A PATTERN BASED KEY GENERATION TO AUTHENTICATION FOR MULTIHOP ROUTING IN WMSN

Prof. P. Kalyani
Computer Science and Engineering, I.R.T.T.,
Erode, India.

Dr.C.Chellappan
Computer Science and Engineering,
Anna University, Chennai, India.

Abstract - Recent research work in the Wireless Sensor Networks involves the homogeneous networks in which the sensor nodes in the specific cluster can get the key value from any other cluster. Most existing key management schemes try to establish shared keys for all pairs of neighbor sensors, no matter whether these nodes communicate with each other or not, and this causes large overhead . The security implementation analysis is separated into two levels, 1. Encryption and Authentication from Sensor modes to Cluster Head. 2. Encryption and Authentication from Cluster Heads to Base Station. This Dual level Encryption standards not only blocks the malicious data from overspreading the network traffic all along the network path but also efficiently shares the dynamic keys. In this research the second level of security has considered and the dynamic keys are generated based on pass pattern or graphical picture. Here dynamic means both 1). The display and selection of characters from a 7x7 matrix called pattern square changes in every session and 2). The strength and degree of security changes dynamically. This pattern consists of a set of symbols such as special characters, alphabets, numbers, etc. by default. The character entered by the user is subjected to the first level of encryption. The encrypted string is placed in 5x5 matrix called magic square. The second level of encryption applied to the pattern value and finally stored in the database in row major. The pass pattern is selected from the pattern square characters which are randomly displayed for each session. This random change in display of characters leads to higher level of security. Also the user is allowed to select their pattern in reverse order which ensures more degree of security against the attack by crackers. This method is strong and robust against all possible attacks and works in the existing infrastructure without compromising the user's comfort.

Key Terms— Pass Pattern, magic square, PPS, Pattern square, matrix encryption.

I. INTRODUCTION

With the technological advancement, alternative authentication schemes are available which are more secure than the conventional pass-word scheme using Biometrics, RSA Secure ID which needs significant changes in infrastructure of the systems and each has its own merits and demerits. In our proposal, we have considered this and it works in the existing system infrastructure with out compromising the user's comfort. The existing system of entering the password, while one logs on to their e-mail. Even though it sounds better, it has some drawbacks, (ie) it is possible to crack the password by the techniques of shoulder surfing, remote access hacking, capturing screen, brute force attack and dictionary attack. The hackers may be of mostly three categories. They are expert hackers (who knows various concepts in hacking), unskilled hackers (who hacks the sites and mail-id's without the deep knowledge on their action) and script kiddies (who hacks almost all the secured systems in the network by the scripting techniques)

In order to overcome this, we have proposed to display a 7x7 square matrix in which the cells are containing the key-board characters that are generated randomly without repetition. The user is requested to enter one's own Pass Pattern sequence instead of the traditional approach. From that entered pattern, the locations of the typed characters are identified from the matrix and they are encrypted through two levels and converted into string. The encrypted string is stored in the database for the future retrieval.

The way of identifying the matrix cells (locations) and encryption steps are elaborated briefly. The main features of this proposed idea is that the characters displayed at every session are different and are almost unique. The total possible combinations of the characters in the 7x7 matrix for display is given by the formula

$$^{n}C_{r} = \frac{n!}{r!(n-r)!}$$

where

n – Total number of characters chosen for display ((ie) only the keyboard characters since it is easy to enter)

r – The total number of characters to be displayed in the matrix

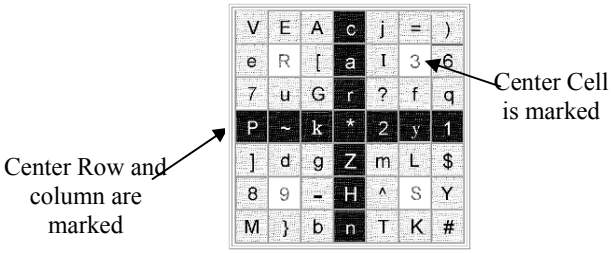
Here, as we are using 94 characters (only the keyboard characters) for random selection and 49 characters for display within the matrix. For our case, the above formula becomes $^{94}C_{49}$ ($\approx 1.4943X10^{27}$). In such a vast number of combinations, it is highly impossible for the dictionary attackers to get the authentication.

There will not be any repetitions or redundancy. The probability for a character to be displayed repeatedly within the 7x7 matrix for various sessions is 0.021(Approx.). Further more, no characters with same case will be displayed for the same session of matrix generation. Hence the probability of repetition will be further reduced to 0.0023(Approx.) for the worst case. This negligible probability ensures the uniqueness of the characters displayed. This in turn increases the performance and degree of security.

II. Related Works

Pass Pattern System is a Dynamic-Password system and is based on the premise that "humans are good at identifying, remembering and recollecting graphical patterns than text patterns". Unlike many User-Authentication systems, in Pass Pattern Scheme (PPS) the user will prove that he knows the secret rather than telling the secret.

Whenever the user wants to get authenticated, the PPS displays an NxN matrix of cells, which is known as Pattern Square. Each cell in the Pattern Square is an image, which represents a character as shown in Figure below. The character can be an alphabet, number or even special characters. The Pattern Square is the challenge that is sent by the server to the user. The Pattern Square will be generated dynamically upon each user request. Hence the characters in each cell of the Pattern Square may change or their position may change or both may change, for every authentication request [1].



III. Still In Practice

Till now, many of the websites and e-mail organizers use the traditional method of getting input from the user in terms of simple characters. And these passwords are compared with the passwords retrieved from the database where it was stored previously during registration. If they are similar then the user is authenticated to access the account. The maximum possibility of the user's choice for the password will be any of the following:

1. Using sequence of characters specifying either name of the person, place or thing either in upper or in lower case.
2. Using special symbols or a non alphanumeric character along with the name for password.
3. Combination of the above two (ie) a string with one non alphanumeric symbol and alphanumeric characters.
4. Using very high password length such as 64 bit characters and the main drawback of this technique is that recalling all those 64 characters is quite impossible.
5. Selecting the sequence of characters from the virtual keyboard rather than from the usual keyboard etc.
6. By using Key loggers (either hardware or software) one can easily access the pass word.

Often it is easy to break the password of the user if the personal information is known. But now-a-days, such a method of getting password is being easy to hack or crack. There are number of methods and various techniques available in the market to hack or crack any of the password protected documents and websites. Some of the frequently used hacking techniques are

1. Shoulder surfing (Looking over another individuals shoulder)[2]
2. Remote access hacking method (Monitoring through network)[2]
3. Capturing screen method (Watching through other system while in usage)[2]

4. Brute force attack (Checking with the most possible combinations i.e. they are the assumptions made by the hackers for choosing the password based on the user's name)[3]
5. Dictionary attack (Trying with all the words from dictionary with all the possibilities of cases until a specific word gets checked as password with an assumption that anyone of the words will be correct) [7]
6. Selecting the sequence of characters from the virtual keyboard rather than from the usual keyboard etc which can be easily cracked by tracing the mouse event or by capturing the mouse pattern [4]
7. The hacker can crack the password by simply collecting the information from the SAM (Security Account Management) data file which stores the username and password[6]

And along with these methods, a number of hacking techniques are also available which are not included in this list. From all these, it is clear that, the present method of document protection is not at all being so safe. Since a number of important documents are transferred and shared by means of the mail, its being a great drawback for such documents. So it is essential to design new authentication scheme that is robust and strong against all attacks.

The shortcomings of the existing system [1] of Pass Pattern are that the Pattern Square (7x7 matrix) is separated into four squares, each of 9 cells by marking the center row and column with a different color. Similarly, the centers of these four squares are also marked with different color. This makes hacker quite easier to remember and hack the pattern by trying with the possibilities applicable for all the four 3x3 matrix. And hence the probability for hacking the password becomes higher.

To overcome this, in our proposal, we have incorporated a sequence of procedures and certain modifications to achieve more efficiency and security. Here, the main transformations which we added in our proposal are the removal of background color pattern and the addition of two levels of encryption along with the reverse sequence of pass pattern allowed.

IV. PROPOSED SYSTEM

To overcome the vulnerabilities of the traditional secret word (password) system discussed above, we have proposed a new idea of using patterns instead of passwords. The core idea of Pass Pattern scheme is that, Instead of remembering a sequence of characters as the secret word, users have to remember a shape as the secret pattern. Otherwise, it can be termed as, Biologically, it will be easier for a human to visualize a pattern or a shape or a graphical cartoon as the secret pattern rather than remembering a sequence of characters as the secret word.

$	#	A	>	/	:	‘
R	s	z	!	)	5	0
,	w	1	_	*	B	.
Q	3	n	<	d	;	=
&	g	L	“	8	`	+
C	p	^	Y	j	?	|
x	~	9	]	%	(	U

Fig.1

In this proposal, we have planned to display a 7x7 square matrix as shown in the above fig.1 which consists of the keyboard characters that are displayed randomly and uniquely for that session. Why 7x7 matrix selected is because to provide uniqueness and avoid redundancy in display of characters in order to achieve high degree of security. Almost the complexity 49! And the probability of repeating a character is .002%. The user must define their own pattern by typing the characters which are evolved in that PPS during that session. This pattern (PPS) will be stored in the database in an encrypted format. This ensures the prevention of hacking. For example, consider the pattern for omega (Ω). For the above chosen pattern, let's consider the cells from the matrix for the pattern can be of some sequence such that it forms a visual image of omega. For instance a sample pattern is highlighted in the following figure.

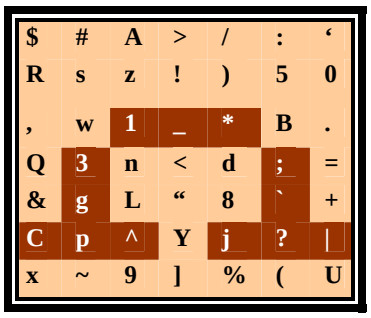


Fig. 2

The sequence of characters for the selected PPS and the traveling order is shown below.

CP^g31_*;`j?|

The sequence of the characters in the 7x7 matrix changes as and when the page is loaded again. This will increase the complexity to the dictionary attackers, shoulder surfing, and brute force attackers. The user is requested to remember the pattern sequence instead of the character sequence as secret word. When the user logs on again, the characters in the user's PPS in the displayed matrix will change. For instance, consider the following 7x7 matrix.

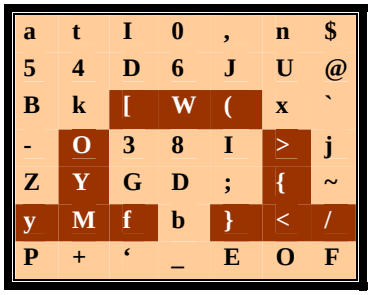


Fig.3.

For the same pattern omega as previous, the character sequence gets altered as

yMfYO[W(>{}</

for the new 7x7 matrix displayed in the above figure 3. The highlighted boxes in the above figure show the pattern not the secret word. Even if the shoulder surfing takes place, the sequence of characters alone is monitored instead of the pattern chosen. If they try to authenticate themselves with the monitored sequence of characters (secret word), they will not get the access, as the characters they entered this time will be appearing in different locations or even they may not appear for this session.

The user is requested to remember the Pass Pattern scheme exactly and the sequence they travel in the matrix during registration along with the starting and ending cell in the matrix. In order to achieve high degree of security over cracking, the user has to remember the data or information compulsorily. The user can easily recall the pattern registered by viewing the Pass Pattern squares. This in turn increases the complexity for hacking, because for the same pattern the user and the hacker can try with the various cells in the matrix but only the correct starting and ending with the traveled sequence during registration will result in authenticating the user. Additionally, as and when the sequence of characters associated with the Pass Pattern stream is entered by the user, before the encryption of the sequence of characters associated with the Pass Pattern scheme (PPS), the string length of the entered sequence is compared with the actual string length of the original sequence of the pattern retrieved from the database. Only when the string length matches, the encryption procedures will take place as the next step. This in turn reduces the overall time complexity required for the computation of

encryption. The sequence of character for the pattern can also be typed in the reverse manner as shown below is also accepted.

/<}{>(W[OYfMy

This is the reverse of the first sequence shown in fig.2. This is also accepted, which is the new concept included in our proposal.

V. SEQUENCE OF THE PROPOSAL

During registration:

1. Get user's personal details.
2. Generate and Display 7x7 matrix with unique characters in the cells.
3. Get Username.
4. Check for availability.
5. If available, get the Pass Pattern from the user.
6. Otherwise go to step 2.
7. Confirm the Pass Pattern.
8. Then, perform the following two levels of Encryption on the Pass Pattern:

A. Add the characters in the sequence with the continuous two digit prime numbers starting from 11.
B. The Magic Square:

Given an $n \times n$ normal magic square, suppose M is the number that each row, column and diagonal must add up to. Then since there are n rows the sum of *all* the numbers in the magic square must be $n \cdot M$. But the numbers being added are 1, 2, 3, ... n^2 and so $1 + 2 + 3 + \ldots + n^2 = n \cdot M$. In summation notation,

$$\sum_{i=1}^{n^2} i = n \cdot M \qquad \textbf{2}$$

Using the formula for this sum, we have

$$n \cdot M = \frac{n^2(n^2+1)}{2} \qquad \textbf{3}$$

and then solving for M gives

$$M = \frac{n(n^2+1)}{2} \qquad \textbf{4}$$

C. Place the encrypted values in the corresponding positions of the dynamic magic square of order 5 created using the above sequence and then add the string length of the PPS with each cell and get the values row wise to store it in the database.

9. Store the username, the length of the Pass Pattern scheme (PPS) and the Encrypted Pass Pattern into the Database.

During login:

1. Generate and Display 7x7 matrix with unique characters in the cells.
2. Get Username and Pass Pattern from the user.
3. Compare the string length of the entered sequence with that of the actual one.
4. If string length doesn't match, go to step 9.
5. Perform two levels of Encryption on the Pass Pattern.
6. Compare the Encrypted Pass Pattern with the existing Pass Pattern that was stored already in the Database during registration.
7. If they are not equal, compare the reverse of the encrypted Pass Pattern with the existing Pass Pattern that was stored already in the Database.
8. If step 4 or step 5 returns TRUE, authenticate the user.

9. Totally five chances are given since five possible combinations of magic square generated. Even if fails then access denied.

The number of encryption operations performed on step 3 is two. One is collecting the address of each character in the entered Pass Pattern and it is added with two digit prime number generated sequentially based on the string length of the Pass Pattern. The next one is, placing the corresponding ASCII characters of the first level encrypted PPS in a magic square of order 5. The placing of PPS in the magic square is based on the step 8.B of the algorithm. The values of the PPS from the first level are mapped directly to the corresponding cell created dynamically. This in turn, added with a private key and stored in the database in the row major.

VI. MERITS OF THE PROPOSAL

The unique background color in the display of 7x7 matrix is made, increases the complexity for hacking the users' Pass Pattern. Another advantage is that, the reversal of the pattern secret word is also accepted in the proposed method. Since the Pass Patterns are stored in the database in the encrypted format, even the decryption or trying in the reverse sequence won't be useful for the hacker because of the second level of encryption. Hence the proposed system becomes more secured than the traditional system. We added two levels of encryption to increase the complexity level of hacking, and the encrypted string is stored in the database for future comparison and retrieval also reversal of entry of PPS is allowed.

Another merit of the proposal it requires only 27 (25+2) bytes (25 characters of cipher text and length of the string entered) for storing the encrypted string in the database. This is less when compared to the storage space of cipher text generated by MD5 encryption algorithm. Since the magic square in which the first level cipher text is going to be placed is also determined dynamically as and when the user enters the details during the creation of the account. The same selection of magic square is achieved by selecting all the possible combinations that are generated by the system during log on to authenticate the user. This in turn increases the complexity of hacking the password by accessing SAM file. The probability for choosing the magic square dynamically is $n(p) = \frac{1}{5}$ (0.2) for success of each magic square.

A. Brute Force Attack:

The complexity of hacking the PPS by the hacker using the brute force technique is high when compared to the normal way[1]. The hacker can try two kinds of Brute force attacks on this system. The first way of attacking the system is to ignore the Pattern Square and try with some random string. For a user Pass Pattern of length 4, there will be a unique Secret Word for the given session. If the hacker wants to guess that Secret Word, the probability of success will be $1/(94^4) = 1.28 \times 10^{-8}$ (Since there are 94 printable characters). If the guess is wrong the probability of success will remain same for the next guess, it is because the Secret Word will change with every attempt. Hence,

The probability of success for every attempt = 1/94"

The other way of doing Brute force search is to try all combinations of positions. For example, if we consider a 7x7 Pattern Square there will be 49^n (if selection of Pass Pattern includes reuse of positions) or ${}^{49}P_n$ (without reuse of positions) different patterns of length n.

$$\text{Number of possible PassPatterns} = \begin{cases} (N^2)^n \\ \frac{N^2!}{(N^2-n)!} \end{cases} \quad 5$$

To break the system, the hacker on an average has to break $(nx49_n)/2$ images (with reuse) or $(nx^{49}P_n)/2$ (without reuse).

$$\text{Number of images that are to be broken} = \begin{cases} \frac{n \times (N^2)^n}{2} \\ \frac{n \times N^2!}{2 \times (N-n)!} \end{cases} \quad 6$$

N represents the size of the Pattern Square and n represents the length of the Pass Pattern. [1]

In addition to the above complexity, in our proposed algorithm of PPS, the user has to break $(5 * {}^{25}P_n)/2$ images because of the 5x5 magic square is used for second level encryption of the pass pattern sequence. Also there are five possible combinations for magic square generation in which one will be matched with registered one.

B. Dictionary Attack:

The efficiency of this proposal is 99.99%. The hacker who follows the dictionary attack technique won't get success since we are using dynamic display of characters in the pattern we selected. Even when they try with all the possible combinations from the display, its complexity level is very high since the stored value is not character or word it is the encrypted pattern.

*C. Script Kiddies***:**

The best, worst and average case efficiency for the script kiddies and the unskilled hackers is

$$(5 * \frac{n(n^2+1)}{2}) + 2. \qquad 7$$

Because, they try to crack the encryption techniques, but here there are two levels of private key and 5 different magic squares are used in the encryption sequence.

D. Password Crack:

It is nothing but Security Accounts Manager file stored in database which contains the hash representation of user name and password. But in this proposal there are two levels of encryption and hence the possibility for cracking the password through SAM file is highly impossible.

VII. Summary And Scope

- Only dynamic password User-Authentication system which does not require any extra Hardware or Mathematical operations [6]
- Gives strong protection from Key loggers, Bruteforce Attack(Text based and Position based), Shoulder Surfing, Social Engineering, Dictionary Attack and Guessing [6]
- Very simple for the user to remember a graphical image or polygonal shape than remembering the Strong Password [1]
- Can be used with the existing infrastructure [1]
- Instead of prime numbers for first level of encryption, memory address for the 7x7 matrix can be taken for considerations
- Replacing the odd number of rows and columns in the magic square for the second level of encryption, with the even number of rows and columns

VIII. Conclusion

In this paper we present a dynamic pass pattern scheme (PPS***)*** based on pattern or graphical picture for key generation. After passing through various testing procedures, it is observed that, the proposal uses two ways for recognizing the Pass Pattern when compared to the existing system. The encrypted string stored in the database provides more security to Pass Pattern sequence when compared to the existing sequence in the database. The row major of the cipher text also increases the complexity of the Pass Pattern when it is tried with brute force attack and dictionary attack. So the key generated based on this dynamic pass pattern scheme for authentication between cluster head and base station in a heterogeneous wireless sensor network.

References

[1] Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 2003.
[2] Micki Krause, Harold F. Tipton, " Handbook of Information Security Management", Vol 1-3 CRC Press LLC, 2004.
[3] Stuart Mc Clure, Joel Scrambray, George Kurtz, "Hacking Exposed", Tata McGraw-Hill, 2003.
[4] Matt Bishop, " Computer Security Art and Science", Pearson/PHI, 2002.
[5] T. Rakesh Kumar, S. V. Raghavan, "Mobile PassPattern System (MPPS): Advanced User Authentication system for mobile devices", 2008.

[6] James F. Kurose and Keith W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet”, Pearson Education, 2003.
[7] Larry L.Peterson and Peter S. Davie, “Computer Networks”, Harcourt Asia Pvt. Ltd., Second Edition.
[8] Andrew S. Tanenbaum, “Computer Networks”, PHI, Fourth Edition, 2003.
[9] William Stallings, “Data and Computer Communication”, Sixth Edition, Pearson Education, 2000.
[10] T. Rakesh Kumar, S. V. Raghavan, "Pass Pattern System (PPS): A Pattern-Based User Authentication Scheme", 2008, Heidelberg.
[11] William Stallings, “Cryptography and Network Security – Principles and Practices”, Prentice Hall of India, Third Edition, 2003.
[12] Atul Kahate, “Cryptography and Network Security”, Tata McGraw-Hill, 2003.
[13] Bruce Schneier, “Applied Cryptography”, John Wiley & Sons Inc, 2001.
[14] Charles B. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Third Edition, Pearson Education, 2003.
[15] Maximilian Miller, Gelöste und ungelöste mathematische Probleme, Leipzig 1982
[16] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. 2003 IEEE Symposium on Security and Privacy, May 2003, pp. 197-213.
[17] A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks Xiaojiang Du, Member, IEEE, Mohsen Guizani, Fellow, IEEE, Yang Xiao, Senior Member, IEEE, and Hsiao-Hwa Chen, Senior Member, IEEE IEEE Transactions on wireless Communications, Vol. 8, No. 3, March 2009

AUTHORS PROFILE

Prof. P.Kalyani received the M.E. degree in Computer Science and Engineering from College of Engineering, Guindy, Anna University, Chennai, Tamilnadu, India in 1992. She is pursuing the Ph.D degree in College of Engineering, Guindy, Anna University Chennai, Currently working as HOD and Associate Professor in the Department of Computer Science & Engineering, in IRTT, Erode, Tamil Nadu, India. Her current research interest includes Routing in wireless Sensor Network & Network Security. She is a life member of ISTE, IEI.

Dr. C. Chellappan received a Ph.D in Computer Science and Engineering in 1986, from the Anna University, Chennai, Tamilnadu, India. He is working as a Professor in Computer Science & Engineering at Anna University, Chennai, Tamilnadu, India, specialised in the field of Computer Science. His present research focuses on Mobile Computing, Computer Network, Object Technology, Network Security and conceptual papers in leading journals.