Advance Secure Login

Zaid Imran and Rafay Nizami

Department of Information Technology, SRM University, India
zaid_imran999@hotmail.com

Abstract- Advance secure login is an advance technique used as a counter measure for the shoulder surfing attack. Shoulder surfing is an observation technique of stealing the information by looking over someone's shoulder. Very often people are unaware of the presence of any external devices like the close circuit cameras and hidden surveillance equipment which are placed to capture their valuable information like the password etc. It is very easy to stand close to someone and look what the other person is typing on the keyboard. Advance Secure login technique could be used in computers where confidential data are used, in highly secured nuclear servers authentication, ATM machines, Email login etc. The Secure Login will also consist of a RSA or MD5 encryption technique to protect the password. This counter measure helps in protecting the password from being stolen even if the password is typed in front of others. Advance secure login is an revised and advance technique of our previous research work (Secure Login) in a more easier and simple way. The mathematical and performance analysis of the software is also represented.

Index Terms- authentication, advance secure login, shoulder surfing, RSA and MD5

I. Introduction

Identity theft is closely associated with the Shoulder Surfing. This can result in fraud activities like stealing money from some ones account, leaking of the confidential data etc. The person whose identity is used often faces various consequences when held responsible for the anti social actions. The people who are truly concerned about their identity should certainly make themselves familiar with Shoulder Surfing. In reality, this terminology is used to describe one of the many ways by which criminals obtain the personal information of the people to commit identity theft. This paper provides a highly secure password entry solution which is resistant to Shoulder Surfing. In the first section of the paper we provide a brief description about the concept of Shoulder Surfing along with few tips to reduce Shoulder Surfing which can be implemented by a casual user. Second section covers some of the related research works that have already been done in the area of Shoulder Surfing.

.

Then we throw lights on the solution provided by us as a counter measure. The solution developed by us employs an encryption feature which is useful in preventing other forms of attack other than Shoulder Surfing. The mathematical and experimental performance is shown in section 4. In section 5 we show the simulation of the developed software and then list utilities & certain constraints associated with it in subsequent sections.

II. Detailed Study and Analysis

A. What is shoulder surfing?

Shoulder Surfing is a direct observation technique, such as, looking over someone's shoulder, to get the information. Shoulder Surfing is an effective way of getting the information whether it is in a user's home while he works on his Personal computer or a public places .Shoulder Surfing can also be done by the long distance advance surveillance devices. The increase in number of laptop and personal digital assistant (PDA) usage has greatly increased the danger of unauthorized observation of authentication procedures. The users have become more prone to password theft due to such kind of sneaking. One should remain cautious of his/her surroundings especially when he/she is authenticating by the traditional authentication methods that are prone to Shoulder Surfing.

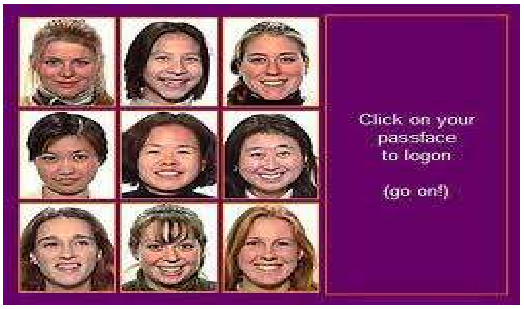
B. Reducing Shoulder Surfing attack

Shoulder Surfing may not be the most technical form of identity theft, but many have used this method to commit major fraud activities. There are certain precautions that may be taken by the users on a small scale while authenticating in any system ,that are presently not using any prevention techniques to control Shoulder Surfing. Shielding keypad from view by using body or cupping by hand while typing passwords – is obviously one such method but sounds a bit UNPROFESSIONAL. One should experiment and create the toughest password by mixing numbers, alphabets and special characters. One should always remember to dispose of the receipts carefully after completing an ATM transaction. It is not a direct solution to Shoulder Surfing, but doing so can be a bit handy when it comes to protecting customers from revealing their personal information.

C. Past Researches on Shoulder Surfing

In the past there had been many researches that deal with secure login authentication techniques that could avoid Shoulder Surfing but fully functional solution has not yet been invented. A very similar approach was design by divyans, samarpan etc in the 13th IASTED conference in USA. There also the positions of the password were input but that solution would fail if the display screen is a "touch screen" or if a "close circuit camera" is keying an eye on them as the user directly touches the password positions and this could be easily seen by anyone who records it secretly.

One such scheme proposed is that of a PASS FACES. It is a challenge response scheme. A user chooses a set of images as his password. During authentication the user needs to select the chosen images in the serial order of his selection. When one picture is selected a new set of images for subsequent selection appears. In this method a user can authenticate by going through several rounds of image selection (which is actually equivalent to the password length). This method is prone to Shoulder Surfing attack because one can easily view the position of the mouse cursor while authentication and the picture can be noted.



Click on your passface to logon

(go on!)

Figure 1: PASS FACES

A scheme similar to this has been proposed by S.Bindu. Here the Pass faces are arranged in a similar fashion and challenge response scheme is carried out. A user enters the coordinates of a particular Pass face rather than choosing it directly.
Similarly Wiedenbal describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks.

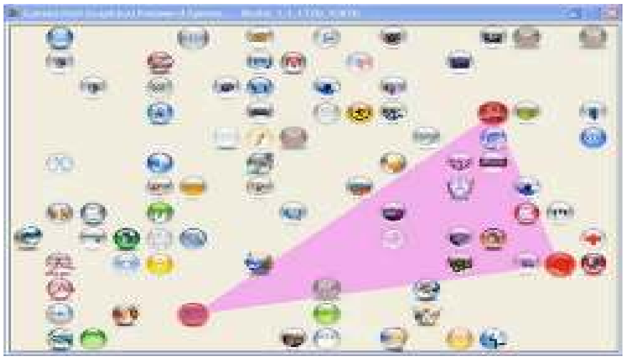


Figure 2: Example of a convex hull

A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

Even a research technique was invented by us by the name "SECURE LOGIN" which we will be representing in the ISAI 2011, Dubai. The approach to tackle the shoulder surfing is excellent but the technique is a little complicated and tough so we have worked hard and invented a new technique (Advance Secure Login) which is a new version of our last research work (SECURE LOGIN).

III. OUR TECHNIQUE

First of all the user creates an authentication account and the information regarding his/her username and password is saved in the DATABASE. For a strong password it is advisable that the password length should be between 7 to 20 characters. Most importantly, this database is hidden from the user and only accessible to the system ADMINISTRATOR of the particular system .Let us suppose that, at a later point of time, someone wants to logon to a system (here system need not be a standalone one, a user could perform remote login too) which contains the information about several users who have already registered and have the right to use the system. The incoming user will be asked to enter his authentication information, Username & Password as is usually done for a secured system. We have an "interactive screen" where, as usual, the username & password need to be entered. The username will be entered in the usual fashion as is done in most computer systems. But the trick lies while entering the password. The software uses an inbuilt technique to make the users enter their password. As the cursor is clicked on the password field a popup box appears. It contains a 7*7 "MATRIX". But only the Columns are numbered (1-7). The elements of the matrix will be a RANDOMLY generated set of alphabets, numerals and symbols "without" REPITITION of any alphabet, numerals or symbols in the matrix.

1	2	3	4	5	6
!	#	@	(	)	^
/	*	$	%	&	?
l	D	V	5	A	1
Q	4	C	Y	M	0
2	J	P	K	E	G
F	Z	3	B	L	S
U	W	6	T	X	9
R	8	N	7	H	O

Thus we include 12 special CHARACTERS in the first two rows followed by the APLHABETS and then the NUMBERS. The special characters are shuffled in the first two columns and are not mixed with the numbers or alphabets. While the numbers and alphabets are shuffled separately.

** Now here’s the trick. The user when asked for the “PASSOWRD” then he/she will type the “column position” of each password character. Now the major advantage is that even if the person would type the position of his password characters then too the person looking over his password would be confuse as there are 8 characters in each columns.

Let us take an example:-

Suppose the username is “UNIVERSITY” and the password is “M6D?9F&”.

For M the column number is “5”
For 6 the column number is “3”
For D the column number is “2”
For ? the column number is “6”
For 9 the column number is “6”
For F the column number is “1”
For & the column number is “5”

Thus while entering the password the user just has to enter the “5326615”.

** *Now in case if the same person comes a second time to login his username and password then first of all the matrix would be “shuffled” automatically and then positions of the characters would change.*

Now the same user comes to login the next time and let us consider that the matrix somewhat becomes like this:-

1	2	3	4	5	6
/	*	)	(	?	@
$	!	#	%	&	^
Z	A	Q	7	S	W
V	5	E	C	R	4
8	T	Y	H	N	U
J	M	P	I	O	L
F	K	3	D	1	2
9	B	X	0	6	G

For M the column number is “2”
For 6 the column number is “5”
For D the column number is “4”
For ? the column number is “5”
For 9 the column number is “1”
For F the column number is “1”
For & the column number is “5”

Thus in the password field the user inputs “2545115”

IV. Performance and Mathematical Analysis

We have assigned the password length as minimum of 7 characters and maximum of 20 characters.

Thus, total possible combinations of choosing a password of length ‘L’ is C = ((48) ^ L) : Where C is equal to the number of combinations & 7 <= L <= 20
Thus for password length equal to 7 characters we have total choice of ((48) ^ 7) = Approx. [(10^ 11)] ways & for password length equal to 20 characters we have total choice of [((48) ^ 20)]*4 = Approx. [(10^ 33)] ways.

Thus we can see that we have a wide range of combinations for selecting the password. Thus it will be very difficult for an unauthorized person to enter into a system by merely guessing a password of another user.

The elements in the first 2 rows can be arranged in the (12!) ways. The elements in the other 6 rows can be arranged in (36!) ways. Thus the entire matrix can be arranged in:

(12!) * (36!) ways = 10^50 ways approx.

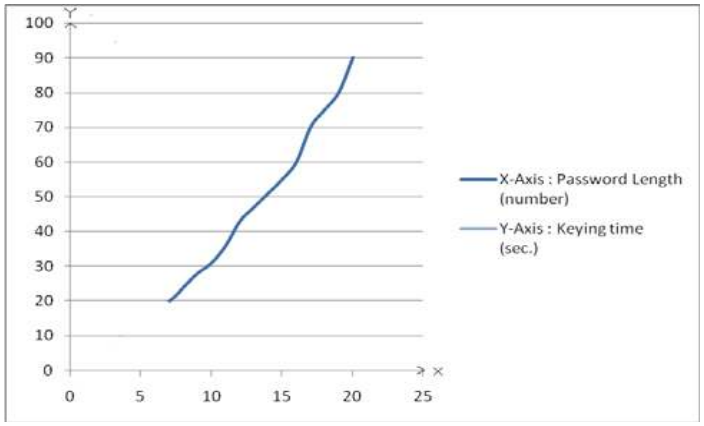
Cracking the password:-

Even if anyone sees the position of the column by the help of close circuit cameras, binoculars etc then:

Total number of columns = 6
Total number of characters in each column= 8

Number of possible guesses/tries an attacker has to perform = (8! * 6!) = 29030400

Which are a big number and not an easy task?



The graph shows that for tying a 7 length password it takes 20 sec while 14 length passwords can take up to 90 seconds. Such long passwords can be used in surveillance and military cases authentication.

V. Simulation

Step 1: A user starts the system to logon.

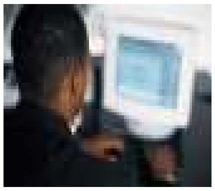


Figure 7: User Logon

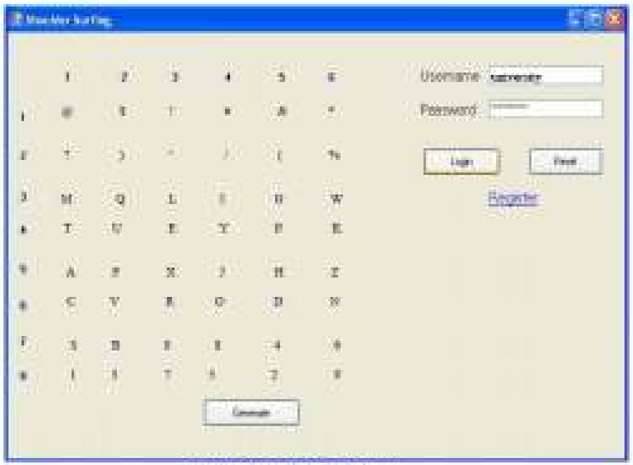


Figure 8. Authentication

The matrix appears on the screen somewhat in this fashion.

VI. Advantages of using our proposed technique

Suppose a sneaker tries to find out the authentication details of a user through Shoulder Surfing. If a system deploys our technique, then the sneaker's efforts would go in vain. A sneaker can either look onto the keyboard or look at the screen at a time. If he looks onto the keyboard then what he will get to see is a false authentication password of the user. Suppose the one who sees the password tries to keep the password in mind and waits for the user to leave the system and then reenters the positions entered by the user previously, again his effort will go in vain because after each login the positions of the elements in the matrix are dynamically shuffled. We can also avoid the loss of passwords which could have been obtained otherwise through the use of binoculars, closed circuit television cameras or other vision-enhancing devices that a shoulder attacker may use in order to trap a user. Yet another effective advantage of using it is that it involves figuring out positions. Unlike the previous techniques we are only using the "column positions" because even if the video recording is done secretly then too the attacker will have to guess between 8 characters in a single row. The most important thing is that after every login whenever the user come the matrix gets shuffled and after every 3 WRONG attempts the user account gets locked temporarily. We have implemented RSA encryption in the software. The encryption and decryption process is carried out automatically without the user's involvement. Thus sending of the password to a remote database to check for its correctness particularly in a networked environment will be secure from the sniffing attack. We have divided the matrix into three parts. The first two rows contain the special characters and the rest of the rows contains alphanumeric. This helps in figuring out the elements of the user's password in a quicker and easier way. From the discussions we can see that our proposed research work so could be a novel solution in controlling the Shoulder Surfing Attack.

References

[1] Secure login by "Zaid Imran and Rafay Nizami" proceedings of ISAI December 2011, Dubai.

[2] SS7 technology by Divyansh, Samarpan, Anup, Ravi in the Proceedings of 13th IASTED International Conference, MIT.

[3] S.Bindu, Raj Mohammed "A Novel Cognition based graphical Authentication Scheme which is resistant to shoulder surfing attack", Proceedings ICIP 08, I.K. International, Bangalore, August, 2008.

[4] William Stallings "Cryptography and Network Security" 4th Edition, Pearson Education Inc.

[5] The world's largest search engine www.google.com.