Two-Way Authentication System

Chaitanya Harde[1], Monika Bhatt[2], Mohit Anand[3], Dnyanada Hire[4]

Department of Electronics and Telecommunication, Dr. D. Y. Patil Institute of Engineering Management and Research Akurdi, Maharashtra, Pune, India
[1]chaitanyaharde@gmail.com
[2]monikabhat57@gmail.com
[3]mohitanand.adp@gmail.com
[4]dnyanadahire@gmail.com

Abstract

All need to use stronger passwords which should not include our names, sequential number and birthdates even if these are easy to remember. But strong passwords are hard to remember so, the solution is Two-Factor Authentication (2FA). Two-factor authentication, also called multiple-factor or multiple-step verification, is an authentication mechanism to double check that your identity is legitimate, and this does not require transferring data over the internet. The two-factor authentication security feature has the following advantages: Enhanced security, helps in fraud prevention, Easy for users to understand and enable, Easier and quick account recovery.

Keywords*—Authentication; graphical passwords; Persuasive Cued Click Point (PCCP)*

I. INTRODUCTION

With so much of our lives happening on mobile devices and laptops, it's no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. And there are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down. And as cybercrime gets more sophisticated, companies find their old security systems are no match for modern threats and attacks. Sometimes it's simple human error that has left them exposed. All types of organizations—global companies, small businesses, start-ups, and even non-profits—can suffer severe financial and reputational loss. Password theft is constantly evolving as hackers employ methods like keylogging, phishing, and pharming. Cyber criminals do more than merely steal data. Often, they destroy data, change programs or services, or use servers to transmit propaganda, spam, or malicious code. Two-way authentication is not important, its critical to protecting your critical assets. Passwords are regularly shared or stolen through phishing or simple guessed based attacks. Users are less and less cautious with the use of their password and more importantly completely unaware of the leaking of their digital identities in the dark web. As per the study results of the human psychology, the human brain is very efficient to remember the graphical passwords than of the text-based passwords. Also, the graphical passwords are recognizable to the user.

II. IDENTIFIEDPROBLEM

As we see the most adaptable password technique is the text-based password. Most of the system is using the text-based password. But the text-based password has the disadvantage such as,

- Easy to break

- Vulnerable to attacks

Because of this reason such system is not secure as they have. To overcome this problem, we have selected the cued click password scheme.

III. PURPOSE ANDSCOPE

Click cued points is a click-based graphical password scheme, a cued-recall graphical password technique. Various graphical password schemes have been proposed as alternatives to text-based passwords. It can be used as password for folder lock, web-driven applications, desktop lock etc. In future it has great scope. It can be used everywhere instead of text-based password. We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used.

IV. METHOD

The main objective of the project is to provide a two-way authentication scheme to the users by using Persuasive Cued Clicked point's technique and 5-bit OTP generation on user's registered device as input for each point. The two-way authentication needs to be developed for the users by using Persuasive Cued Clicked points technique and OTP which can be effectively used for any system for secure login but difficult to be guessed by attacker.

Our system provides a two-way authentication to the users by using Persuasive Cued Clicked points technique and OTP. The user has to register him by entering his user's name, mobile number and email-id. Then will have to select the five images with which user wants to generate the password by clicking one point on each image. After the five clicks unique password is generated and the registration process is completed.

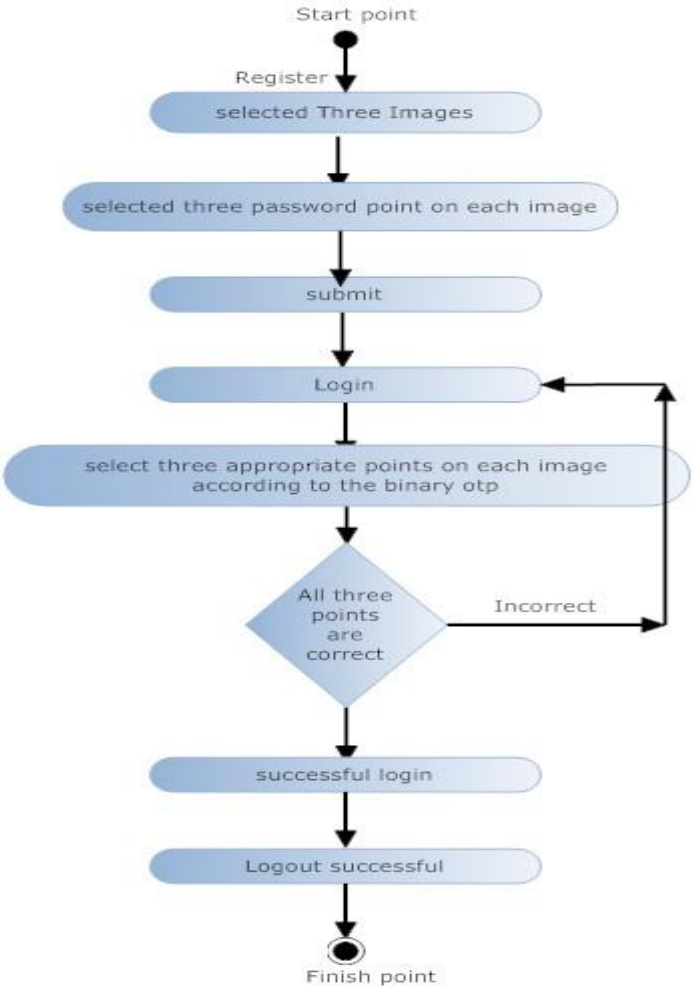
Start point
Register
selected Three Images
selected three password point on each image
submit
Login
select three appropriate points on each image according to the binary otp
All three points are correct
Incorrect
successful login
Logout successful
Finish point

Fig. 1 Flowchart

Now every time the user wants to login will have to enter the username and select the continue button. Fig.1 shows the flow chart of the process After user selects login; user will receive the OTP containing 5-bit binary code on his mobile. Now user want to select the same points which he had selected at the time of registration for the images when the bit in the OTP is 1 and select any other point except the point select while registration for the image when the bit in the OTP is 0. Only if the user has followed this process correctly, he/she will get the access to the system using login.

VI. RESULT

The system is designed in such a way thatthe Improved Authentication Scheme Using Persuasive Cued Click Points system is very efficient to use. This system founds very secure and flexible to use. This system allows very attractive GUI to user so user finds very attractive and convenient to use this type of password.

VII. SOFTWARE INTERFACE

In fig 2. Interface of Software is shown the software should be developed according to the system. The user interface module should be developed in such a way that the user can easily operate the system. The software is designed in .NET Framework,programming. C# is a programming language designed for building a wide range of enterprise applications that run on the .NET Framework, and the database used is RDBMS in Microsoft SQL server. The Hardware Requirements would be 1 GB RAM, 200GB HDD and Intel 1.66 GHz Processor Pentium 4 and Windows XP, 7,8,10 CPU.

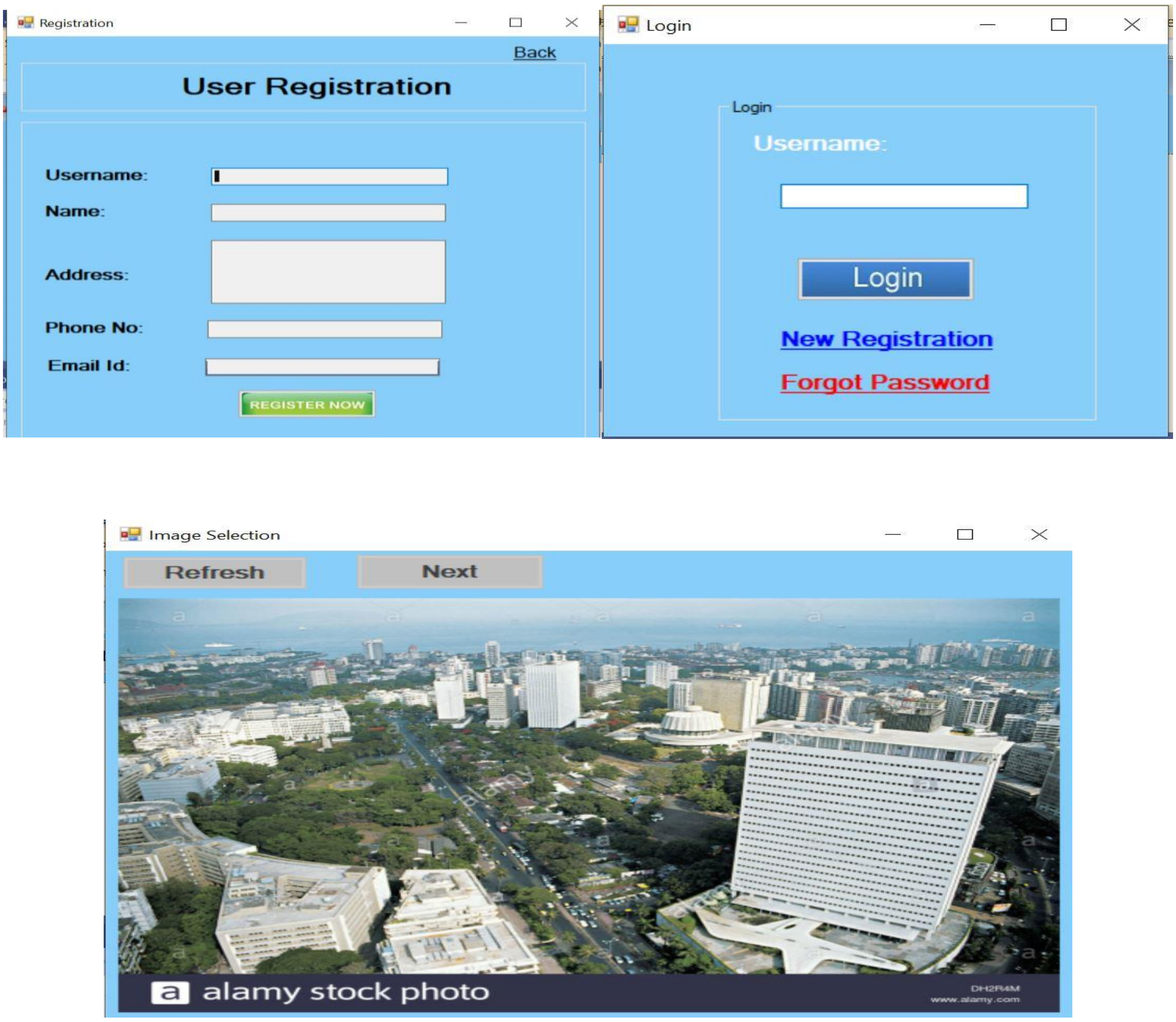

Fig. 2 software interface

VIII. CONCLUSION

Theproposed Cued Click Points (CCP) scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages overpass Points in terms of usability. Being cued as each image shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image.CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy Mag., vol. 1, no. 2, pp. 33–42, 2003

[2] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

[3] M .Swathi, M. V. Jagannatha Reddy, Authentication Using Persuasive Cued Click Points International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July - 2013 IJERT ISSN: 2278-0181

[4] Sonia Chiasson,Member, IEEE, Elizabeth Stobert,Alain Forget, RobertBiddle,Member, IEEE, and P.C. vanOorschot,Member, IEEE "Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, volume 03-No.3.Issue 01 March 2012

[5] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007

[6] Fatehah M.D., MohdZalishamJali&Wafa M.K., Nor BadrulAnuar, "Educating Users to Generate Secure Graphical Password Secrets: An Initial Study" 2013, IEEE

[7] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, NorafidaIthnin, Hazinah K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", 2008, IEEE.

[8] Smita Chaturvedi, Rekha Sharma, "Securing text & image password using the combinations of Persuasive Cued Click Points with the help of Improved Advanced Encryption Standard, International Conference on Advanced Computing Technologies and Applications(ICACTA-2015)

[9] Madhuri Achmani , Radhika Dehaley , AnujaGaonkar , AninditaKhad, Two Level Authentication System Based on Pair Based Authentication and Image Selection, IJRASET Volume 4 Issue IV, April 2016 ISSN: 2321-9653

[10] N. S. Joshi,"Session Passwords Using Grids and Colors for Web Applications and PDA" in International Journal of Emerging Technology and Advanced Engineering

[11] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[12] MohdSarosh Umar and MohdQasim Rafiq, "A Graphical Interface for User Authentication on

Mobile Phones", in ACHI 2011: The Fourth International Conference on Advances in Computer-Human Interactions, Guadeloupe, France, February 23-28, 2011