Scientific Journal of Impact Factor (SJIF) : 3.134

ISSN (Print) : 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

One Time Password Generation Using Mathematical Random Function In Sphere Space For Mid-Sized Applications

[1]Ishupreet Kaur, [2]Gargi Narula

[1]Computer Science & Engineering Department, SVIET, Patiala, Punjab, 140601, India ,kaurishupreet1@gmail.com
[2]Computer Science & Engineering Department, SVIET, Patiala, Punjab, 140601, India ,garginarula@gmail.com

Abstract--*The proposed vOTP scheme is designed by keeping the mid-sized online application requires the OTP scheme. The proposed one time password scheme is used to generate the one time password from the spherical space using random function from a larger spherical number space. This technique is useful to generate thousands of unique and unrepeatable OTPs at one point of time. The results have shown that the system can serve a large number of users every minute. The system is capable of serving one user in fraction of seconds, 100 users in 28 seconds and 1000 users in less than 10 minutes.*

Keywords—*one time password, random function, sphere space, phishing attack, multiple ID generation attack.*

I. INTRODUCTION

The One Time password is unique value which can be used for one transaction only. Once it is used it becomes outdated. One Time Password can be generated Time Based and Event Based. It is used to prevent our system from unauthorized access and harmful attacks. Similarly, One Time Password can also be used to prevent against botnet attacks. Botnet attacks are the attacks in which the bot programs are installed on users system without its prior knowledge. This bot attack can be a snooping attack or a key logger attack.

Now, whenever a OTP is used for authentication purpose, it can be a text or graphic based. Because we are using OTP against Botnet/Autobot, we will be using graphics based OTP. As bot programs which are available can detect the text-based passwords but they cannot recognize graphics. A text based OTP is generated using a random generator function which is later converted to graphics based password. One Time Password can be delivered to the user using many ways like mobile phone, e-mail, etc.

The Basic Idea of this scheme is to generate a One Time Password for authentication purpose and each time the one time password generated should be unique. The one time password adds another layer of security to login process used widely over internet for authentication. One time password can be generated using spherical random function which has a large amount of number and can produce unique combinations. Spherical random function is capable of generating more unique combinations of integers than any other mathematical random function. Then the random is uniquely selected among the sphere matrix, which creates more unique passwords. Then the integer based password is converted into image hardens the security layer of the mobile/SMS based authentication environments. The visual form of OTP increase the security of the authentication process and protect passwords against interception attacks, the concept of one-time visual passwords (OTVP) is proposed. The OTVP concept takes advantage of the differences between computer encoding of data and the human visual perception of images.

Here, we have taken a Client and Server based architecture. In this, a authentication request is made by client to server. And server will send a text based password to client. Further, the text based password is converted to graphic based password. If the recipient is actually a human being, then a human can recognize the graphic and get authenticated. But if it is a Autobot or botnet, then it cannot recognize the password received and authentication is failed. The graphics based password can be delivered to client using MMS, watsapp or email. Therefore, the given mechanism can be used for authentication purpose in online portals where Autobot are using users identification for login purpose without their consent. Then the bots can steal important information or can have financial gains. So it is better to use graphics based one time password to prevent from autobots or botnet problems.

II. LITERATURE REVIEW

R.R.Karthiga and associates have proposed an OTP generation technique to minimize the damage by phishing and spyware attacks. The OTP is used to authenticate the clients to protect the server from unauthorized access using the long-term public keys and digital certificates. Ahmad Alamgir Khan et al. have discussed the phishing attack used by cyber criminals to steal the user's personal information, credit card or debit card information in detail. The authors have also proposed the security mechanism against phishing attacks. The proposed approach is based on the OTP retrieval using SMS or email systems., which are submitted by the users to the server and server reverts the decision logic after inspection. The OTP is used an encrypted token in very smart way to tackle the phishing attack problem. Andrew Y. Lindell et al have performed the comparison of two approaches of the OTP: time-based OTP and event-based OTP. They have provided the usability and security comparison of both of these one time password techniques. Both of the techniques compared under this comparison uses cryptographic mechanism. Mihai Ordean and his research associates have conducted the performance analysis of security and usability of authentication systems based on components. They have introduced the one-time visual authentication (OTVP) concept which in real is representing a novel approach to the security of authentication interfaces that combines one-time passwords (OTPs) with visual authentication interfaces

III. EXPERIMENTAL DESIGN

The major task of the proposed system is to create the one time password based on the random sphere value space to authenticate the users to avoid various cyber attacks like phishing attack. The one time password generation scheme must be able to produce a larger space of unique passwords so that it can be used to authenticate multiple users at one time without any duplicity.

The OTP adds an extra security layer to protect the user login. The OTPs are widely used over internet for authentication.OTP generation is using values in the sphere space based random number generation system for large density users at once. Cubic random function provides the capability of larger number of random number combinations. The OTP generation initially generates the matrix of million values. The different numbers of values are randomly selected among the million values generated earlier and concatenates them to make an OTP. Then the complex number is converted into integer based password is converted into image using visual encoding makes it more secure and send it via mobile/SMS based authentication environments.

Algorithm: OTP Generation Algorithm

Step 1: Sphere Random Function to generate random number

A. *Initialization of the random number generator and calculate the angle of elevation in the sphere. Sphere contains values in open interval,* $(-\pi/2, \pi/2)$ *, but not uniformly distributed.*
B. *Creation of the angle of azimuth for each sphere point on the basis of uniformly distributed in the open interval,* $(0, 2\pi)$
C. *Compute radius value for each point based on open interval,* $(0, 3)$ *not uniformly distributed.*
D. *Rearrange and concatenate the random matrix values and return OTP.*

Step 2: Visual encoding

A. *Break OTP into list of characters*
B. *Convert each character to ASCII value*
C. *Fetch the visual code/encode for ASCII value for each character in the list*
D. *Concatenate the visual encoding of all characters to form an image and Return vOTP*

Step 3: Client/Server Communication

A. *Server send the vOTP to client system using SMS or MMS or Other-App.*
B. *Client submits the OTP to server on web portal*
C. *Server verifies the replied OTP and return the decision logic*

IV. RESULT ANALYSIS

The experimental design has been developed using MATLAB simulator and the results have been observed and analyzed deeply. The OTP generation procedure is using multi-level random value generation from the sphere, and further concatenated in uneven fashion to produce the unique one time password every-time. One time password generation process is flexible and unique to produce the unique one time passwords at one point of time to reduce the possibility of two users receiving the same password at one point of time. This random one time password generation framework can used with medium or smaller sized web or utility based portals. This sequence will be able to handle thousands to tens of thousands of users at one point of time. The uniqueness calculation has shown that this OTP framework is capable of handing flexible number of unique OTP at one point of time with minor changes in the program sequence. The framework simulation is designed to generate the one time password which is followed by visual encoding to produce one time image password (OTIP). OTIP is then forwarded to the client side, where client enters the password the OTP input box and submit the information to the server side. The server then verifies the original OTP with the generated OTP and returns the decision logic, which is further used to take the programmed action in the software architecture according to the decision logic. The OTP send by the Client to Server is compared with the OTP generated and saved at the Server. If the both the OTPs are same, then the OTP is verified and the access is granted.

Rotation Size	Time in Seconds
1	0.23
10	2.63
50	12.69
100	28.71
200	61.14
500	190.53
1000	505.43

Table 1: The Time (in seconds) to Rotations size comparison table

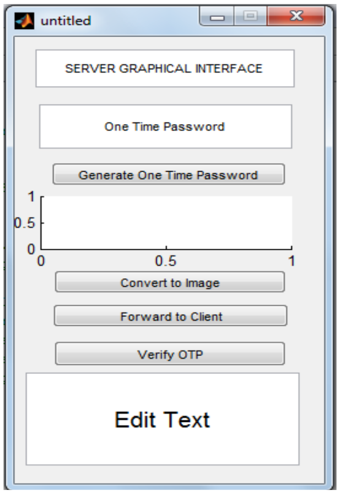
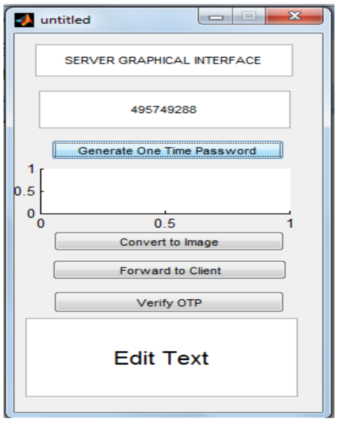
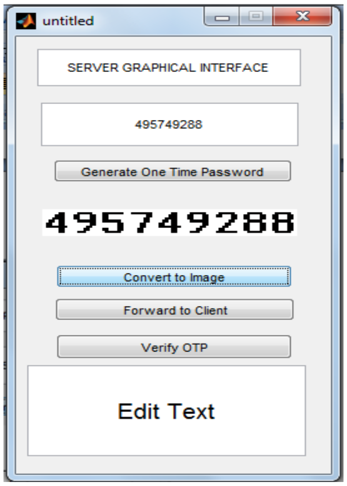


Figure 1- The Server Graphical Interface



495749288

Figure 2- Generate One Time Password

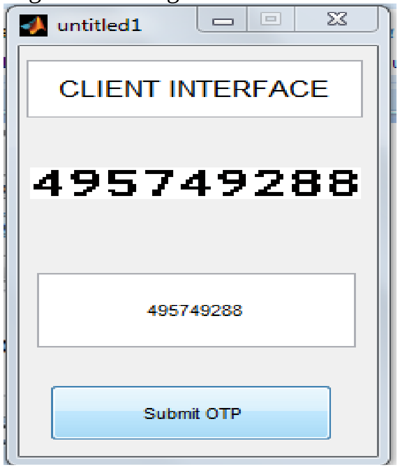


495749288

495749288

Edit Text

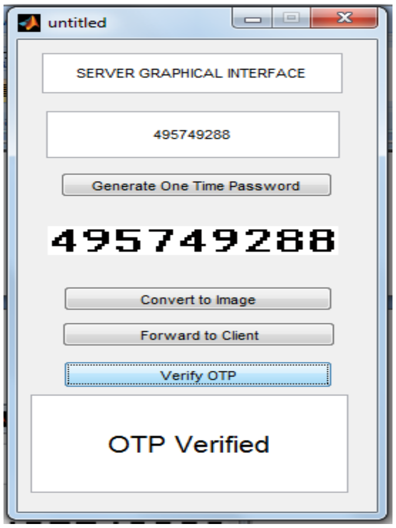
Figure 3- Convert Integers into Image Based Password and forward to client



495749288

495749288

Figure 4- The user retrieve the vOTP and submit the OTP to the server.



495749288

495749288

OTP Verified

Figure 8- The OTP Verification

The OTP send by the Client to Server is compared with the OTP generated and saved at the Server. If the both the OTPs are same, then the OTP is verified and the access is granted.

V. CONCLUSION AND FUTURE WORK

The proposed vOTP scheme is a scheme is capable of producing a large number of unique word in one time space to facilitate its implementation with mid-sized user authentication applications. The proposed OTP scheme generates the password from the cubic value space using random number selection function from a larger possible numbers in the space. This technique is useful to produce thousands of unique OTPs at one point of time. The results have shown that the system can serve a large number of users every minute. The system is capable of serving one user in fraction of seconds, 100 users in 28 seconds and 1000 users in less than 10 minutes. In future this scheme can be enhanced using the dizzy images scheme, which also protect against the botnets/autobots with image processing or optical character recognition capability. Also this scheme can be enhanced to produce alphanumeric passwords and can be used with existing or improved visual encoding scheme.

REFERENCES

[1] R.R.Karthiga, 2013."One-time Password: A Survey", International Journal of Emerging Trends in Engineering and Development Issue 3, Vol.1, pp. 613-623.
[2] Ahmad Alamgir Khan, 2013. "Preventing Phishing Attacks using One Time Password and User Machine Identification", International Journal of Computer Applications (0975 – 8887) Volume 68– No.3.
[3] Indu S., Sathya T.N., Saravana Kumar V., 2013" A Stsnd-alone and SMS-Based approach for Authentication using Mobile Phone", IEEE-International Conference on Information Communication and Embedded.
[4] Andrew Y. Lindell, 2007."Time versus Event Based One-Time Passwords", Aladdin Knowledge Systems.
[5] Soonduck Yoo1 , Seung-jung Shin1, Dae-hyun Ryu1, 2013. "An effective Two Factor Authentication Method using QR code", ISA 2013, ASTL Vol. 21, pp. 106- 109, © SERSC 2013.
[6] www.ietf.org
[7] Bin Li, Shaohai Hu, Yunyan Liu, 2006."A Practical One-Time Password Authentication Implement on Internet", ICWMMN Proceedings.
[8] Ping Wang, Lei Wu, Baber Aslam and Cliff C. Zou, 2009. " A Systematic Study on Peer-To-Botnets", International Conference on Computer Communications and Networks, 2009. ICCCN 2009. San Francisco, CA, IEEE.
[9] Yu tao, Fan, Gui ping, Su, 2009."Design of Two-Way One-Time-Password Authentication Scheme Based On True Random Numbers", Second International Workshop on Computer Science and Engineering, pp. 611-614.
[10] Jivika Govil, 2007. "Examining the Criminology of Bot Zoo", IEEE.
[11] Mihai Ordean, 2012. "Secure Authentication Using One Time Visual Password", Ph.D. Dissertation, The technical university of Cluj-Napoca.
[12] Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, and Jingyuan Zhang, 2009." Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures", Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2009,11 pages doi:10.1155/2009/692654
[13] Julian B. Grizzard, Vikram Sharma, Chris Nunnery,and Brent Byung Hoon Kang, David Dagon, 2007, "Peer-To-Peer Botnets: Overview and Case Study". HotBots'07 Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. USENIX Association Berkeley, CA, USA.
[14] Abebe Tesfahun and D.Lalitha Bhaskari, 2013. "Botnet Detection and Countermeasures- A Survey", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, ISSN 2278-6856.
[15] Takasuke TSUJI, 2003. "A One-Time Password Authentication Method", Kochi University of Technology.
[16] Márk Jelasity, Vilmos Bilicki, 2009. "Towards Automated Detection of Peer-To-Peer Botnets: On the Limits of Local Approach", Hungary, www.usenix.org
[17] S. Behal, A. S. Brar, and K. Kumar, "Signature based Botnet Detection and Prevention", ISCET, pp. 122-127, 2010.