A comparative analysis and review of OTP Grid Authentication Scheme: Development of new scheme

Benedicto B. Balilo Jr.*, Bobby D. Gerardo, Ruji P. Medina***
*Technological Institute of the Philippines, Quezon City, Philippines
**West Visayas State University, Iloilo City, Philippines

Abstract - Grid authentication factor is about XY coordinate lookup system. The random cell in the grid carries the correct combination of numbers and letters in the cell. An example of grid authentication scheme is the bingo card. Bingo card is a less secure alternatives because of the scheme it used (the three digits) which is fewer than most random OTP schemes making it exposed to threats. However, grid authentication is one of the interesting authentication scheme that can be explored to maximize the random generation of codes with mathematical computation and algorithmic scheme. This study aims to compare the different grid authentication scheme to determine which of these schemes provides better performance, complexity, saves memory resources and gives quality key generation.

Index Terms: grid authentication, one time password

I. INTRODUCTION

One-Time Password (OTP) is a modern authentication scheme which offers accuracy, security and confidentiality. OTP Two-Factor Authentication is considered as one of the promising methods in any web-enabled information system. Currently, there are many schemes have been developed to safeguard and protect confidential information. However, they differ from functional properties, methods and materials used. Each of which has unique approach in handling risks and attacks [1].

Grid authentication factor is about XY coordinate lookup system. The random cell in the grid carries the correct combination of numbers and letters in the cell. An example of grid authentication scheme is the bingo card. It is a less secure alternatives because of the three digits used fewer than most random OTP schemes and can be photocopied making it exposed to threats [2]. However, grid authentication is one of the interesting authentication scheme that can be explored to maximize the random generation of codes with mathematical computation and algorithmic scheme.

The increasing popularity and application of OTP served as the greatest motivation of this research study. Though there is no best approach to secure authentication, this study will analyze and compare the different approaches OTP for grid authentication to determine which of these schemes provides better performance, saves memory resources and gives quality key generation. Accordingly, the results generated by OTP is unique considering its complexity and randomicity.

II. RELATED WORKS

The one time password (OTP) is a security layer that increases the security level for authorization and authentication. The user presents something or in possession like mobile phone, PIN or uses fingerprint to establish connection or access to the computer system. OTP is just one of many authentication schemes use to authenticate valid user.

Authentication can be performed in many ways. The importance of selecting an appropriate authentication method is considered as the crucial decision in designing secure systems. It may be viewed as simply presenting credentials and authenticating the connecting party but failure to authenticate can compromise the network and the resources are vulnerable to misuse [3].

To identify the user, a computer system or application will require authentication. Authentication is the process of establishing or making access to computer network, making purchases online, transferring accounts through bank website or perhaps visiting social media sites involve a method called authentication; [4][5]defined, authentication as the process of verifying the identity of a user, tracing the origins of an event, or ensuring that the information comes from a trusted site. It is the act of confirming the truth or genuineness of an attribute or entity. It establishes the authenticity or proves genuineness. Authentication is classified into three factors: owner factor typically takes the form of a one-time token key from an external source, knowledge factors takes no additional hardware needed to provide the secret codes. Password, pass phrase, identification PIN and challenge response are examples of something you know factor, and inheritance factors; these tends to be the strongest and hardest to crack because this factor uses fingerprint, retinal pattern, signature, face, and voice. But, the deployment of this type of technology is expensive and does not translate easily to all the ways we all access resources [6].

User authentication is one of the fundamental procedures to ensure secure communications and share system resources over an insecure public network channel. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources [7]. Social engineering, phishing, brute force attacks, shoulder surfing, keystroke logging, eavesdropping, and dictionary attacks are among the many threats to authentication.

The traditional username and password has shortcomings giving for the OTP to be introduced to increase the level of security. OTP are passwords which are valid only once for an authentication. Its main advantage is that the user is free from impersonation and the password will not be reused. The core of

Lamport’s scheme requires that client cooperates and agrees to use a common sequencing algorithm to generate a set of expiring OTP, and validate client-provided passkeys included in each client-initiated request [8].

Nowadays, the use of One-Time Password is a common authentication scheme to many companies, organizations and institutions.

The implementation of two-factor authentication method reduced the cost associated with multiple passwords, enhancing the user experience while increasing productivity, increasing security around a single point of access, and simplifying auditing and compliance. While, others have benefited from customer confidence, regulations and best practices, threat prevention and fraud prevention [9].

Nonetheless, these authentication techniques contain weaknesses and gap. While there is no appropriate or best design for specific problems, every application has its own specific strength and vulnerabilities, but the development of a two-factor authentication is already a landmark and as added feature is a serious improvement in protecting information.

There are many studies conducted relative to the application of the different methods with the inclusion of OTP as added features to authentication. The SMS, Transparent Token, email or printer token achieved a two-factor authentication. SMS and Email are both in active attack but SMS has higher in terms of passive attack. But, in terms of ease of use and portability they are both high. The major advantage of email is in terms of cost, user can use the available email account without cost to the organization.

There are different techniques or schemes involved in the generation of OTP. These includes random number generation, timestamp, keyboard manipulation, location, IP address or a combination of the different parameters (like biometric characteristics + pseudorandom numbers).

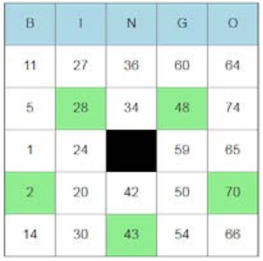
III. ANALYSIS OF DIFFERENT GRID AUTHENTICATION SCHEME

The start of letter labeled columns (bingo card) have generated interest to card bingo players community. The game started in 1500 Italy in a lottery game called lo Giucco del Lotto d'Italia. The game was modified into 2 versions – a 12-card and a 24-card set [10]. Several varieties of cards have been developed, tested and played. The U.S. style (5x5 grid for 75-ball Bingo) and U.K. style “Housie”--90-ball are the known modern bingo card game [11].

Bingo cards are interesting and attractive because it is easy to implement and they do not require a chip or internal mechanism compared to smart cards and token. It offers flexibility, ease of use, they are cheap, easy to produce and easy to replace. However, this have drawbacks like dependent on number of cells, combinations become stale and just like with old and weak password eventually can be cracked [2].

5x5 Bingo card scheme

The 5x5 bingo card (also known as American bingo card) is the most popular and commonly played numbers format. The card contains 25 squares, arranged in 5 vertical and 5 horizontal rows. Figure 1 shows the sample 5x5 bingo card scheme. The numbers are randomly generated from specified column range.



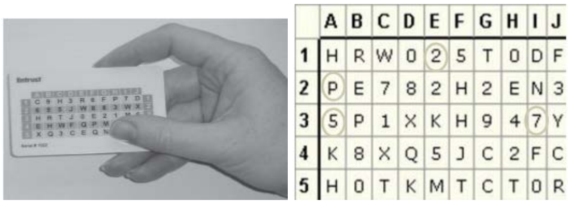
B	I	N	G	O
11	27	36	60	64
5	28	34	48	74
1	24		59	65
2	20	42	50	70
14	30	43	54	66

FIGURE 1. SAMPLE 5X5 BINGO CARD SCHEME

The middle square of the card is a “free space”. The columns of the card are labeled with the letters “B.I.N.G.O”. The rows are labeled with numbers between 1 and 75, allowing to generate 5.53x10^26 possible number arrangements. The column B includes numbers between 1 to 15, column I has numbers 16 to 30, column N has numbers 31 to 46, column G has numbers 46 to 60 and column O has numbers 61-75 [10]. The generated codes is purely a combination of numbers from 1 to 75 with specific column range. This makes the scheme simple and easy to predict numbers which an attacker can simply apply brute force attack to predict the next round of numbers.

Entrust Grid card scheme

The Entrust-patented grid card is a credit card-sized authenticator consisting of numbers and characters in a row-column format. A user is presented with authentication challenge when they log in to a restricted network, application, cloud service or site. The challenge presents the user with coordinates such as A2, A3 and E1. The user refers to their unique grid card to provide the information from the requested cells: P52 (Figure 2).



	A	B	C	D	E	F	G	H	I	J
1	H	R	W	0	2	5	T	0	D	F
2	P	E	7	8	2	H	2	E	N	3
3	S	P	1	X	K	H	9	4	7	Y
4	K	8	X	Q	5	J	C	2	F	C
5	H	0	T	K	M	T	C	T	0	R

FIGURE 2. SAMPLE ENTRUST IDENTITYGUARD GRID AUTHENTICATION SCHEME (A) SAMPLE PRINTED ENTRUST CARD AND (B) SAMPLE ENTRUST GENERATED GRID CARD

Each grid card is unique and carries a serial number, so every user can be uniquely identified and authenticated. Each time a user is asked to authenticate they are presented with a different challenge requiring them to validate via a different set of grid coordinates. The coordinate request changes for each authentication challenge. An enhanced version of the grid card was released with enhancement on the generation of 2-pair values (like H3, I5, A6). The grid consists of approximately 50 values (5*10) with combination of uppercase characters and numbers. A total of 36 (26 uppercase letters + 10 numbers (0-9)) values formed the entropy of the seed [13]. These gives the scheme the limit in generating the entropy aside from fixed-size length of grid card.

Other form of grid scheme
The grid that has 16 squares marked A to P and numbers corresponding to the letters used in ICICI card [12].

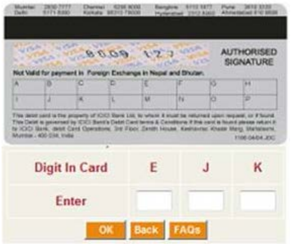


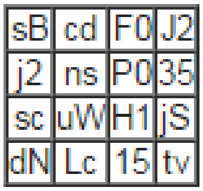
FIGURE 3. SAMPLE ICICI FORM (PRINTED AT THE BACK OF CREDIT SIZE CARD)

The user simply look into the card and with the corresponding letters fill-in the blank space. Similar with mentioned scheme, this is simple and easy to brute force because of the limited numbers/characters involved in the process.

IV. RESULTS AND DISCUSSIONS

A. *Development of new grid scheme*

The usual bingo card scheme consists of single number in a square. An improvement in the values was used in 2-pair value grid scheme with assigned row-column mapping sequence (Figure 4).



sB	cd	F0	J2
j2	ns	P0	35
sc	uW	H1	jS
dN	Lc	15	tv

FIGURE 4. PROPOSED GRID AUTHENTICATION SCHEME

The 2-pair value grid scheme is an algorithmic process where it used the concept of random number generation, attribute-based and string manipulation technique. The Lamport formula was adopted in generating the 2-pair codes. That is, additional parameters was added to the initial seed such as string of characters, numbers, date and timestamp. Using the formula given, the initial seed captures the current OTP and integrated as part of the next OTP to be generated. The letter g as the initial seed and letter b represents the OTP to be generated.

$$b=g,\ b1=(b(g+otp^{1}),\ b2=(b1(g+otp^{2})).. \ bn+1=(bn+1(g+otp^{n}))$$

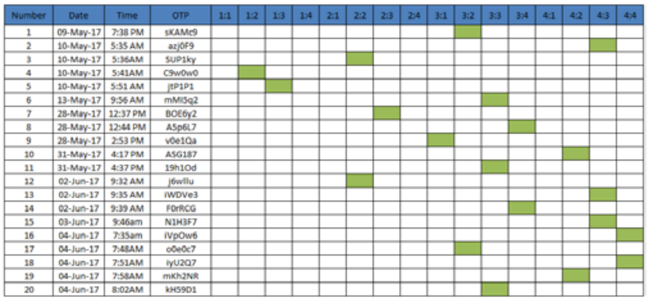
This method was considered to be free from brute force and dictionary attack as the applied algorithmic pattern used the combination of randomized code to generate the initial seed of the OTP. The XY values will be randomly chosen together with the assigned pair of codes. These will be mapped out into the 4x4 matrix schedule. The user is require to complete the challenge process given by the XY pattern like sc and cd that intersect the code uW. These patterns of code will be grouped to form the initial seed (i.e. sccduW), and the center four (4) characters will be the final OTP codes.
In this approach, a new algorithmic OTP is applied to increase the level of security for users. It makes use of table sequence schedule send to user with successful advantage over the printed OTP mechanism like BINGO scheme.

B. *Runtime performance*

The algorithm fixed-length table schedule selected the number ranging from 1 to 4 in two separate randomization process. From the table schedule, each cell element has its own corresponding XY-axis coordinates.
Figure 5 shows the summary of randomly selected XY-axis values generated by the algorithm. The date, time, OTP codes, XY-axis and origin (value where XY-axis intersect---in order to complete the OTP codes) was provided as parameters in dealing with the simulation process.

TABLE 1. SUMMARY COMPARISON BETWEEN BINGO-LIKE SCHEME AND PROPOSED OTP (IN MSEC)

#	BINGO card scheme 1	BINGO card scheme 2	Proposed algo	BINGO card scheme 1	BINGO card scheme 2	Proposed algo
1	825314765	D1-h;F1-W;C4-o	A8ai23	0.262	0.824	0.252
2	524414871	E3-w;F2-f;C5-c	S4gv59	0.239	0.829	0.088
3	518444774	D5-4;D3-T;E2-d	qOpiBJ	0.340	1.490	0.729
4	423364662	E3-k;B4-5;E3-k	s1EUJ4	0.740	1.328	0.521
5	1327315669	A2-Y;E1-J;B2-b	Wun9vC	0.382	0.808	0.139
6	629454768	A3-t;B5-o;C5-W	wIfMe7	0.501	0.698	0.861
7	1027355470	F4-o;C4-O;E5-D	57X3V5	0.704	0.926	0.093
8	1030414964	A4-e;B4-d;B5-m	H8yGoI	0.271	0.618	0.489
9	216434763	E5-y;C1-m;F1-M	E7rJ23	0.644	0.961	0.231
10	816345873	C4-C;E5-l;A2-d	EIsBF0	0.677	0.629	0.545
			Average	**0.476**	**0.911**	**0.394**



Number	Date	Time	OTP	1:1	1:2	1:3	1:4	2:1	2:2	2:3	2:4	3:1	3:2	3:3	3:4	4:1	4:2	4:3	4:4
1	09-May-17	7:38 PM	sKAMe9										🟩						
2	10-May-17	5:35 AM	azj0F9															🟩	
3	10-May-17	5:36AM	SUP1ky						🟩										
4	10-May-17	5:41AM	C9w0w0		🟩														
5	10-May-17	5:51 AM	jtP1P1			🟩													
6	13-May-17	9:56 AM	mMI5q2											🟩					
7	28-May-17	12:37 PM	BOE6y2							🟩									
8	28-May-17	12:44 PM	A5p6L7												🟩				
9	28-May-17	2:53 PM	v0e1Qa									🟩							
10	31-May-17	4:17 PM	A5G187														🟩		
11	31-May-17	4:37 PM	19h1Od											🟩					
12	02-Jun-17	9:32 AM	j6wllu						🟩										
13	02-Jun-17	9:35 AM	iWDVe3															🟩	
14	02-Jun-17	9:39 AM	F0rRCG												🟩				
15	03-Jun-17	9:46am	N1H3F7															🟩	
16	04-Jun-17	7:35am	iVpOw6																🟩
17	04-Jun-17	7:48AM	o0e0c7										🟩						
18	04-Jun-17	7:51AM	iyU2Q7																🟩
19	04-Jun-17	7:58AM	mKh2NR														🟩		
20	04-Jun-17	8:02AM	kH59D1											🟩					

FIGURE 5. SUMMARY OF RANDOM XY-AXIS VALUES GENERATED BY THE ALGORITHM

The result shows that the XY-axis coordinate 1:1 was never selected throughout the entire simulation of the algorithm. This was the consideration in the inception phase of the study as this will produce a redundant two-pair value which may be a possible hint for guess attack and an easy to obtain brute force attack. With the in-placed statements in the, XY-axis 1:1 will be bypassed from the selection. The deployment of this segment allows the generation of OTP values to be reliable, free from some form of attacks (like guess attack, dictionary and brute force attack) which is one of the primary goals of this study.
Table 1 shows the summary comparison of runtime performance between BINGO-like scheme and proposed OTP scheme. Same language was applied in the development of the scheme. The system was executed ten (10) times to record the time and computed the average.
As a result, the proposed OTP scheme recorded the fastest to generate the codes (0.394 msec) while 0.476 msec and 0.911 msec recorded for the BINGO-like scheme. The proposed OTP scheme produced a combination of numbers and characters (lowercase and uppercase letters) while the BINGO-like scheme generated numbers or single character only. With 0.517 msec difference, the proposed OTP scheme managed to generate somewhat complex OTP values compared with BINGO-like scheme.

V. CONCLUSIONS AND RECOMMENDATIONS

The new algorithmic OTP scheme provided a new level of security for users, it allows the pair of codes to be randomly generated and mapped out in matrix. It made use of XY schedule send to user with successful advantage over the other Bingo-like card scheme.

The results were conclusive that the proposed OTP authentication scheme proved to generate a randomize XY-axis taking advantage for OTP values to be complex. The effect of restriction in 1:1 value allowed the system to be free from brute force attack and dictionary attack.

The performance of the algorithm is conclusive that the proposed algorithm proved to be faster and posed advantage over traditional authentication and OTP printed scheme as this incurred cost in printing the OTP codes and limited key generation parameters.

VI. REFERENCES

[1] Fan, Y.T. & Su, G.P. (2009). Design of two-way one-time-password authentication scheme based on true random numbers, in *2nd International Workshop on Computer Science and Engineering, WCSE 2009*, *1*, 11–14.

[2] Corum, C. (2006, 25 September). Grid-based two-factor authentication comes to campus cards. https://www.secureidnews.com/news-item/grid-based-two-factor-authentication-comes-to-campus-cards/

[3] Duncan, R. (2002, October 23). An Overview of Different Authentication Methods and Protocols. Retrieved from https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118

[4] Hameed, S. (n.d.). Two-Factor Authentication [Powerpoint Slides]. Retrieve from www.slideshare.net dated December 12, 2016.

[5] Mishra, D. & Ali, H. (n.d.). Authentication [Powerpoint Slides]. Retireved from www.slideshare.net dated December 12, 2016.

[6] FRSecure (2011, Sept. 2). *What Authentication Means in Information Security*. Retrieved from http://www.frsecure.com/what-authentication-means-in-information-security/

[7] Liao, K.C., Lee, W.H., Sung, M.H., & Lin, T.C. (2009). A one-time password scheme with QR-code based on mobile phone, in *NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC*, 2069–2071.

[8] Lacona, L. J. (2009, March 31). Lamport's one-time password algorithm. *A design pattern for securing client/service interactions with OTP*. Retrieved from JavaWorld http://www.javaworld.com/article/2078022/open-source-tools/lamport-s-one-time-password-algorithm--or--don-t-talk-to-complete-strangers--.html dated January 22, 2017.

[9] PortalGuard (2012). *The Cost and Loss of NOT Using Single Sign-On with Two Factor Authentication*. Retrieved from www.portalguard.com dated December 11, 2016.

[10] BingoCards (2007, September 17). Bingo Cards. Retrieved, from https://codetechnology.wordpress.com/2007/09/17/bingo-cards/ dated July 30, 2017.

[11] Hoeft, Mike (2014). The bingo queens of Oneida : how two moms started tribal gaming in Wisconsin (First edition. ed.). ISBN 0870206524. Retrieved 20 January2016.

[12] Bhalla, I. (n.d.). *Good Design: Axis Bank- Debit Card Based Authentication*. Retrieved from http://ishanbhalla.com/good-design-axis-bank-debit-card-based-authentication/ dated July 30, 2017.

[13] Entrust (2014). Entrust IdentityGuard Grid Authentication. *Easy-to-use, Cost Effective Strong Authentication.* Retrieved from https://www.entrust.com/wp-content/uploads/2014/03/DS_IDG-GridAuthentication_web_Mar2014.pdf

Benedicto B. Balilo Jr., received the B.S. degree in Computer Science from Dynamic Computer Centrum, Legazpi City, Philippines in 1994. He is a recipient of BU-UC MIT offshore program under CHED FDP II scholarship grant earning his Master's degree in Information Technology (MIT) in 2015 and Master in Business Administration from Aquinas University in 2012. Also, he earned units in Master in Information System in UPOU and Bachelor of Laws in Aquinas University, Legazpi City. He is a 3-termer Municipal Councilor of LGU Sto. Domingo, Albay from 1998-

2007 and former Regional BOD of PCL and NMYL of the Province of Albay.
Currently, he is a recipient of CHED FDP II scholar for the program Doctor in Information Technology (DIT) at Technological Institute of the Philippines (TIP), Quezon City, Philippines. He is presently working his research in information security. He is a faculty member of Bicol University, Legazpi City, Philippines with a rank of Assistant Professor III. He is the PSITE (Bicol Region) Regional President and a member of Philippine e-Learning Society (PeLS), NMYL, PCL and Association for Computing Machine (ACM-Student).

Bobby D. Gerardo is currently the Vice President of Administration and Finance of West Visayas State University, Iloilo City, Philippines. His dissertation is “Discovering driving patterns using rule-based intelligent data mining agent (RiDAMA) in distributed insurance telematic system”. He has published 54 research papers in national and international journals and conferences. He is a referee of international conferences and journal publications in IEEE Transactions on Pattern Analysis and Machine Intelligence and IEEE Transactions on Knowledge and Data Engineering. He is interested in the following research fields: distributed systems, telematics systems, CORBA, data mining, web services, ubiquitous computing and mobile communications.

Dr. Gerardo is a recipient CHED Republica Award in National Science Category (ICT field) in 2010. His paper entitled “SMS-based automatic billing system of household power consumption based on active experts messaging” was awarded best paper on December 2011 in Jeju, Korea. Another best paper award for his paper was “Intelligent decision support using rule-based agent for distributed telematics systems,” presented at the Asia Pacific International Conference on Information Science and Technology, on December 18, 2008. An excellent paper award was given for his paper “Principal component analysis mechanism for association rule mining,” on Korean Society of Internet Information’s (KSII) 2004 Autumn Conference on November 5, 2004. He was given a university researcher award by West Visayas State University in 2005.

Ruji P. Medina is Dean of the Graduate Programs and concurrent Chair of the Environmental and Sanitary Engineering Program of the Technological Institute of the Philippines in Quezon City. He holds a Ph.D. in Environmental Engineering from the University of the Philippines with sandwich program at the University of Houston, Texas where he worked on the synthesis of nanocomposite materials. He finished his MS in Environmental Engineering from the Mapúa Institute of Technology, graduating Summa Cum Laude. He obtained his Bachelor’s degree in Chemical Engineering from the University of the Philippines in Diliman, Quezon City. His research interests include urban mining, electronic wastes, and nanomaterials, He counts among his expertise environmental modeling and mathematical modeling using multivariate analysis.