One Time Password Using Sphere Angle Based Random Password Generation for Online Portals - A Review

[1] **Ishupreet Kaur,** [2] **Gargi Narula**

[1, 2] Computer Science & Engineering Department, SVIET, Patiala, Punjab, 140601, India

Abstract - The one time passwords (OTPs) are widely used in the various application to protect the bot or autobot from repeated access without human interaction to the online portals. The OTPs are usually sent over the mobile phone numbers, from where the user read, fill and submit the one time password, which is later verified on the server side and the next step is taken according to the requirement. These message based OTPs are prone to the various autobot/bot based repeated access attacks because it is easier to read the message automatically fromt the phone. Also it can be easily submitted using automatic form submission script. In this paper, we have proposed a new image based OTP which can be sent to the user's phone using MMS or various other social or chatting applications. The image based OTP provides more harden protection from the bot/autobot. than the ordinary text-based OTPs. The OTP is generated using the elevation angle and azimuth angle followed by radius value matrix, which provides a robust environment to generate the unique OTP every time. The OTP is the converted into the image using ASCII character identity based visual encoding which will be forwarded to the user later. The new technique can be used on various web portals require OTP on service.

Keywords **- One Time Password, Autobots, Replay Attacks, Keyloggers.**

1. Introduction

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.

One Time passwords can be Time Based or Event Based. The Time Based OTP is valid for a particular time stamp and it gets expired if not used within that particular time stamp. This can be beneficial to prevent delayed messages from being accepted. The Event Based OTP is generated whenever it is requested and it is not changed within a time. It is valid until it is used and requested for next generation. The OTP can be delivered to clients using many ways like Text Messages, Mobile Phones and Proprietary Tokens, E-mails etc. The client has to read the OTP and submit it for successful login. The additional security layer will be added to the authentication process with the use of One Time password. The One Time Passwords used for authentication process can be represented using text or graphics. Both the authentication processes are knowledge based. The text based authentication is widely used because they are easy to deliver, implement and deploy whereas the graphic based (visual passwords) are difficult to deploy and are made of complex components. They both suffer from problems like password remembrance, illegal coping strategies, etc. Now the basic difference between text based password and visual password which we are using is the readable part. During the delivery time, text based one time password will be readable by intruder or machines unless it is in encrypted form. But the visual one time password is difficult to be recognized by machines.

Authentication process suffers from a lot of attacks like Man-In-Middle, Eavesdropper, keylogger attacks, customer fraud detection, phishing attacks, password cracking, Shoulder surfing, replay attacks and session hijacking attacks. Now these attacks can be done by humans or machines like bots/autobots.

We are here more concerned about bots/autobots. Bots or Autobots are also malicious software which are installed and run on users system without their consent. They may be installed through viruses, trojan horse and worms. The network of a number of bots is called botnet. The architecture of botnet can be Command& Control or Peer To Peer. The bots can harm the user's system by password cracking, keylogging, distributed denial of service and web or email spamming.

In this paper we concentrate on protecting our authentication process from autobots using visual one time password. The drawback of autobot machines is that they cannot read images. So we will be using graphics based one time password during authentication process.

2. Literature Review

R.R.Karthiga et al. he proposed a OTP survey and find that to reduce the damage of phishing and spyware attacks, 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. Ahmad Alamgir Khan et al. discussed the problem of phishing attack in which cyber criminals steal personal and financial data. 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 and the server will create a encrypted token for users device. The one time password and encrypted token is a smart way to tackle this problem. Andrew Y. Lindell et al compare the two main approaches of one-time passwords (OTP): time-based OTP and event-based OTP. It gives the usability and security comparison of both the OTPs. Both approaches use cryptographic mechanism. Mihai Ordean et al. provide the analysis of security and usability of authentication systems based on components. It introduces the one-time visual authentication (OTVP) concept which represents a novel approach to the security of authentication interfaces that combines one-time passwords (OTPs) with visual authentication interfaces.

3. Problem Formulation

In normal OTP based web portals, the one-time password is sent to user's phone as an SMS. After that, user enter and submit the code, which is later verified and authentication is granted if found correct. Usually this type of authentication is used by some web portals for the integrity of real user and to prevent the auto-bots created by hackers, while signing up. In this era of smart phones this technology is not fool proof. Hacker can attach his smart phone with his computer and can generate an automatic application to read the OTP from SMS and to fill it in the required field on web portal to gain access. Using this method a hacker can create several IDs (can be millions), which can be either used for spamming or various DDoS attacks or other similar attacks. Henceforth, this becomes need of the hour to develop an auto-bot proof method to prevent such attacks.

3. Proposed System

In this research, we proposed a novel OTP algorithm using auto-bots proof Graphical password representation on smart phone devices. In this research project, an OTP will be generated on the server side using mathematical random function. Then, this OTP will be converted to image from text using Graphical Representation Method. This image based OTP will be sent to the client/user's smart phone, which will not be readable by auto-bot techniques, hence cannot be auto filled to gain the access of web portal. The delivery of graphical OTP from server to user's smart phone scan be made using MMS or Whatsapp.

Algorithm 1: Proposed Algorithm Flow

Step 1: Sphere Random Function to generate random number

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

Step 2: Visual encoding

1. Convert number or string to ASCII-number array
2. Find the correspondent pre-defined ASCII number graphical encoding for **i***th* array value.
3. Repeat B on all array values
4. Concatenate the visual encoding of all characters to form an image
5. Return Visual OTP

Step 3: Client/Server Communication

1. Server forwards the generated visual OTP to client/user via SMS/MMS/Other-App.
2. Client/User submits the OTP on web portal, wherever it is required or requested.
3. Server receives the reply as OTP submitted by client/user
4. Server verifies the OTP reply.
5. Returns the decision logic

4. Methodology

At first stage, a detailed literature study would be conducted on the existing one time password methods and algorithms. Literature study will lead us towards refining the structure of the proposed OTP algorithm. The literature for one time password methods would be studied and different aspects would be learnt from the perspective of security and attacks. Afterwards, the proposed algorithm will be implemented in the MATLAB and a thorough performance analysis would be performed. Obtained results would be analyzed and compared with the existing techniques.

5. Need and Scope

One time password scheme with visual encoding is used as a authentication technique to prevent the unnatural access of the internet or intranet applications. One time password scheme is used to identify the human as a user. This scheme will be used to prevent the automatic task driven botnets/autobots. The proposed spherical random function with visual encoding based one time password scheme will be used to produce the visual password by converting a randomly generated password into image using a unique function. This scheme is adaptable in all of the mobile OTP or SMS OTP based internet or intranet applications, where ever is the requirement to protect against autobots/botnets.

6. Conclusion and Future Work

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.

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] Bin Li, Shaohai Hu, Yunyan Liu, 2006."A Practical One-Time Password Authentication Implement on Internet", ICWMMN Proceedings.

[7] Jivika Govil, 2007. "Examining the Criminology of Bot Zoo", IEEE.

[8] Mihai Ordean, 2012. "Secure Authentication Using One Time Visual Password", Ph.D. Dissertation, The technical university of Cluj-Napoca.

[9] 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

[10] 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.

[11] Takasuke TSUJI, 2003. "A One-Time Password Authentication Method", Kochi University of Technology.

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