IJCSE International Journal of Computer Sciences and Engineering Open Access
Technical Paper Volume-4, Issue-5 E-ISSN: 2347-2693

A New Technique For User Authentication Using Numeric One Time Password Scheme

Salim Istyaq*
Computer Engineering, University Polytechnic, Faculty of Engineering & Technology,
A.M.U. Aligarh-202002, UP, India

Lovish Agrawal
Computer Engineering, University Polytechnic, Faculty of Engineering & Technology,
A.M.U. Aligarh-202002, UP, India

Available online at: www.ijcseonline.org

Received: Apr/21/2016 Revised: May/04/2016 Accepted: May/18/2016 Published: May/31/2016

Abstract—*The text-based password has been the default security medium for years. However, the difficulty of memorizing secure strong passwords often leads to insecure practices. In this fast computer era, the Internet users are increasing on each second. Now mostly people are using different online service provided by Banks, Schools, Hospitals, online utility bill payment and online shopping sites. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. For example, if the user is not intelligently constructed the password with extra security measures, it is very easy for hacker to hack. On the contrary, if a password is hard to guess, then it is often hard to remember. A person has to memorize as many passwords as many different websites he/she is using. So he/she gets confused and/or forgets the correct user Id/password combinations. We should have an alternative system to overcome these problems. In this paper, a comprehensive study of existing graphical password scheme and shoulder surfing problem is performed. The best way in One Time Password authentication is proposed for enhancement in security and privacy.*

Keywords— One Time Password (OTP), Authentication, Usability, Security, Shoulder Surfing.

I. INTRODUCTION

Due to the increased use of different services online, there is need to develop a secure system is very important. The system should be able to authenticate right user and provide the online transactions in terms of high privacy and security [1]. Now days, number of user authentication schemes are available. But out of those entire how many are truly secure us? To answer it lets goes through the background of text-based and OTP passwords. The most common computer authentication method is for a user which submits a user name and text password. The vulnerabilities of text-based method have been well known to us. One of which main problem is the difficulty to remember passwords. Studies have shown that users tend to use small size password or passwords that are easy for remembering [2]. Unfortunately, these passwords were easily guessed or broken. The graphical passwords scheme act as a possible alternative to text-based schemes, which are proposed mainly by the fact that humans can remember pictures better than text [3].

II. METHODS OF AUTHENTICATION

The methods of authentications are following [4]:

- Token Based Authentication
- Biometric Based Authentication
- Knowledge Based Authentication

Token-based techniques, such as smart cards, key cards and bank cards are widely used. Many token-based authentication systems also use techniques based on knowledge to improve security. For example, ATM cards are normally used in combination with a PIN.

Biometric based authentication techniques, such as iris scans, fingerprints, or facial recognition has been developed due to biometrics' uniqueness properties [5]. These systems are very secure. The major drawback of biometric based approach is that these systems are expensive, and the identification process will be slow and often unreliable.

Knowledge based techniques are most widely used technique of authentication and include both text-based and picture-based passwords. The picture-based techniques are further sub divided into two categories: recall-based graphical and recognition-based techniques. In recognition techniques, user is presented with a collection of images and the user passes the authentication if he or she identifies the correct images that he or she selected earlier during the registration phase. Using recall-based techniques, a user is needed to reproduce something that he or she created or selected during the registration phase.

III. TOLERABLE ATTACK ON TEXT BASED PASSWORD AND GRAPHICAL PASSWORD TECHNIQUES

A. *Brute Force Attack*

It is generally difficult to protect against brute force attack. Hence, brute force attack attempts on a huge number of key combinations on trial-and-error basis [6]. To protect from Brute Force Attack there is sufficiently large password space. There is 94N password space for text-based passwords where N is length of password, 94 is the number of printable characters excluding SPACE [7]. In graphical password's technique password space is similar to or bigger than that of text based passwords. It is seen that for recognition based graphical password has smaller password spaces then the recall based methods. It is difficult to carry brute force attack against graphical password than text-based password. To reproduce human input it is required to automatically generate accurate mouse movement which is more difficult as in case of recall based graphical passwords.

B. *Dictionary Attacks*

It is necessary that recognition based graphical passwords involve mouse as input instead of keyboard input; it will be impractical to carry out dictionary attacks against this type of graphical passwords. It is possible to use a dictionary attack but an automated dictionary attack will be much harder than a text based dictionary attack for some recall-based graphical passwords. Overall, graphical passwords are more vulnerable to text-based passwords than dictionary attacks.

C. *Guessing*

Many users tend to use their passwords based on their personal information like the name of their house, pet names, phone number, passport number etc. In these cases, the attacker tries to guess the password by trying the main password possibilities based on the user's personal information [8]. As problem occur in the case of text based password guessing same problem occur in the case of graphical password. For example, on studying Pass Face technique it is seen that people often choose weak and predictable password. Similar predictability is found among graphical passwords created using DAS technique.

D. *Spyware Attack*

Ignoring few exceptions, key logging or key listening spyware cannot be use to break graphical based passwords. It is not clear that whether "mouse tracking" is act as effective tool against graphical passwords or not. It is seen that mouse motion is not enough to break graphical passwords. Such information has to be clearly connected with application information, such as size and position of window, and as well as time information.

E. *Social Engineering*

To tell graphical passwords to another person is difficult as compared to text-based password. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

F. *Shoulder Surfing*

Drawback of graphical password scheme is that when user input their password in public place then there may be chance that some other person who stands near to user can capture their password either by simply observation or by recording user's authentication session. This whole is known as shoulder surfing and also a serious problem when user type their password in public place. This problem of shoulder surfing may not occur when password is type of alphanumeric text.

IV. FLOW-CHART

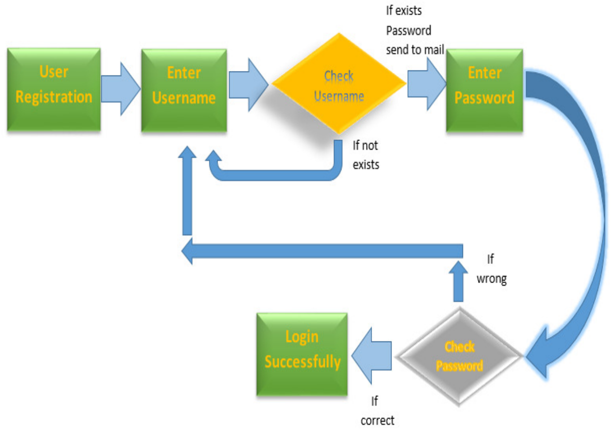

Figure 1. Flowchart of our Proposed Scheme

V. PROPOSED ALGORITHM

- Start.
- User can register by Username and Email Id.
- **Authentication of User:**

User will enter Username which he entered at time of registration.

a) *If Username exists.*

Computer program send mail to his Email Id which is entered during registration. The mail contains OTP.

b) *If not exists.*

User can enter Username Again.

- User enters the OTP send on his Email Id.

a) *If Password is correct.*

User can access his Account.

b) *If Password is wrong.*

User can Login Again.

- Stop.

VI. ANALSIS AND RESULT

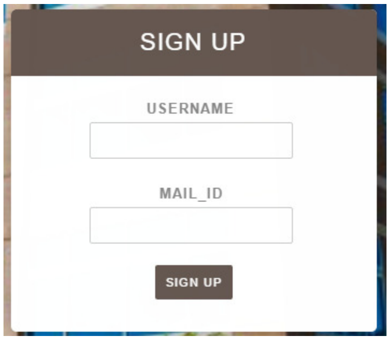

Figure 2. Registration Form of Our Scheme

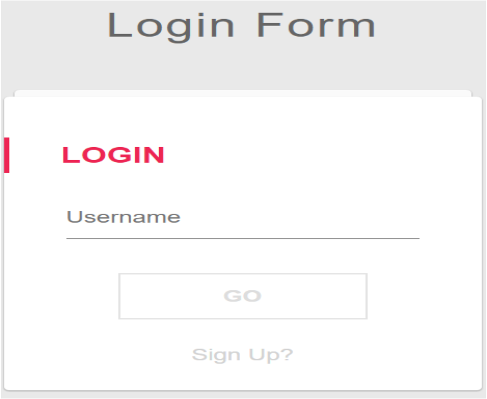

Figure 3. User Name Entering Page of our Scheme

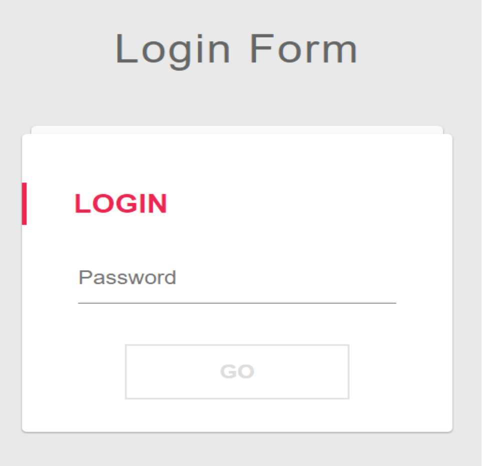

Figure 4. Password Entering Page when user enters Correct User Name

VII. CONCLUSION

One-time password systems are already being widely deployed by banks, governments, and corporate virtual private networks (VPNs) to reduce the effects of password compromise. In this paper, we have proposed to new idea to enhancing the performance of OTP to provide authentication for system. OTP is send to user email id and user can login through this OTP only. We have described a system that allows users one-time password access to accounts. The method is entirely general and can be applied to almost any login server. As there is no additional secrets to remember or tokens for the user to carry. Every OTP is readable without ambiguity no matter what display or font is used, each time it gets changed. In this paper One Time Password (OTP) based login system is designed and explained to avoid shoulder surfing in combination of text/graphical password authentication scheme.

REFERENCES

[1] http://rroij.com/open-access/an-approach-for-user-authentication-one-time-password-numeric-and-graphical-scheme-54-57.php?aid=37786

[2] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures", Communications of the ACM, Volume-**42**, Page No (**41-46**), **1999**.

[3] Pavan Gujjar Panduranga Rao, Dr.G. Lavanya Devi and Dr.P.Srinivasa Rao, "A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach" , Volume-**10**, Issue-**6**, Page No (**6**), May-Jun **2013**.

[4] Brajesh Kumar Kushwaha, "AN APPROACH FOR USER AUTHENTICATION ONE TIME PASSWORD (NUMERIC AND GRAPHICAL) SCHEME", Journal of Global Research in Computer Science, Volume-**3**, Page No (**1**), Nov **11, 2012.**

[5] Mohite Sandhya, Kare Rohini, Bhongale Pooja, Bhosale Priyanka, "Graphical Password Authentication using Modified Persuasive Cued Click-Point", International Journal of Computer Science Engineering (IJCSE), Volume-**2,** Page No (**2**), Mar 2, **2015.**

[6] Jesudoss A., Subramaniam N.P., "A SURVEY ON AUTHENTICATION ATTACKS AND COUNTERMEASURES IN A DISTRIBUTED ENVIRONMENT", Indian Journal of Computer Science and Engineering (IJCSE), Volume-**5,** No.-**2,** April-May **2014.**

[7] http://www.bioinfo.in/uploadfiles/13476885341_1_2_WRJHCI.pdf

[8] Saranya Ramanan and Bindhu J S, "A Survey on Different Graphical Password Authentication Techniques", Volume-**2**, Page No (**7**), Dec **12**, **2014**.

AUTHORS PROFILE

Salim Istyaq is an Assistant Professor in Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, A.M.U., Aligarh-202002, U.P.-India since 2004. Earlier, worked as Guest Faculty in ECE Department, Jamia Millia Islamia, New Delhi-110025. Also worked in Computer Engineering, Al-Mergheb University, Alkhoms, Libya. So far published 03 Papers in International Journals and 02 in IEEE Conferences. Review Committee Member in Editorial Board of various International Journals.

Lovish Agrawal is a Scholar of VI Semester Diploma in Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, A.M.U., Aligarh-202002, U.P.-India.