% at intermediate level with only a small percent (4%) having a basic level of computer skills.

The results revealed that 57% of the participants have used OTP as an alternative authentication method. Regarding the importance of multiple levels of authentication where various authentication approaches from the same category (usually knowledge-based) are combined, 90% of the participants were supportive of this kind of technique, agreeing that it was important.

An important question was asked aiming to measure the users' opinions on carrying around multiple security devices to fulfil the authentication requirements of multiple online accounts. Table 2 demonstrates that most respondents opposed the idea with 69% feeling that carrying multiple tokens is not convenient and 38% thinking it is unnecessary. However, 38% of the participants said it is acceptable on balance.

	Convenient		Necessary		Acceptable	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Agree	44	17.6	90	36.0	96	38.4
Neutral	34	13.6	64	25.6	71	28.4
Disagree	172	68.8	96	38.4	83	33.2

Table 2: Participants' opinion about carrying multiple tokens

The participants were also asked some banking-related questions. As per the survey results shown in Figure 1, the vast majority of respondents (93%) were online banking users. Amongst these, 65% were managing more than one online account with 56% having between 2 and 5 online accounts. Noticeably, 9% of the respondents had more than five online accounts, while approximately a quarter of the participants had only a single online account. Around two thirds of the online banking respondents stated that they access their online banking accounts on a regular basis, while nearly a quarter of the respondents accessed their accounts occasionally. The final part of this section investigated the purpose of using online banking services. The results shows that 40% of the participants were utilizing this service to conduct a variety of online payment services, such as paying bills or transferring funds, while 36% of them used the service for checking bank account information/transactions.

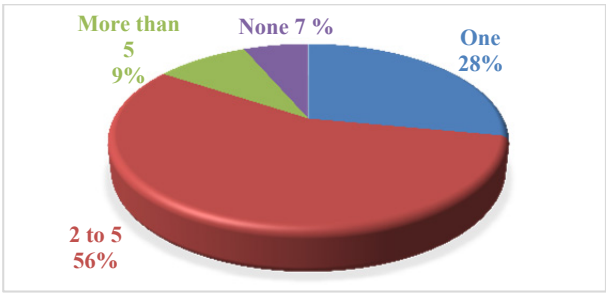

Figure 1: Number of online banking accounts

With regards to the online banking experience, more than 85% of the participants' online banking systems require multi-factor authentication. Remarkably, OTP authentication was offered by the banks of 90% of the participants, as shown in Table 3. Furthermore, since most of the participants were from the UK and Saudi Arabia, a further analysis was carried out to assess the popularity of certain types of OTP techniques in these countries. The findings indicated that the most used

technique in the UK was the security token device whereas SMS text messages were the most common in Saudi Arabia. It should be noted here that the responses to some questions were open to multiple choices which explain why the responses count in Table 3 exceeded the number of participants.

Type of OTP	Count	Responses %
None - the online banking system does not facilitate a One-Time-Password	32	10.4%
SMS text message	136	44.2%
Security token device (Hardware)	114	37.0%
Soft token (Software)	26	8.4%

Table 3: The offered types of One-Time-Password

Table 4 illustrates that 76% of the responses indicated that they were satisfied with the use of One-Time-Password authentication, while in contrast a very small portion were dissatisfied with this type of technique.

OTP experience	Frequency	Percent
Satisfied	160	76.2
Neutral	38	18.1
Dissatisfied	12	5.7

Table 4: Participants experience with OTP technique

As part of multi-factor and OTP authentication, the participants were asked if they had failed to login using these methods before. The result shows that 64% had experienced failure in fulfilling the login requirements for several reasons (Figure 2), such as mistyping the code which comes first with (48%), the lack of mobile services (21%) and lost token/mobile (9%). However, 43% of these incidents occurred only rarely, while less than 3% happened frequently.

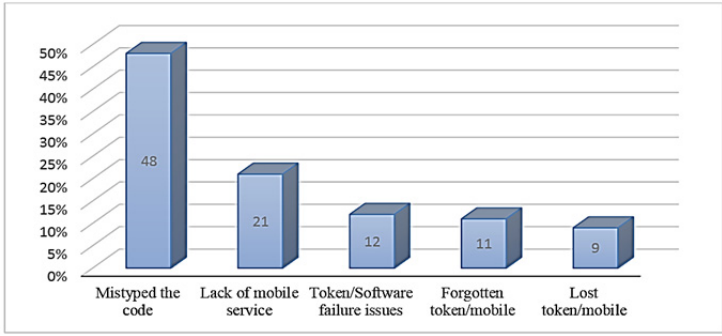

Figure 2: Reasons of experienced login failure

Table 5 shows that 73% of the participants who had login problems were still expressing themselves to be 'satisfied' overall when using one-time-password. However, only less than 5% of the participants with multiple online accounts had dissatisfaction experience using one-time-password and approximately 18% of the responses were 'neutral' as presented in Table 6.

		Frequency of login failure using multi-factor or One-Time-Password authentication			
		Rarely	Sometimes	Frequently	Percentage%
Experience of using One-Time-Password	Satisfied	103	22	4	73
	Neutral	31	10	2	22
	Dissatisfied	7	4	0	5
Percentage %		70.2	25.5	4.3	

Table 5: Satisfaction of the participants who experienced login failure

		Multiple online banking accounts %
Experience of using One-Time-Password	Satisfied	77.7
	Neutral	17.6
	Dissatisfied	4.7

Table 6: Satisfaction of the participants with multiple accounts

The last section presented a conceptual model (Figure 3) about the prospective solution with a concern about participants' opinions towards alternative authentication mechanisms. In terms of accepting the idea of replacing or supplementing the existing one-time-password method with a one-time graphical password technique, responses showed that almost half of the participants (49%) accepted the idea, while in contrast, less than a quarter (23%) rejected it. Another question in this regard was about the participants' confidence in the alternative graphical authentication method for online banking. 49% of the participants responded with "confident" and 26% with "un-confident".

Figure 3: One-time graphical password conceptual model

4.2. Discussion of research survey

The collected data showed diversity in the participants' experiences and knowledge of authentication and online banking. It appears that plenty of the participants had a reasonable understanding of authentication enhancement in the online banking environment; nevertheless, a small percentage of participants had little knowledge of online banking authentication. The positive record of participants' computer experiences indicates the development of users' computing skills and their competency to perform more complex computer tasks.

As per the survey results, it was found that a high percentage of respondents hold and manage several online banking accounts. This demonstrates a trend towards the utilization of the online channel to simplify performing banking transactions as well as other account management tasks. Moreover, the results also emphasize the difficulty of using multiple security tokens to manage these accounts; many participants disagreed with the idea of carrying around multiple devices for login purposes, describing it as inconvenient and unnecessary. Additionally, the survey showed that a high proportion of the total sample number access their accounts on a daily or weekly basis, which obviously proves the increasing popularity of and demand for online banking services.

One of the interesting results of the survey was the high percentage of responses indicating that the online systems of the participants' banks require multi-factor authentication. Furthermore, many of those systems make use of the OTP authentication method. More than half of the participants had already been using One-Time-Password as an alternative method of authentication. That in turn reveals the importance and feasibility of both techniques for the online banking environment. Interestingly, the result shows that the majority of respondents have had satisfactory experiences using OTP techniques. In spite of this positive statistic, the survey recorded a relatively high ratio of failing to satisfy the login requirements for multi-

factor or OTP authentication but these failures were not frequent. By excluding half of the incidents (experienced failures) caused by mistyping the code, which is a common human mistake, it can be inferred that a lack of mobile services is the cause of many login failures. However, a number of participants have different views on this, believing that the main reason for login failure is forgetting or losing a token/mobile.

Although user satisfaction with the existing OTP methods is reasonable, that does not negate the need to consolidate the overall authentication mechanism for such a crucial system. In other words, the current system is to some extent able to fulfil the needs of a large number of customers and match the functional expectations of many customers and providers of online banking services; however, at times customers find themselves unable to access their accounts because of the inability to fulfil the login requirements of the primary authentication method and at the same time the lack of alternative authentication methods. As a result of this, the demand for further investigation and consideration of this issue has emerged. The authentication system should cover most possible login scenarios to ensure high availability and less restriction.

The aim of the final section of the survey was to determine participants' views towards alternative authentication mechanisms. Specific questions were asked about graphics utilisation for authentication purposes, which were positively answered with acceptance to such technique's implementation. In addition, the participants were asked about how acceptable it would be to replace or supplement the existing one-time-password system with one-time graphical password system. The result presented that a large number (nearly half) of participants were open to the idea of using such graphical authentication in the context of online banking system with confidence.

5. Overview of the proposed solution

The conducted review of the current state of graphical techniques along with the outcome of the survey study has pointed to the need for an enhanced authentication method to fulfil the security and usability requirements. This research aims to contribute in overcoming the major issues in the existing graphical schemes to obtain an enhanced scheme that can be utilised for filling-in the authentication shortage in the online banking systems. Therefore, a hybrid secure solution is proposed – a One-Time-Graphical-Password "OTGP" which intends to leverage a multi-level authentication to ensure a robust and secure authentication. For which purpose, a combination of multiple authentication mechanisms will be employed which are a One-Time-Password along with a Graphical password. In addition, various graphical password methods have been merged to form a new mixture of Recall and Recognition-based techniques. The final component of this integrated authentication system will involve a determination task of OTP input formats. More precisely, the method will be established by solving the lock-pattern (Draw-based), followed by identifying password images (Image-recognition) and last step will be entering the corresponding OTP code according to the pre-chosen format (Knowledge-based).

Table 7 illustrates a breakdown of the hybrid scheme characteristics. For better clarification, this study suggests the addition of some distinguishing details in a manner that involves several design aspects. Firstly, the input approach, for instance, is what the user needs to submit as the login information for the authentication session. This input approach includes the following: Draw, Click, Choice or Typing. The second aspect is the display style, which means the presentation mode that forms the password challenge, such as: Grid, Image, Icon.

		Category	Approach	Style
1	**Pattern unlock**	Recall	Draw	Grid
2	**Image recognition**	Recognition	Choice	Multi-images
3	**OTP formation**	Recall	Typing Entry	Keyboard

Table 7: Categorisation and characteristic breakdown

The main expected technical advantages of the proposed scheme are summarised as follows:

- Combination of multiple authentication mechanisms (Graphical password and One-Time-Password).
- Combination of multiple graphical password categories (Recall-based [Draw] and Recognition-based [Choice]).
- System assigned themes with user chosen images.
- Various OTP formats.

The proposed scheme involves two phases; enrolment and authentication. The steps of the process flow for these phases are shown in more detail in Table 8.

General Process Flow	Enrolment Phase	Authentication Phase
Secret Knowledge (Username)	Select a unique username	Enter correct username
Pattern Unlock Graphical Password (Recall-based, Draw-based)	A 4x4 Pattern grid will be displayed. The user needs to draw a pattern as minimum of 4 points (strokes)	Unlock pattern grid by redrawing the pre-chosen pattern
Image Recognition Graphical Password (Recognition-based, Choice-based)	The system will assign 4 random themes for the user. A panel of images from each of the assigned themes will be presented for the user to make his/her own selection	The system displays a 4x4 panel of images containing (2 random pass-images out of the 4 previously chosen pass-images + 14 other decoy images). The user needs to identify the two pass-images
One-Time-Password Formation of the final password entry	Since the edge side of each row and column of the panel will be assigned 4 random digits, user can choose from a number of different OTP format combinations such as: (1st pass-image = Top axis code + 2nd pass-image = Left axis code)	Enter the associated OTP with each image in the same OTP format chosen previously
Confirmation / Authentication	Confirming the entire password process (Pattern redrawing, choosing pass-images, OTP format selection	Access is granted when all provided information is correct

Table 8: Process flow for the enrolment and authentication phases

6. Conclusion and Future Work

An overview of various authentication features provided by some of the leading banks has been presented and discussed. It was found that the adoption of multi-factor authentication using hardware token OTPs has increased. However, the study has shown that there are some failures in fulfilling the login requirement using the OTP method, even though the user experience with such a technique has been found to be satisfactory. Furthermore, carrying around multiple security tokens to manage several online accounts has been described as inconvenient and unnecessary. In this paper, the issue of the absence of an alternative authentication method when the main hardware OTP token is not present has been discussed. To overcome this issue, a general conceptual structure of the proposed solution has been introduced involving several authentication mechanisms such as graphic-based and One-Time-Password that aim to meet the main objective of having a usable secure authentication mechanism that is available anytime and anywhere without the need for additional devices. The initial features and advantages of the OTGP scheme were briefly presented. The next phase will look at system implementation with initial user trials

and lab experiments. Statistical data such as time, security level, and password memorability over time intervals will be some of the outputs of the experiment. Upon the assumption of positive results from the initial trials, the final phase of the OTGP project will then expand the study through a field experiment to obtain a wider range of participants for more accurate results.

7. References

Alexander, C. (2008) 'Two Factor Authentication That Doesn't Use Chips'. *Card Technology Today*, 20 (5). pp 9.

Anderson, R. J. (2001) 'Access Control'. *Security Engineering: A guide to building dependable distributed systems.* 1st edn.: Wiley, pp 51-71.

AuthenticationWorld.com (2012) *Password Authentication*. Available at: http://authenticationworld.com/Password-Authentication/index.html (Accessed: 02/04/2014).

Chakrabarti, S. & Singbal, M. (2007) 'Password-Based Authentication: Preventing Dictionary Attacks'. *Computer*, 40 (6). pp 68-74.

De Angeli, A., Coventry, L., Johnson, G. & Renaud, K. (2005) 'Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems'. *International Journal of Human-Computer Studies*, 63 (1–2). pp 128-152.

Dhamija, R. & Perrig, A. (2000) 'Déjà vu: A User Study Using Images for Authentication', *the 9th USENIX Security Symposium*. pp. 45-58.

Dube, D. & Gulati, V. P. (2005) 'Information System Audit and Assurance'. (Appendix B). pp 594.

FFIEC (2003) 'FFIEC E-Banking Booklet'. [Online]. Federal Financial Institutions Examination Council. Available at: http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/GroupDocuments/e_banking.pdf (Accessed: 02/04/2014).

Fu, K., Sit, E., Smith, K. & Feamster, N. (2001) 'Dos and Don'ts of Client Authentication on The Web', *Proceedings of the 10th conference on USENIX Security Symposium*. Washington, D.C. USENIX Association, pp. 19-19.

Furnell, S. (2005) 'Authenticating Ourselves: Will We Ever Escape the Password?'. *Network Security*, 2005 (3). pp 8-13.

Furnell, S. & Zekri, L. (2006) 'Replacing Passwords: In Search of the Secret Remedy'. *Network Security*, 2006 (1). pp 4-8.

Gyorffy, J. C., Tappenden, A. F. & Miller, J. (2011) 'Token-based Graphical Password Authentication'. *International Journal of Information Security*, pp 1-16.

Kuber, R. & Yu, W. (2010) 'Feasibility Study of Tactile-based Authentication'. *International Journal of Human-Computer Studies*, 68 (3). pp 158-181.

McDonald, D. L., Atkinson, R. J. & Metz, C. (1995) 'One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication', *the Proceedings of the 5th USENIX Security Symposium*. Salt Lake City, Utah.

Pinkas, B. & Sander, T. (2002) 'Securing Passwords Against Dictionary Attacks', *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, pp. 161-170.

Ray, P. P. (2012) 'Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices'. *Journal of Information Engineering and Applications*, 2 (2). pp 1-11.

relbanks.com (2012) *Banks Around the World*. Available at: http://www.relbanks.com (Accessed: 02/4/2014).

RBS (2014) Will I be charged for any mobile phone text alert messages I may get? - Ask a Question. The Royal Bank of Scotland ©. Available at: http://supportcentre-rbs.custhelp.com/app/answers/detail/a_id/745/kw/network%20operator (Accessed: 12/4/2014).

Suo, X., Zhu, Y. & Owen, G. S. (2005) 'Graphical Passwords: A Survey', *Computer Security Applications Conference, 21st Annual*. 5-9 Dec. 2005. pp. 10 pp.-472.

Verizon (2013) *2013 Data Breach Investigations Report.* Verizon Enterprise Security Solutions. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (Accessed: 02/04/2014).

Weir, C. S., Douglas, G., Richardson, T. & Jack, M. (2010) 'Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience'. *Interacting with Computers*, 22 (3). pp 153-164.

Williamson, G. D. & Money–America's, G. (2006) 'Enhanced Authentication in online Banking'. *Journal of Economic Crime Management*, 4 (2).

Yampolskiy, R. V. (2007) 'User Authentication via Behavior Based Passwords', *Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island*. 4-4 May 2007. pp. 1-8.

Zhao, Z., Dong, Z. & Wang, Y. (2006) 'Security Analysis of a Password-based Authentication Protocol Proposed to IEEE 1363'. *Theoretical Computer Science*, 352 (1–3). pp 280-287.