ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 66, No. 12, pp. 1899~1904, 2017
http://doi.org/10.5370/KIEE.2017.66.12.1899

테이블 패턴 스케줄 기반 OTP 인증

New OTP Authentication Approach based on Table Pattern Schedule

B. B. Jr. Balilo* · B. D. Gerardo* · R. P. Medina* · 변 영 철†
(B. B. Jr. Balilo · B. D. Gerardo · R. P. Medina · Yung-Cheol Byun)

Abstract - This paper presents a new one-time password approach generated based on 4x4 pattern schedule. It demonstrates generation of passkey from initial seed of random codes and mapping out in table pattern schedule which will produce a new form of OTP scheme in protecting information or data. The OTP-2FA has been recognized by many organizations as a landmark to authentication techniques. OTP is the solution to the shortcomings of the traditional user name/password authentication. With the application of OTP, some have benefited already while others have had second thoughts because of some considerations like cryptographic issue. This paper presents a new method of algorithmic approach based on table schedule (grid authentication). The generation of OTP will be based on the random parameters that will be mapped out in rows and columns allowing the user to form the XY values to get the appropriate values. The algorithm will capture the values and extract the predefined characters that produce the OTP codes. This scheme can work in any information verification system to enhance the security, trust and confidence of the user.

Key Words : One Time Password, Two-Factor Authentication (2FA), Information Security

1. Introduction

One-Time Password (OTP) is a generated string of characters and numbers that is used for authentication and valid only for a single transaction or session. In 1979, [1] introduced the concept of OTP to provide effective protection for distributed client/server interaction. In the scheme, the initial seed was used to generated the passkey values which will be formed part of the succeeding seeding process. Many researches have work on different OTP schemes and mechanisms like random number generation, time-based and attribute-based scheme. Others have work on the combination of some parameters to generate OTP values, but, each existing work has its own unique features designed for specific problems.

Many different schemes have been proposed and implemented for protecting information like SMS, biometric technology and smart cards to increase the level of security and reduce the risk of unauthorized access and tampering of data [2]. One reason for differences among these protection schemes is the different functional properties [3]. Moreover, many of these schemes still use mathematical methods or simple combinations of parameters to generate passwords but still suffer potential attacked risks [4].

Currently, the application of attribute-based and combination of different scheme along with other mechanisms (i. e. keyboard and mouse dynamics, screen manipulation, etc) has exposed OTP to different levels of transaction. The more the parameters involved along with algorithm applied the more complex the password values will be produced and the longer space will be covered.

OTP has been recognized in authentication technique for it increases the level of security and added features in protecting and securing confidential and sensitive information. The time period of the password's life span is 180 seconds; the time to break the OTP password in ratio is 166 = 16,777,216 possibilities in a single input of passwords [5].

This paper presents a new one-time password scheme generated based on 4x4 pattern schedule. It demonstrates generation of codes from initial seed of random parameters to mapping of values to XY and extract a new form of OTP scheme in protecting information or data.

2. Related Studies

Leslie Lamport scheme offers the advantage of, free from

† Corresponding Author : Dept. of Computer Engineering, Jeju National University, Korea.
E-mail: ycb@jejunu.ac.kr
* Bicol University, Legazpi City, Technological Institute of the Philippines, Quezon City, West Visyas State University, Iloilo City, Philippines
Received : October 16, 2017; Accepted : November 14, 2017

impersonation and password will not be reused. The values are stored in client side using the mathematical scheme *s=seed, s1=h(s), s2=h(s1), s3=h(s2),…s(n)=h(s(n-1))*, where h is a one-way function with s in an incremental value. 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 (client side), and validate client-provided passkeys included in each client-initiated request (service side) [6]. Currently, there are various innovations on one-time password researches including those with latest technologies and combination of the different methods-like random number generation [8, 20], time based [10-12], monitor [20], keyboard and mouse manipulation [9], location, and IP address. Each method can be applied in both mobile phones using SMS gateway [15, 16] and email system.

Other researches include, the use of hash function MD5 together with the username, SPP and random number generation or timestamp [13]. The scheme can withstand decimal attack and re-play attack. However, the weakness of MD5 and SHA-1 algorithm was found to produce collisions with only 242 hashes can be solved by PingPong128 stream cipher. PingPong-128 cipher is a specific cipher from the PingPong family of stream ciphers [14], QR Codes [17, 18], and dropped call [19].

3. Proposed Approach

The design concept of the study presents a total of 87 characters as parameters for OTP two-factor authentication. The algorithm used a combination of RNG, attribute-based and string manipulation technique. Let initial seed represented by letter g to be the *string of characters + numbers + date + timestamp*. Using the formula, the initial seed captures the current OTP and integrated as part of the next OTP to be generated. The letter b represents the OTP to be generated.

A total of 87 characters will serve as parameters. The generation of OTP is represented by the formula *OTP = xy(PassCode, Combi (aA, Num,Date,TimeStamp),2)* producing a two(2) pair code. The XY values will be randomly selected and formed the 6 character codes.

Table 1 shows the process of generating the OTP codes. The random codes will be accessed sequentially and will be mapped out into the sequence pattern table consisting of steps and operations. On the retrieve process, the sequence codes will be randomized with mixtures of lowercase and uppercase letters and numbers as the initial seed.

Table 1 Algorithm of the proposed study

```
ALGORITHM:

  set param =
  A..Za..z0..9 datetimestamp
  set Array
  do{
        generateTwoPairValue( )
        displayTwoPairValue( )
        increment flag;

        if (flag>3 {
            flag=0;
            increment cn;
        }
  }

  getRandomTwoPair( )
  finalOTP =
     middleSquare(GetTwoPair())
  print final OTP
```

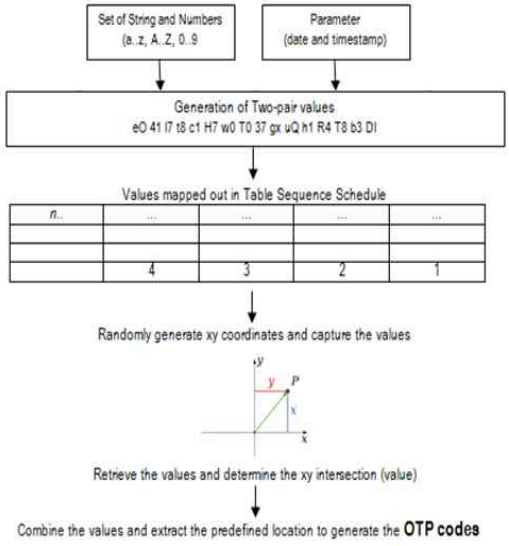

Fig. 1 The diagram showing data flow in OTP generation process

Here are the step by step sequences for the processing.

- The combination of strings (a..z, A..Z), number (0..9), parameters (date and timestamp) will form the initial seed.
- A generated two pair values is produced to be mapped out in the table sequence.
- From the table sequence will produce the random values and randomly generate the XY values. These values will be part of the OTP codes.
- The XY values together with the intersected value will form another value for consideration in the determination of the OTP code.
- The values of the XY and its intersection will determine

the predefine location to produce the OTP codes. These codes will be the final and actual OTP.

The combinations of characters were initialized in an array together with the parameters to form the initial seed of the code. A two-dimensional was set for XY values, each of which had parameters but produced different randomized codes. The weight of the algorithm put emphasis on the generation of two separate randomized codes stored in array as temporary storage and random selection of XY coordinates from the mapped table schedule avoiding the 0,0 values. The mapping of values returns the row and column element.

Table 2 Sample XY-duplication prevention statements

Line	Statement
1	$row_element = rand(0,7);
2	$col_element = rand(0,7);
3	if ($row_element==0)
4	{
5	$row_element = rand(0,7);
6	}
7	if ($col_element==0)
8	{
9	$col_element = rand(0,7);
10	}

It is important to avoid producing the 1:1 XY coordinate in the table as it will only duplicate the values producing similar codes. In Table 2, in order to avoid such result, the row and column element was processed randomly and checked whether the zero value was produced, if the values generated matched the zero value then randomization process shall be initiated.

This means that the process of generating OTP shall pass through two (2) randomization processes. The processes include the generation of initial seed and sequence pattern schedule. This is an improvement to the OTP concept generating the 4x4 matrix sequence schedule. Upon verifying the OTP, mutual authentication will be accomplished, and the user can now work on trusted communication.

4. Implementation and Results

The implementation of the proposed algorithm was simulated the following specifications: XAMPP/1.8.1, BootStrap, Apache/2.4.3, Sublime and PHP Language version 5.4. These applications were used for the purpose of determining the runtime performance of the proposed OTP authentication. The performance of the developed OTP authentication model was performed on a PC with Intel Corei5-4460 32-bit processor based running at single processor 3.210GHz with 4GB of memory, 32bit Service Pack (SP1) Operating system (OS) and 1Mbps ISP bandwidth.

Fig. 2 shows the sample generated 4x4 table schedule and XY values. The matrix was sent via registered email address, completing the challenge process.

The privileged access was granted to limited user only. The minimal access control and least privilege to the system will bring slice to security level allowing access only to information and resources that are necessary for legitimate purpose. The principle of least privilege is important in enhancing the protection of data and functionality from faults and malicious behavior. Among the benefits of this

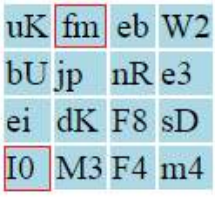

Fig. 2 Sample generated 4x4 table schedule and XY values

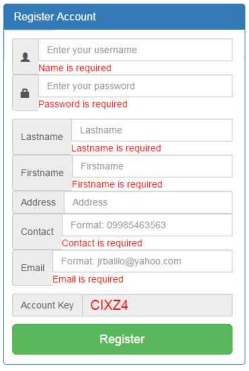

Fig. 3 A Snapshot of Sample Registration

Fig. 4 A Snapshot of Login for a user

Fig. 5 A Snapshot of OTP Window

OTP: nzBMsA

Fig. 6 Sample Result of OTP using Middle Square Technique

Table 3 Results from simulation based on runtime performance of the proposed algorithm

Indicators	First Round	Second Round	(F+S)/2
Generation of two (2) pair codes	0.238	0.241	0.239
Generation of 4x4 matrix schedule	0.040	0.161	0.100
Total Runtime	1.499	1.709	1.604

principle includes better system stability, better system security, and ease of deployment [19]. Fig. 3, 4, and 5 show the sample registration, login and OTP window, respectively.

The registration phase allows the user to input the details for proper login authentication. To control the usability of the system, login and OTP validation works in login attempts. User will be redirected after three(3) failed login attempts. Also, user will be redirected if no mouse movement will be monitored.

Fig. 6 shows the sample result of OTP using middle square technique. The challenge process was given by the xy pattern (nz and BM) that intersect the code sA. These patterns of code will be grouped to form the initial seed (i.e. nzBMsA), and the center four (4) characters will be extracted as the final OTP codes.

Table 3 shows the results of the test performed through simulation in two (2) separate rounds with the interval of five (5) minutes. The algorithm produced a total runtime performance of 1.604 msec. Simulating in two (2) rounds, the results of generating pair codes was 0.239 msec and generation of 4x4 matrix schedule (0.100 msec).

5. Conclusion

Every authentication technique has its own unique feature. The One Time Password has been part of the day-to-day authentication mechanism adopted by many companies, organizations and institution to grant access to authorized user and protect confidential and sensitive information. The new algorithmic OTP scheme based on table sequence pattern schedule provided a new level of security for users as it applied a new scheme in generating OTP codes allowing the pair of codes to be randomly generated and mapped out in tables. It made use of XY schedule send to user with successful advantage over the printed grid scheme like BINGO card.

The results were conclusive that the proposed improvement on OTP scheme proved to generate a randomize XY 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 and the system in general were conclusive that the new algorithm posed advantage over traditional authentication and OTP printed scheme as this incurred cost in printing the OTP codes. The study further states that the comparative analysis yielded conclusive ratings taking advantage of the proposed OTP scheme. This means the new OTP scheme managed to handle the procedure with less operations with minimal number of elements.

Acknowledgments

This research was supported by the 2017 scientific promotion program funded by Jeju National University. Our thanks to Technological Institute of the Philippines, Commission on Higher Education and Bicol University for the support extended.

References

[1] QueensLand Government, “Disaster Management Phases. The State of Queenland 2010-2013,” http://www.disaster.qld.gov.au dated January 6, 2017.

[2] Phil-Japan. Philippines, Japan sign agreement on disaster communication, http://www.gov.ph, 2014.

[3] Zukime, M., Junoh, M., Osman, A., Ab Halim, M.S. & Adbullah, S. “Data Security: Issues And Challenges For Disaster Management In The New Millennium,” International Journal of Scientific & Technology Research 3(8), 2014.

[4] Semer, L.J., "Disaster recovery planning for the distributed environment," Internal Auditor, Vol. 55 No. 6, pp. 41-47, 1998.
[5] Javidan, R. & Pirbonyeh, M.A., "A new security algorithm for electronic payment via mobile phones," 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2010.
[6] Lacona, L. J., "Lamport's one-time password algorithm. A design pattern for securing client/service interactions with OTP," http://www.javaworld.com/article/2078022/open-source-tools/lamport-s-one-time-password-algorithm—or—don-t-talk-to-complete-strangers--.html, 2017.
[7] Shally & Singh Aujla, G., "A Review of One Time Password Mobile Verification," International Journal of Computer Science Engineeringand Information Technology Research, Vol. 4, Issue 3, pp. 113-118, 2009.
[8] Fan, Y.T. and Su, G.P., "Design of two-way one-time-password authentication scheme based on true random numbers," 2nd International Workshop on Computer Science and Engineering, vol. 1, pp. 11-14, 2009.
[9] Chen, X.J., Xu, F., et al. (n.d.). "A Practical Real-Time Authentication System with Identity Tracking Based on Mouse Dynamics," INFOCOM, pp. 121-122, 2014.
[10] El-Booz, S.A., Attiya, G., and El-Fishawy, N. (2015). "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol," 11th International Computer Engineering Conference: Today Information Society What's Next?, pp. 188-194, 2016.
[11] Sudhakar, K., Srikanth, S., & Sethuraman, M., "Secured mutual authentication between two entities," IEEE 9th International Conference on Intelligent Systems and Control, DOI: 10.1109/ISCO.2015.7282338, 2015.
[12] Huang, Y., Huang, Z., Zhao, H., and Lai, X., "A new One-time Password Method," IERI, 2013.
[13] Li, Y., "Research on e-business identity authentication system based on improved one-time password," International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-5, 2008.
[14] Davaanaym, B., Lee, Y.S., Lee, H, Lee, S., and Lim, H., "A Ping Pong based one-time-passwords authentication system," 5th International Joint Conference on INC, IMS, and IDC, pp. 574-579, 2009.
[15] Sediyono, E., Santoso, K. I. and Suhartono, "Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS," International Conference on Advances in Computing, Communications and Informatics, pp. 1604-1608, 2013.
[16] Alghathbar, K. and Mahmoud, H.A., "Noisy password scheme: A new one time password system," Canadian Conference on Electrical and Computer Engineering, pp. 841-846, 2009.
[17] Kumar, D., Agrawal, A. & Goyal, P., International Conference on Advances in Computer Engineering and Applications. IMS Engineering College, Ghaziabad, India. 978-4673-6911-4/15, 2015.
[18] Liao, K.C., Lee, W.H., Sung, M.H., & Lin, T.C., "A one-time password scheme with QR-code based on mobile phone," International Joint Conference on INC, IMS, and IDC, pp. 2069-2071, 2009.
[19] Sodhi, B., "Using dropped call as an authentication factor," 15th IEEE International Conference on Computer and Information Technology, pp. 2031-2035, 2015.
[20] Margosis, A. "Problems of Privilege: Find and Fix LUA Bugs," Microsoft, 2006.

저 자 소 개

Benedicto B. Balilo Jr.

He 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 program for the program Doctor in Information Technology (DIT) at Technological Institute of the Philippines, Quezon City, Philippines. He is a faculty member of Bicol University, Legazpi City 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

Dr. 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 in distributed insurance telematic system". 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, data mining, web services, ubiquitous computing and mobile communications. His paper entitled "SMS-based automatic billing system of household power consumption based on active experts messaging" was awarded best paper in 2011. Another best paper award was "Intelligent decision support using rule-based agent for distributed telematics systems," presented at the Asia Pacific International Conference on Information Science and Technology, 2008. An excellent paper award was given for "Principal component analysis mechanism for association rule mining," in 2004. He was given a university researcher award by West Visayas State University in 2005.

Ruji P. Medina

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.

Yung-Cheol Byun

Dr. Byun is a full professor at the Computer Engineering Dept. (CE) at Jeju National University. His research interests include the areas of AI, Machine Learning, Intelligent Security System, and RFID & IoT Middleware. Outside of his research activities, he has been hosting international conferences, CNSI, ICESI, and also serving as a chair in various international conferences. He received his Ph.D. from Yonsei University in 2001. Before joining the current university, he was a senior researcher of Electronics and Telecommunications Research Institute (ETRI).