International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Protection against Multi-Id Generation Autobots/Botnets Using Using Colored Visually Encoded OTPs Generated by the Random Function in the Spherical Space

Taranpreet Kaur[1], Harmandeep Singh[2]

Punjabi Univeristy, Patiala, India

Abstract: ***The one time passwords are the password valid for only one transaction or login. One time password authentication system protect the IT systems against repeated access, replay attacks, click frauds, etc. The alpha numeric one time passwords are sent to the user end using mobile phone or email. Existing OTPs are prone to the bot attacks, where bot is given access to the mobile phone or email system to auto submit the OTP on the online portal. In this paper, a new graphical password scheme is being proposed to protect against the repeated access, which can be stopped by using the graphical one time password scheme. The dizzy and unreadable graphical one time passwords will be created using colored visually encoded OTPs generated by the random function in the spherical space. The spherical space is having a large number of unique values and later encoded visually using pre-programmed visual encoding for each character being used in the OTP generation. The new graphical OTP will be sent to users end using email, MMS or chatting aps. The proposed system is adaptable to the small-sized to mid-sized online portals requiring the OTP service.***

Keywords: One time password, Protection Against autobots, Protection against botnets, Sphere random function, Visual Encoding

1. Introduction

One-Time Password (OTP) is a password that can be used only a single time. After it has been used, it becomes invalid (or depleted) and cannot be used again. This helps to prevent some shortcomings of static passwords – passwords that do not change typically. It avoids the various attacks that occur on static password such as replay attack, man-in-middle attack, phishing, keyboard logging etc. It also prevents the identity theft by ensuring that same password cannot be used again. Today the use of OTP is prevalent, most of corporate companies, banks etc use OTP to authenticate users. There are different ways to generate OTP's depending upon security, convenience, cost and accuracy; and each has its own significance. There are basically two types of OTP's, time based and event based. In time based OTP, OTP is generated at frequent interval and at particular time value of OTP is current time and is valid for few minutes. In event based OTP, OTP is generated by applying random looking cryptography function to a series of unique values and is valid until the request of next OTP.OTP is much better than static password but still it suffers from botnet attack which continuously have the generated one-time password . Botnet is a network of compromised computers which run malicious software that are installed through various attacks such as Trojan horse, worms and viruses. These computers are under control of attacker who initiates the various activities as like email spam, denial of service attack, password cracking and key logging. Botnet create two basic structures among compromised computers, one is centralised and other is peer-to-peer. In centralised structure, attacker has direct control of all compromised computers and in peer-to-peer, all compromised computers are connected with each other. In order to prevent the OTP from botnet attack, we convert the one-time password into image by coding in Matlab which will become one time visual password. We follow this approach because one time password is captured by botnet but it is not able to understand the one-time visual password. Thus one-time visual password confirms the identity of user as only user retrieve one-time password from an image of one-time password. We use random mathematical function to create one time password the transform it into image by using graphical user interface.

2. Literature Review

In this survey report the research papers published by a number of authors related to the discipline of preventing autobots with one time password using fool proof image representation are taken into consideration and discussed. **R.R.Karthiga et al. (2013)** he proposed a OTP survey and find that to reduce the damage of phishing and spyware attacks, banks, governments, and other security-sensitive industries one-time password is required. The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates. Authentication is based on knowledge of the shared password. **Indu S. et al. (2013)** describes a method of implementing two factor authentication using mobile phones. The proposed system involves using a mobile phone as a software token for One Time Password generation. OTP algorithm powered with user's unique identifications like International Mobile Equipment Identification and Subscriber Identification Module; makes a finite alphanumeric token valid for a session and for a single use. The generated One Time Password is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization. **Ahmad Alamgir Khan et al. (2013)** discussed the problem of phishing which is a type of attack in which cyber criminals tricks the victims to steal their personal and financial data. It has become an

organized criminal activity. Spoofed emails claiming to be from legitimate source are crafted in a way to lead victims to reveal their personal, financial data by misdirecting them to the counterfeit website. It presents a novel approach to combat the Phishing attacks. An approach is proposed where user will retrieve the one time password by SMS or by alternate email address. After receiving the one time password the web server will create an encrypted token for the user's computer/device for authentication. The encrypted token will be used for identification, any time user wishes to access the website he/she must request the new password. The one time password and encrypted token is a smart way to tackle this problem. **Andrew Y. Lindell.et al. (2007)** compare the two main approaches to one-time passwords (OTP): time-based OTP and event-based OTP. Our main conclusion is that they are very similar from both a security and usability perspective (with each having slight advantages of a different nature). **Soonduck Yoo1 et al. (2013)** discussed that the most prevalent form of login has used an ID and password which is classified 1 factor authentication. However the lax of security, user required the more secure way to login so firms have implemented 2 factor authentication involving OTP(One time Password). Despite the increased security, users must endure the inconvenience of downloading a program on their device and inputting a 6 to 8 digit code. In his study he explore leading 2 factor authentication programs that combines both security and convenience using QRcode. By scanning QRcode with smart phone users can login to the website without to put a 6 to 8 digit code such as OTP. This is able to solve the key logger problems and provide the strong security on line system. Users can enjoy the both security and convenience.

3. Botnet/Autobot Attacks

Authentication process is a way to protect the network for illegitimate access. In a Client-Server Architecture it is required to authenticate client, server and the network between them. The attackers can attack the network by using illegal means like spoofing, phishing, bot/botnet. Authentication process can be understood using Authentication Interface and Authentication protocols. The Authentication interface is human-computer interface (HCI). HCI is the way by which human interacts with the authentication process. It can be text based or graphic based. The authentication interface suffers from problems like weak passwords and shoulder surfing. The Authentication protocol is the verification of client and server and the safe and reliable transmission of messages between during authentication. This kind of protocol mostly suffers from problems of Man-In-Middle attacks and replay attacks. Most web based services uses two components for authentication i.e. ID & Password. Now for successful authentication of the person, the combination entered by the person to be verified should be same with that of the combination saved in the database of server.

The passwords are secret phrases which are used for safety purposes against various attacks over the internet. The traditional static password is a password that remains same in every login session and they are always at risk of replay attacks because they can be easily hacked by intruder. This shortcoming can be solved using One Time Password. One Time Password (OTP) is a password which is different for every session. It can be a list of passwords available with the user and each time user uses a different password. OTP which has been once used from the list is no longer valid for next session. One Time Password can also be generated every time the requests for it. One Time Password authentication helps preventing the access to unauthorized access to restricted areas.

4. Proposed Model

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.

5. Experimental Design

Algorithm 1: OTP algorithm flow

1. First, initialize the random number generator to make the results in this example repeatable.
2. Calculate an elevation angle for each point in the sphere. These values are in the open interval, $(-\pi/2, \pi/2)$, but are not uniformly distributed.
3. Create an azimuth angle for each point in the sphere. These values are uniformly distributed in the open interval, $(0, 2\pi)$
4. Create a radius value for each point in the sphere. These values are in the open interval, $(0, 3)$, but are not uniformly distributed.
5. Randomly select and concatenate the coordinates or values to create the OTP.
6. Return OTP
7. Count characters in **OTP**
8. Convert char variable **OTP** to ASCII array, denotes **ascOTP**
9. Find the correspondent pre-defined ASCII number graphical encoding for ***ith*** array value **ascOTP(i)** → **gOTP(i)**
10. Concatenate the visual encoding of all characters to form an image, C←**horzcat (C,gOTP),** where **horzcat** is horizontal concatenation function.
11. Repeat B to D on all index values of **ascOTP** in group of two values in each rotation

12. Return Visually encoded **vOTP**
13. Server forwards the generated visual OTP to client/user via SMS/MMS/Other-App.
14. Client/User submits the OTP on web portal, wherever it is required or requested.
15. Server receives the reply as OTP submitted by client/user
16. Server verifies the OTP reply.
17. Returns the decision logic

6. Result Analysis

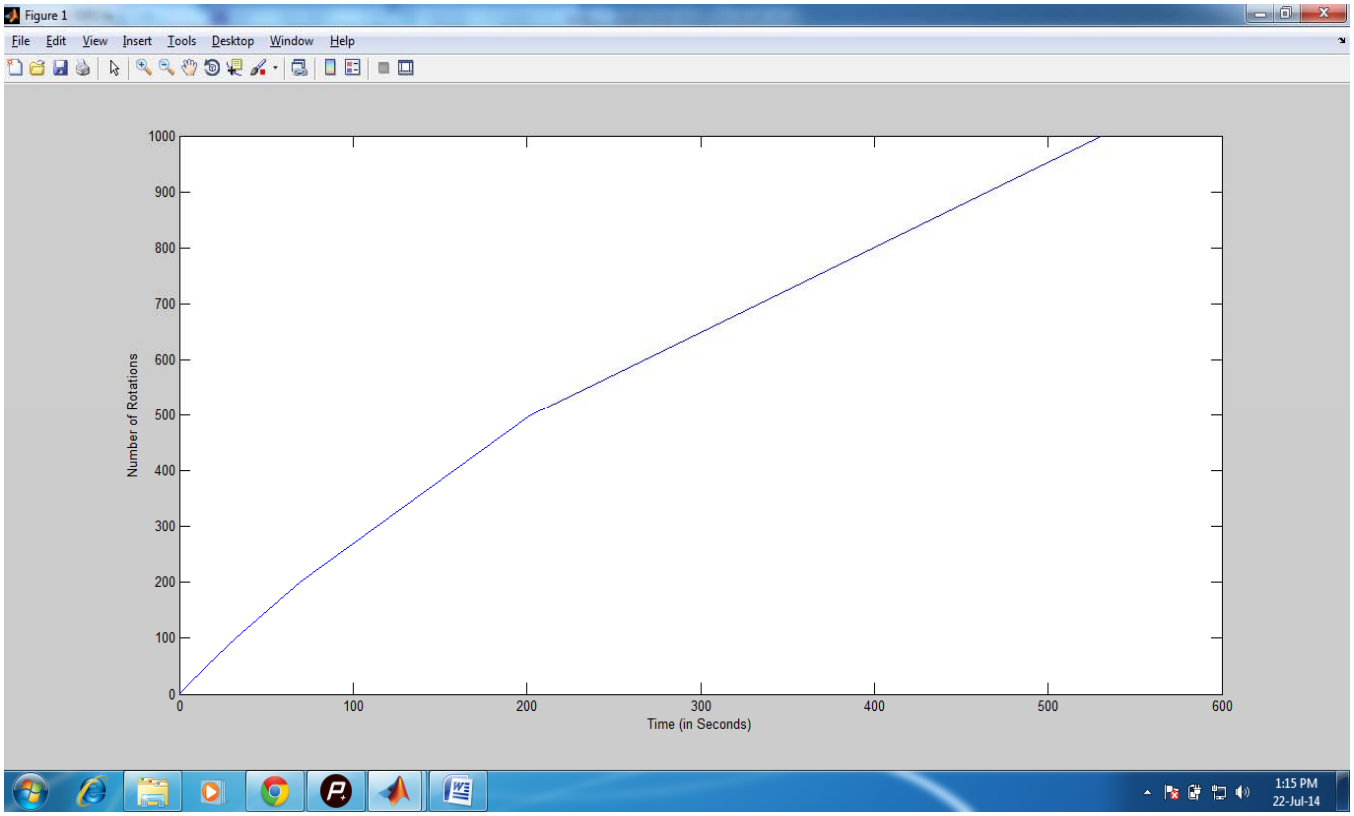
The experimental design has been developed using MATLAB simulator and the results have been observed and analyzed deeply. The OTP generation procedure is using multi-level random value generation from the sphere, and further concatenated in uneven fashion to produce the unique one time password every-time. 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

Table 1: The uniqueness of one-time passwords shown for 5 rotations

Sr. No.	Rotation 1	Rotation 2	Rotation 3	Rotation 4	Rotation 5
1	25286222	209279231	248264273	289234261	238292210
2	27422498	287294297	283218245	107271247	263180221
3	256159207	202283285	294244194	136262282	270171123
4	138292287	115206291	102187199	296264253	184291160
5	165252216	264273278	229227134	205258277	284232255
6	152262204	151261283	289260210	43249272	128251226
7	273265151	250202227	230254287	255200256	292149276
8	286269237	287245139	297240197	213295190	291227266
9	286162191	184223227	218244197	300273282	20116962
10	259299293	264220274	156246276	263216188	193295229

Table 2: The Time (in seconds) to Rotations size comparison table

Rotation Size	1	10	50	100	200	500	1000
Time in seconds	0.3484	3.1416	15.6925	32.6291	69.2329	201.9823	530.5974



Graph 1: The time (in seconds) to Rotation size graph

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 OTPs are same, then the OTP is verified and the access is granted.

Figure 1: The Server Graphical Interface

Figure 2: Generate One Time Password

Figure 3: Convert Integers into Image

Figure 4: Forward the Image Based Password to the Client

Figure 5: Client Interface receives Image Based Password.

Figure 6: The user or client reads and Fill the image password.

Figure 7: The user submit the OTP to the server.

Figure 8: The OTP Verification and decision Logic

7. Conclusion

OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are used in real-time systems. Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time), Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order) or Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. The purpose of a **one-time password** (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced. But the text based one time passwords are not being proved to be strong enough to protect against the bots accessing the online portals. Hence, there has to be an strong and secure alternative to the text based one time passwords. By taking the above research gap in account, the new one time password authentication system is proposed in this research. The proposed one time password scheme is a scheme which can be widely accepted over the internet applications. This scheme generates the password using the sphere random function, which carries a heavier amount of numbers and can produce many 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. The conversion of the integer based password into image hardens the security layer of the mobile/SMS based authentication environments. Also, sphere random function generates the passwords very quickly, which means it is perfectly adaptable to the internet application scenarios with millions or billions of users.

8. Future Work

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. Some new scheme can proposed in future to generate the passwords in larger number than the proposed system to meet the requirements of the large online enterprise applications. Also the new one time password scheme can be used along with the SSL or other innovative encryption layer to produce the more secure one time password authentication system.

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] S. Behal, A. S. Brar, and K. Kumar, "Signature based Botnet Detection and Prevention", ISCET, pp. 122-127, 2010.
[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