International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.06,
March-2016,
Pages:1183-1185

www.ijsetr.com

MRGA Scheme for Client Side Authentication using Session Passwords and Colors

AMRUTA MANE[1], MONIKA AVHAD[2], SUCHITA PATIL[3], PRIYANKA BIRAJDAR[4], PROF. V. R. GHULE[5]

[1]Dept of Computers, SKNCOE, Pune, India, E-mail: amrutamane777@gmail.com.
[2]Dept of Computers, SKNCOE, Pune, India, E-mail: monika33avhad@gmail.com.
[3]Dept of Computers, SKNCOE, Pune, India, E-mail: suchitap94@gmail.com.
[4]Dept of Computers, SKNCOE, Pune, India, E-mail: priyankabirajdar2710@gmail.com.
[5]Dept of Computers, SKNCOE, Pune, India.

Abstract: Generally, for the authentication scheme textual passwords are widely used. But the attacks like eves dropping, dictionary attack, social engineering and shoulder surfing are occurred. The Random and lengthy passwords can make the system secure. But remembering those passwords is difficult. The short passwords are easy to remember. But, these passwords can be easily guessed or cracked. So there are alternative techniques like graphical passwords and biometrics. The major drawback of this approach is that those systems can be expensive and the identification process is slow. The graphical passwords are suffering from shoulder surfing which is becoming large problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login. Authentication should be provided for increasing the security level. Rivest-Shamir-Adleman (RSA) algorithm is a popular encryption process that guarantees confidentiality and authenticity over an insecure communication channel. However, several attacks are introduced to break the security of these algorithms due to certain constraints. Also, it may not be guaranteed that the cipher text is fully secured. To overcome such issue, an innovative algorithm, namely, Magic Rectangle is being proposed in this work. It is helpful to enhance the security on account of its complexity of the encryption process. The singly even magic rectangle is constructed based on the seed number, start number, row sum and column sum. It is very difficult to trace these values because of their randomness. So security level is increasing in this proposed system.

Keywords: Session Password, Magic Rectangle, Shoulder Surfing, Secrete Key, Seed Value, Column–Row Shifting, Encryption –Decryption.

I. INTRODUCTION

The textual passwords, graphical passwords are most commonly used schems for authentication. But, such methods are having its own drawbacks. The shoulder surfing attack is direct observation technique, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes. The dictionary attack is a technique for defeating a authentication mechanism by trying to determine its decryption key by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.To overcome these problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this application, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. The two level securities is provided in these work. The first level security is pair based with Magic Rectangle and the second level is pair based with color scheme. When the session password is entered an innovative algorithm namely Magic Rectangle Generation Algorithm (MRGA) is being proposed in this work. It is helpful to enhance the security due to its complexity in encryption process. The singly even magic rectangle is formed based on the seed number, start number, row sum and column sum. The value of row sum and column sum is very difficult to be traced.

II. RELATED WORK

Alaa Hussein Al Hamami et al [4] proposed enhancing the RSA algorithm through the use of additional third prime number in the composition of public and private key. This will increase the factoring complexity of the variable n, where the process of its analysis with the development of equipment and tools become much easier nowadays. GAJBHIYE S.K and ULHE P [10] proposed that textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual pass-words. Most of the graphical schemes are vulnerable to shoulder surfing. To solve this problem session password was introduced. Session passwords can be used only once and every time a new password is generated. Also proposed a scheme related to the grayscale images which will be advantageous as compared to many of the well known formats. Sami A Nagar and Saad Alshamma [5] proposed a new method to speed up the implementation of RSA algorithm during data transmission between different

communication network and Internet. It introduced a new manner by which instead of exchanging the keys between gateways, the indexes refers to the fields, are getting exchanged.

III. PROPOSED METHODOLODY

The Session passwords are generated by using pair based scheme. The singly even magic rectangle is constructed and each character of the plain text is converted into cipher text. The numerals are then encrypted and decrypted using AES algorithm with MRGA. The color ratings are given for the purpose of enhancing security for authentication as shown in Fig.1.

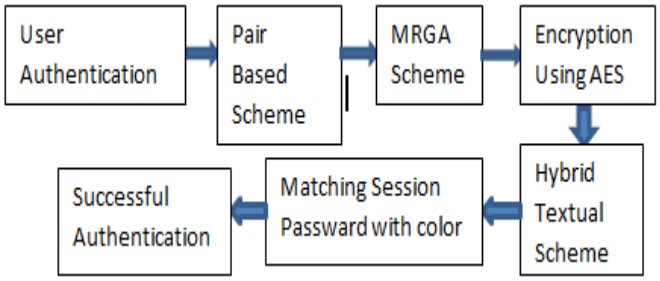

Fig.1. Proposed System Architecture.

A. Pair-based Authentication Scheme

During registration user submits his password. Maximum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass as shown in Fig.2.

Secret pass	A	1	B	2	C	3
SKNCOE16	4	D	5	E	6	F
Pairs	H	7	I	8	J	9
SK NC OE 16	T	K	U	L	V	M
Q P X C	N	W	O	X	P	Y
Session password	Z	Q	G	R	0	S

Fig.2. Paired Based Authentication Scheme.

B. Magic Rectangle Generation Scheme

The Magic Rectangle generation is the first level security obtain by combining the pair-based scheme. The session password generated in pair-based is processed in generation of Magic Rectangle in order to make the password secure. There are many operations are performed and the password text is made such that is not cracked by any others. The text obtained after processing the magic rectangle scheme is not in readable format called as cipher text. The encryption and decryption of cipher text is done by combining Magic Rectange Generation Algorithm (MRGA) with Advance Encyption Standard(AES). After this the text is in readable format for the user.The features of the MRGA involves increasing the randomness of the cipher text value. There is not much difference in Encryption and decryption process time. Magic rectangle increases the complexity of initial activity such as character to number conversion using magic rectangle instead of ASCII. The magic rectangle can be constructed from any starting value and ending value. This Magic Rectangle generation concept is applicable to any public key algorithm. Magic Rectangle is mainly introduced to overcome the attacks in RSA algorithm.

C. Hybrid Textual Authentication Scheme

The User should rate colors from 1 to 4 and he can remember it as "RGBY". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 4×4. This grid contains digits 1-4 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 2 pairs of colors. Depending on the ratings given to colors, we get the session password. This is second level security provided in this work.

IV. RELEVANT MATHEMATICS

Input: Secrete Pass, Session Password, Minimum No, Maximum No, 4 Digit Seed No, Initial Column Sum

Output: Singly Even Magic Rectangle

Method:

Step 1: Read seed number, Minstart, Maxstart value and Initial column sum

Step 2: Compute the row sum and column sum

Step 3: Generate the magic rectangle

Step 4: If (seed number == 1)

Shift either row/column

• Mathematical terms:

A. Magic Square

The base of the magic rectangle is magic square. A magic square of order n is an arrangement of integers in an nxn matrix such that the sums of all the elements in every row, column and along the two main diagonals are equal. The magic constant of a magic square depends only on n and has the value M(n) =n (n2+1) / 2. Magic square can be classified into three types namely odd, doubly even (n divisible by four) and singly even (n is even and not divisible by four). A magic

rectangle of order mxn is an arrangement of integers such that the sums of all the elements in every row are equal and also the sums of all the elements in every column are equal. The magic rectangle is in the category of singly even.ie, the order of the matrix is even but not divisible by four such as 4x6, 8x12, 16x24 etc. Any order with even can be used in this work. It can be followed only the order 4x6, 8x12, 16x24 etc.

B. Divide and Conquer (D and C)

Solving smaller instances recursively Obtaining solution to original instance by combining this solution in magic rectangle, column sum is fixed as 16x24.The existing column sum is divided by two and then applies in 8x12. Further the column sum is divided by two and applies in 4x6 matrixes. For example: Column sum of 16 x 24 = 54320 Column sum of 8 x 12 = 27160 Column sum of 4 x 6 = 13580 The row sum is calculated by using the following formula 5Row sum= column sum +(column sum / 2) Creation of singly even magic rectangle: The singly even magic rectangle is generated by using any seed number, starting number and magic sum. The numbers are generated in consecutive order. Notations used in this work are listed below:

MR : Magic Rectangle

nxm : Order of MR

where n=4x and m=6x

where x=1, 2, 4, 8 etc

MRnxm : MR of order nxm

MRB4x6 : Base MR of order 4x6

MRnxmrsum : Row sum of MR of order nxm

MRnxmcsum : Column sum of MR of order nxm

The values in the MRB4x6 are filled as shown in Fig.3. The function is called MR4x6 fill order (Minstart, Maxstart).

Max_{start}	*(+2)	*(+4)	-6	-16	*(+16)
*(+8)	-10	-12	*(+14)	*(+24)	-24
-14	*(+12)	*(+10)	-8	-30	*(+30)
*(+6)	4	-2	$*Min_{start}$	*(+22)	-22

Fig.3. Magic Rectangle Filling Order.

In Fig.3, '*' represents the places in magic rectangle to be filled, starting from Minstart and incremented by 2 each time to get the next number where as the empty places to be filled, starting from Maxstart and decremented by 2 to get the next number.

- Success Conditions: Even character length password, Rate color from 1 to 4.
- Failure Conditions: Odd character length password is not accepted.

V. CONCLUSION AND RESULT

The proposed work analyzes the various attacks of existing RSA algorithm with ASCII code and introduces security enhancement using singly even magic rectangle. It prohibits any intruders from obtaining the plain text in a readable form. So using these two level model the more security is given for authentication.

VI. REFERANCES

[1] Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting ,IEEE2014.
[2] Article on Web Application Security 101 by Appliclure technologies dot-Defender Web Application Security 2011.
[3] Enhancing Security level for Public Key Cryptosystem using MRGA 2014.
[4] Alaa Hussein Al-Hamami and Ibrahem abdallah aldariseh, "Enhanced Method of RSA cryptosystem Algorithm", 978-0-7695-4959-0/13 , IEEE2013.
[5] Sami A Nagar and Saad Alshamma, "High speed implementation of RSA Algorithm with modified Keys exchange", SETIT2012,IEEE.
[6] Adam Rogers, and Peter Loly ,"The inertial properties of Squares and Cubes", Nov-2004, pp.1-3.
[7] en.wikipedia.org/wiki/Golden_rectangle.
[8] William Stallings, "Cryptography and Network Security", Prentice Hall, Upper Saddle River, New Jersy, USA, Second Edition ,1997.
[9] Ashish Agarwala, R Saravanan," A Public Key Cryptosystem Based on Number Theory" 978-1-4673-0255-5/12, IEEE2012.
[10] Authentication Schems for session passwords using color and gray-scale Paper 2012.
[11] Bernard Menezes, Indian Institute of Tech, Mumbai, Network Security and Cryptography, Cenage Learning Publiactions.
[12] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma Modified RSA Encryption Algorithm(MREA)- 978-0-7695-4640- 7/12, IEEE2012.