ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (27-32), Month: April 2015 – September 2015, Available at: www.paperpublications.org

Smart Password

Mr. Sandeep Agarwalla[1], Ms Priyanka Roy[2]

[1]Faculty [Dept. of Computer Science], Indian Institute of Management & Commerce, Khairatabad, Hyderabad, India
[2]Lecturer at Computer Science Dept. Aurora PG College, Ramanthapur, Hyderabad, India

Abstract: **Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. Every user now holds email account for different web sites or holds a username password for their office work in their computer system. In this paper, we shall present the result of our survey through basic currently available password-authentication-related schemes. We know that Apart from getting the password hacked by some intruder, a serious threats comes from the surrounding environment, specially the colleagues, friends or visitors nearby the system. Most of them have a tendency of observing keenly while you cast your password. Here we propose a simple way to provide a new way of password through clicks that would provide a secure mechanism from both the intruders and the people nearby while you type your password in the application.**

Keywords**: Smart Password, Secure, Login, Authentication, Encryption, intruder.**

I. INTRODUCTION

Today there is an increasing recognition that security issues are also fundamentally human computer interaction issues. A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource. It is a critical area of security research and practice. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, bio-metric password or retina scan are possible alternatives. This paper reports on research aimed to design a new kind of password system, empirically test its usability and also done economically, and compares it to traditional passwords. The significance of this research is the provision of a flexible password system with extensive human factors data to support it.

The problem arises because passwords should be secure, not only from the intruders or hackers but also from the people who surrounds you while you cast your password. So it must be given in such a way so that it should be secure, i.e., they should look random and should be hard to guess. It should not be understood or cracked even by person(s) keenly watching the password being typed by another user/person. Neither it is easy for a hacker to get to know about the user's password by injecting malicious programs.

II. OBJECTIVES & METHODOLOGY

1. Provide a highly secured authentication for users.
2. Left/Right mouse clicks of password leads to confusion for people nearby the user clicking the password.
3. Dual Encryption secures the password string from getting hacked.

Methodology:

The present study focuses on the secondary sources of data from Books, Journals, Articles, and interviews with eminent personalities from various departments of the University.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (27-32), Month: April 2015 – September 2015, Available at: www.paperpublications.org

Problems with the existing way of giving username and password:

The username and password based login systems is most widely used authenticating system. The password is a secret word or string of characters that is used for user authentication to prove his identity and gain access to the resource(s). Access to computer systems/Applications is most often based on the use of alphanumeric passwords. Users normally create short, simple, and insecure passwords.Though user thinks that he/she has given a strong password for intruder to detect but due to carelessness often the security is lost when the password is given in front of someone unknown or in front of a user/device that is keen to know the password. All valuable information will be lost when such authentication is lost.

Figure: Users keen in watching the password being typed by a user

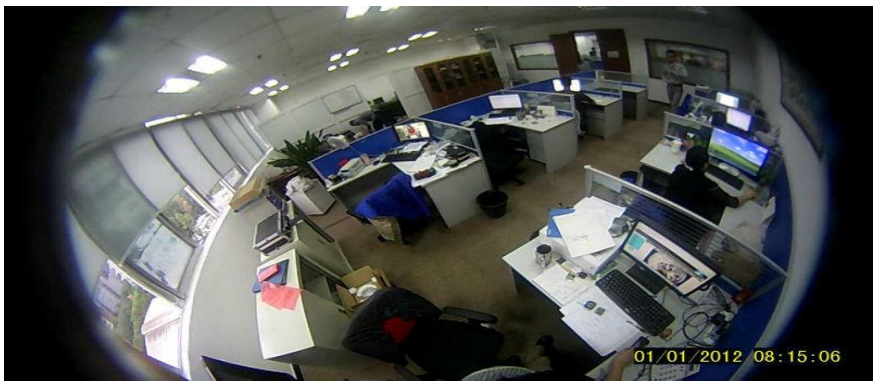


Figure: How Web cam (device) can be used to know the password being typed by a user

The Login screen used for giving username password for most of the applications used worldwide.

Figure: Login Screen for existing way of giving password

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (27-32), Month: April 2015 – September 2015, Available at: www.paperpublications.org

III. SMART PASSWORD (Proposed way of giving username and password)

The proposed way would be using of mouse clicks in addition to the password given for a user. During any login registration process, an additional dialup box will open only for registering the password. Here the user needs to give the user name and the corresponding password is selected from the drop down list. Additionally the user needs to select the left and right option from the drop down menu presented beside each of the letters selected for password. The same left/right key combination will used during login when password is given. The figure below shows the sample how exactly the registration process will be done.

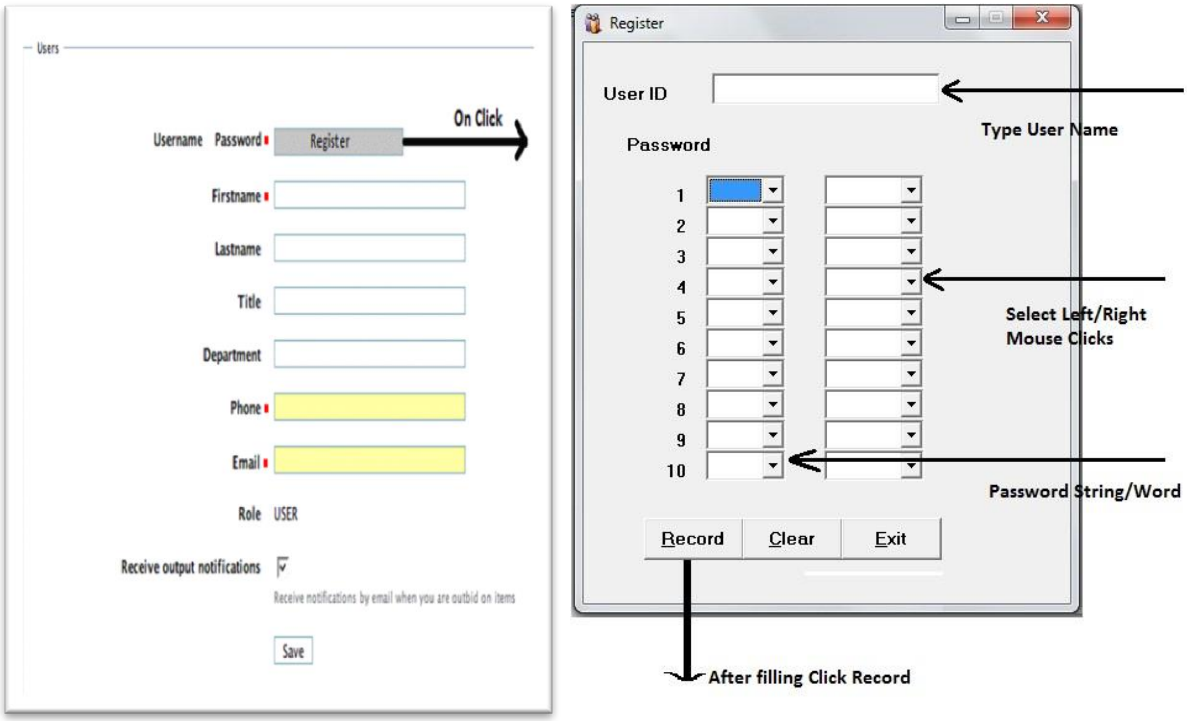


Figure: User registration process for SMART PASSWORD

Sample Registration form for *SMART PASSWORD:*

The sample figure shows how exactly the registration process for username and password will work. First the username is to be given as usual, and then the password *"milku24"* is selected from the drop down menu which the user wants to give for the username. The mouse combination is selected for each character of the password as shown.

m→**left mouse button** to click from virtual keyboard during login.

i→ **left mouse button** to click from virtual keyboard during login.

l→**Right mouse button** to click from virtual keyboard during login.

k →**left mouse button** to click from virtual keyboard during login.

u→ **Right mouse button** to click from virtual keyboard during login.

2 →**Right mouse button** to click from virtual keyboard during login.

4 →**Right mouse button** to click from virtual keyboard during login.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (27-32), Month: April 2015 – September 2015, Available at: www.paperpublications.org

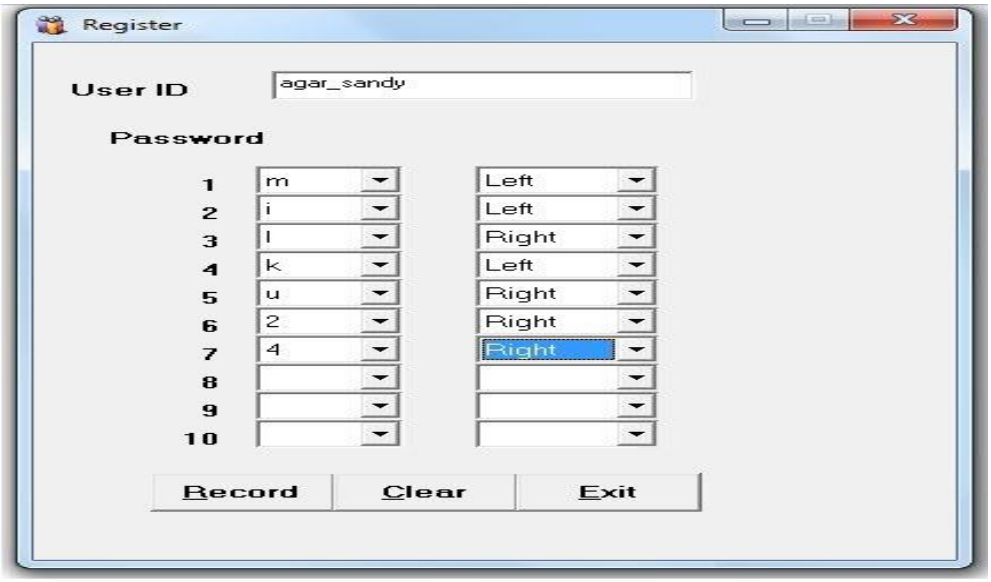


Figure: Sample Register SMART PASSWORD

Login form for *SMART PASSWORD:*

The user will enter the username and the password which is given should be clicked withthe mouse,using the virtual keyboard displayed. Correct combination of mouse clicks must be used for the password as it has been set while registering it with the left/right combination of mouse click.

Hence it is safe from the people/device around to track the password as the combination will be greater than hundred which is difficult to crack for normal user.

Further we will discuss how the password is dually encrypted for the intruder / hacker to crack the password.

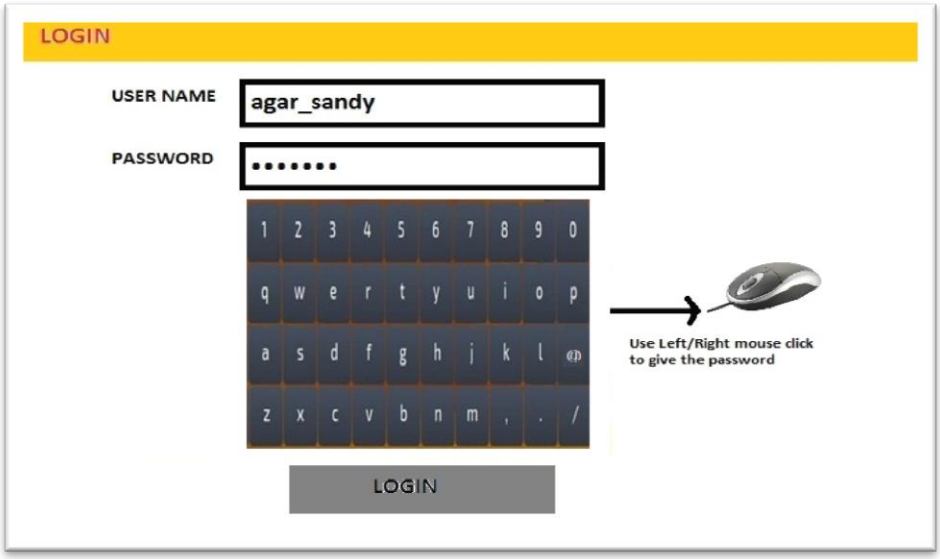


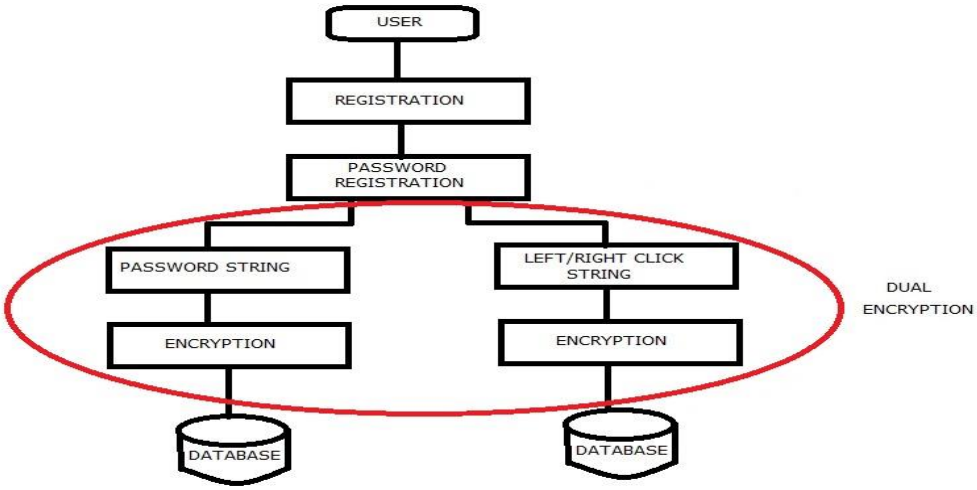
Figure: SMART PASSWORD LOGIN SCREEN

Dual Encrypted Password Protection:

Even If an intruder/Hacker uses his/her skills to crack the password, the hacker would concentrate more on the password string and the encryption associated with it. Hacker will not think of mouse click combination; even if he/she does, it would be very difficult to crack.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (27-32), Month: April 2015 – September 2015, Available at: www.paperpublications.org



IV. EXPERIMENTAL RESULTS

Data collected from 15 participants. Each one was asked to login himself/herself with 5 times trail allowing them to view the username and password while I logged in. Participants are mainly Graduate and Post Graduate students of age group 20-28 Y. Few were allowed to use in campus high CCTV Surveillance Camera to watch the username and password and crack it. However none succeeded. The following table shows ***smart password*** is a Good Tool for Login.

Table 1: Attempts by Participants (5 attempts each)

Sl No.	Username	Login Trails	Times Accepted	Times Rejected
1	agar_sandy	5	0	5
2	agar_sandy	5	0	5
3	agar_sandy	5	0	5
4	agar_sandy	5	0	5
5	agar_sandy	5	0	5
6	agar_sandy	5	0	5
7	agar_sandy	5	0	5
8	agar_sandy	5	0	5
9	agar_sandy	5	0	5
10	agar_sandy	5	0	5
11	agar_sandy	5	0	5
12	agar_sandy	5	0	5
13	agar_sandy	5	0	5
14	agar_sandy	5	0	5
15	agar_sandy	5	0	5

V. CONCLUSION

We have proposed a novel approach which uses clicks to give password for a user. No previously developed system used this approach this system ishelpful when user is logging in any application or email account; no person sitting around/ web cameras can be able to trace the password given during login. Not only from general people around the password is protected but also protected from intruders/hackers who can break through encrypted password stored in database. Hope, future application developments would use the smart password tool for more secure Login.

REFERENCES

[1] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. ASecond Look at the Usability of Click-based GraphicalPasswords. ACM SOUPS, 2007.

[2] Sood S., "An Improved and Secure Smart CardBased Dynamic Identity Authentication Protocol",International Journal of Network Security, Volume14, Number 1, pp. 39-46, 2012.

[3] Li, C. Lee C., Wang L., "A Two-Factor UserAuthentication Scheme Providing MutualAuthentication and Key Agreement over InsecureChannels", Journal of Information Assurance andSecurity 5, pp. 201-208, 2010.

[4] Hsiang H., and. Shih W., "Improvement of theSecure Dynamic ID Based Remote UserAuthentication Scheme for Multi-serverEnvironment", Computer Standards & Interfaces,Volume 31, pp. 1118-1123, 2009.

[5] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remoteuser authentication schemes," Computers & Security, vol. 24, pp. 50–56, 2005.

[6] R.M.Needham and M. D. Schroeder. Using encryption for authentication in large networksof computers. Communications of the Association for Computing Machinery, 21(21):993–999, Dec. 1978.

[7] Chien H., Jan J., Tseng Y., "An Efficient andPractical Solution to Remote Authentication: Smartcard", Computers & Security 21, pp. 372–375, 2002.

[8] Altinkemer K. and Wang T., "Cost and BenefitAnalysis of Authentication Systems," DecisionSupport Systems, vol. 51, pp. 394-404, 2011.

[9] Choo K.., McCullaghBarreto, "Two-Party Id-basedAuthenticated Key Agreement Protocols", InternetJournal of Network Security, 1 (3), pp. 154–160, 2005.