Grid based Approach for Data Confidentiality

Sreelatha Malempati
Dept. of Computer Science & Engg.,
R.V.R. & J.C. College of Engineering,
Chowdavaram, Guntur, A.P

Shashi Mogalla
Dept. of Computer Science & System Engg.,
Andhra University College of Engineering
Visakhapatnam, A.P.

ABSTRACT

Network security measures are required to protect data during their transmission. Sensitive information transmitted across a network requires confidentiality. Data confidentiality is the protection of transmitted data from passive attacks. Passive attacks are eaves dropping or monitoring the traffic. The goal of the intruder is to obtain information being transmitted. These attacks can be prevented by encryption. This paper proposes a simple grid based method for providing confidentiality to the data or the session key being transmitted. The sender and the receiver share a global secret key which is used for extracting the data from a grid.

Keywords

encryption, confidentiality, grid based, graphical passwords, passive attacks.

1. INTRODUCTION

Network security measures are required to protect data during their transmission. Security attack is any action that compromises the security of information owned by an organization. Confidentiality is the protection of transmitted data from passive attacks. Passive attacks are in the nature of eaves dropping on or monitoring of transmissions. The goal of intruder is to obtain information being transmitted. These attacks can be prevented by encryption. Encryption is the process of transforming data into a form which is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and one or more keys. Encryption techniques are of two types , namely asymmetric-key encryption and symmetric-key encryption techniques [1]. Asymmetric-key encryption uses two keys a public key and a private key for encryption and decryption. In symmetric key encryption, same key is used for both encryption as well as decryption. The sender and the receiver should agree on this key.

One time pad is a simple way of encrypting the plain text. It consists of choosing a random bit string as the key, converting the plain text in to a bit string and computing the XOR of the two strings bit by bit. One time pad is immune to all present and future attacks. DES (Data Encryption Standard) algorithm and AES (Advanced Encryption Standard) are the most popular symmetric-key algorithms. DES requires 56-bit key and AES requires minimum 128 bit key for encryption [2]. Both sender and receiver should agree on this key. In either one time pad or DES/AES , secret key is to be shared between the sender and the receiver. Diffie-hellman key exchange protocol allows the sender and the receiver to establish a shared secret key. These keys are sensitive information and for transmitting this information, confidentiality is essential.

This paper is organized as follows: Related work is discussed in section 2, in section 3 the grid based approach for sharing data is introduced, security analysis is done in section 4, conclusion is given in section 5.

2 Related work

Conventional textual passwords use a string of alphanumeric characters. Textual passwords are vulnerable to dictionary attacks, social engineering , brute force attacks and shoulder surfing. Graphical passwords are designed as an alternative to textual passwords. There exist various approaches that focus on graphical authentication schemes. Blonder [3] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of the locations.

Dhamija and perrig [4] proposed a graphical authentication scheme in which the user selects a certain number of images from a set of random pictures. Later user has to identify the pre-selected images for authentication. Jansen [5], [6] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. Weinshall and Kirkpatrick [8] proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes.

Some grid-based approaches are designed for authentication. In grid based methods, users select cells on a grid for authentication. Jermyn et al [7] proposed a technique called " Draw A Secret"(DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order. Zheng et al [9] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text. The user has to select a shape which can be a number, character, geometric shape or a random shape. The password is encoded by a sequence of grid cells, represented by two-dimensional coordinate pairs.

Tao H et al [10] designed a graphical password scheme "pass-go". Pass-go requires a user to select intersections instead of cells, as a way to input a password. An intersection is actually a point which does not have an area. Grid based approaches have many advantages - no need of storing the images in the server, transmitting images and there is no limit on the length of the password. Sreelatha Malempati and Shashi mogalla [11] proposed an authentication technique based on native language passwords. Same concept is used in this paper to provide confidentiality.

Authentication with one-time codes is based on the idea that both client and server share a secret. The client presents it to the server either directly or in a derived form according to some algorithm, possibly with additional data also known to the server. In the one-time code approach, clients present each code to the server only once; codes can't be reused. A scratch list is the simplest form of a one-time code. A Scratch list is typically given to the client once, in paper form, and usually contains about 40 to 100 codes. The server knows these codes, and clients use them sequentially or in an indexed form. So, the shared secret is the listed code and clients use it as is, without further derivation. If the client uses an indexed scratch list, the server decides which one-time code should be used next by specifying its index in the list; otherwise, clients typically have to track the used codes themselves. Either way, each code is used once and only once, and the server automatically sends the client a new list when only a certain number of codes are left. This paper proposes a different method of generating one time codes.

3 GRID BASED APPROACHES FOR SHARING DATA

Grid based approaches are designed for authentication. Every time for login, when the user enters his name the server generates an interface with a grid of randomly generated data and transmits it to the user. The user enters the password based on the grid data. User is then authenticated by the server using the password sent by the user. This grid based approach can be used to exchange data or session keys between two parties. In this approach, as data is not directly transmitted, confidentiality is provided to the data being transmitted.

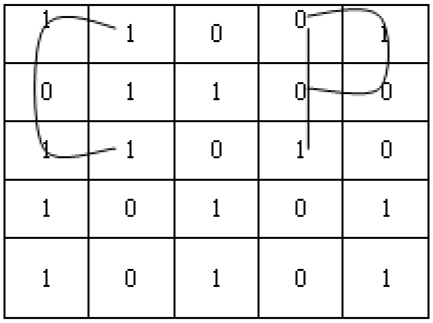
3.1 Sharing random data

Many cryptographic algorithms require the sender and the receiver to share some secret information. The sender may select some random information and send it to the destination. Both of them can extract from it some key or data. A simple grid based method is proposed here for sharing some random information. The sender and the receiver initially share one global key which is used for extracting data from the grid. The sender generates some random data in the form of a grid as shown in fig 1. The random data generated will be transmitted to the receiver. Then the sender and the receiver extract same data from the grid which can be a secret data or a session key.

1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

Fig 1: Random data generated by sender

The sender generates random data consisting of 0s and 1s in the form of a grid. This data is transmitted to the destination as { 1100101100110101010101011 }. The receiver after receiving the data arranges it in the form of a grid. Suppose the global key shared by them is "CP". The global key consists of two characters C and P. Based on the shape of these characters, data is extracted from the grid. Each character may contain one or more strokes and each stroke contains a sequence of grid cells.



1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

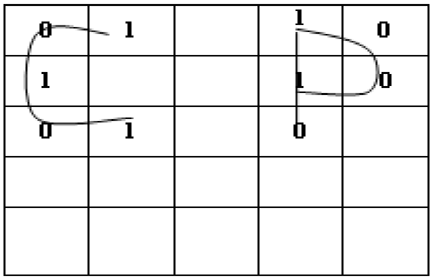
Fig 2 : shape of global key characters

The sender and the receiver follows the shape of the characters in the grid and extracts {11011} for C and {{001},{0100} } for P, all together data is { 110110010100 }. Here C consists of single stroke and P consists of 2 strokes. Now both sender and receiver are having the same data which can be secret information or a session key.

3.2 Sharing selected data

If the sender wants to share some selected data with the receiver, the sender arranges data in the shape of the global password, and then transmits it to the receiver.

Suppose the sender wants to send { 101011101001 }, then the sender arranges data in the form of a grid as shown fig 3. The remaining part of the grid is filled with random data as shown in fig 4 and then transmitted to the receiver as {0111010010010010011111001}.



0	1		1	0
1			1	0
0	1		0	

Fig 3: Selected data for global password

0	1	1	1	0
1	0	0	1	0
0	1	0	0	1
0	0	1	1	1
1	1	0	0	1

Fig 4: grid filled with random data

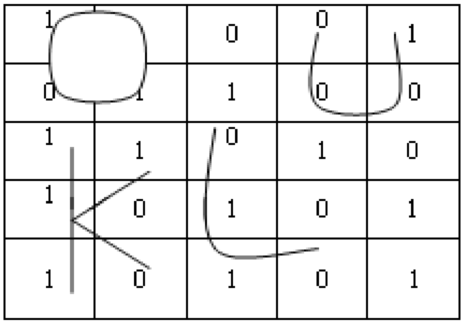
When the receiver receives the data, based on the global password he extracts the data from the grid. There is no limit on the length of the global password and it can be used to extract the required amount of data from the grid.

4 SECURITY ANALYSIS

Between the sender and the receiver , an intruder can capture the data and he can try to break the code. If an intruder captures the data, there are two possibilities to attack . The intruder may or may not be having the knowledge of global secret key. In both the cases, it is not easy to break the grid data and extract actual information.

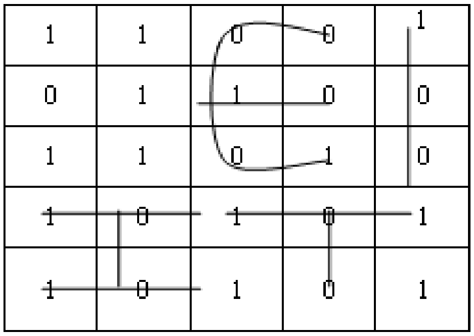
(a) Intruder has no information about global secret key

The intruder captures the grid information, but he is not having the knowledge of global secret key. In order to get the information, three things are required – **the characters, the exact shape of the characters and position in the grid**. The intruder has to try all possibilities of the characters, variants of the characters and their positions in the grid which is a difficult job (fig 5 and fig 6). The intruder should know even the length of the password and there is no limit on the length of the password that can be extracted from the grid.



1		0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

Fig 5 : some of the possible characters

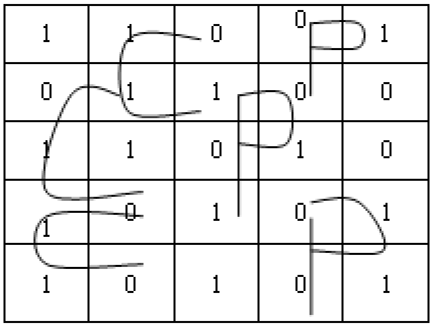


1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

Fig 6: Another set of possible characters

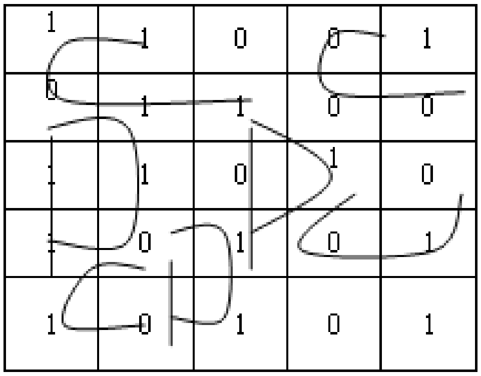
(b) Intruder has information about the global secret key

If the intruder knows that the global secret key is "CP" , he can try to extract the data from the grid. In this case, he requires only two things- **the exact shape of the characters and their position in the grid**. The shape of the characters C and P can be represented in many ways, in different locations and this leads to different sets of data. Fig 7 shows three different representations of the global secret password. For the password "CP" first set gives {011100010}, second set gives {101101011010} and the third set gives {011000010}.



1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

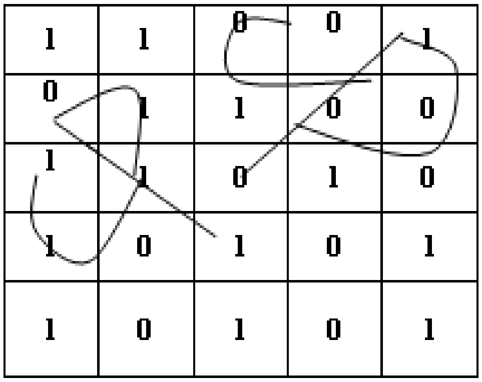
Fig 7: 3 representations of "C" and "P"



1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

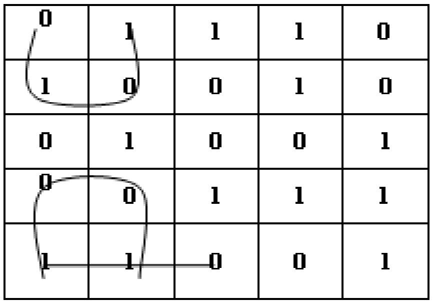
Fig 8 : variations of “C” and “P”

There can be variations in the representations of C and P which leads to different sets of data as shown in fig 8 and fig 9. fig 10 and fig 11 shows different representations of “C” and “P” with same data.



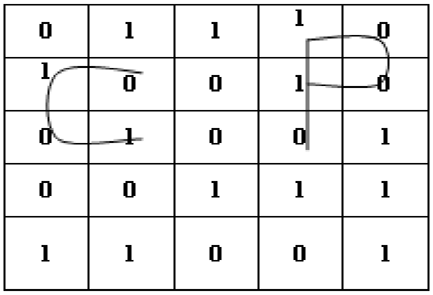
1	1	0	0	1
0	1	1	0	0
1	1	0	1	0
1	0	1	0	1
1	0	1	0	1

Fig 9: variations of “C” and “P”



0	1	1	1	0
1	0	0	1	0
0	1	0	0	1
0	0	1	1	1
1	1	0	0	1

Fig 10: a representation of “C” and “P”



0	1	1	1	0
1	0	0	1	0
0	1	0	0	1
0	0	1	1	1
1	1	0	0	1

Fig 11: “”C” and “P” with the same data (at different grid cells)

Grid / Characters: A separate grid can be transmitted for each character or many characters can be extracted from the same grid. The important point is the sender and the receiver should consider the same shape and position of characters in the grid. In order to provide security from other attacks, the grid data can be encrypted and encrypted data can be transmitted.

5. CONCLUSION

Data confidentiality is necessary for the data being transmitted. This paper proposed a simple grid based approach to provide confidentiality to the data or session keys being transmitted. The sender and the receiver share a global secret key which can be used to share random data or session keys.

The shape of the characters in the global key are used in extracting data from the grid. There is no limit on the length of the global password and it extracts required amount of data from the grid. The intruder should have the knowledge of the length of the password, the characters in the password, the shape of the characters and their position in the grid to break the code. This is simpler than conventional encryption techniques. An extensive study has to be done on the effectiveness of the proposed approach.

6. REFERENCES

[1] A.S. Tanenbaum, 1999. Computer Networks, 3rd Edn., Pearson and Education.

[2] S. William, 2003. Cryptography and Network Security, principles and Practice, 3rd edn., Pearson and Education.

[3] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[4] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[5] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[6] W. Jansen, "Authenticating Users on Handheld Devices” in Proceedings of Canadian Information Technology Security Symposium, 2003.

[7] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin, “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[8] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[9] Z. Zheng, X. Liu, L. Yin, Z. Liu “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5 May 2010.

[10] Tao H. and Adams C. 2008. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2): 273-292.

[11] Sreelatha Malempati and Shashi Mogalla, “Intrusion Prevention by Native Language Password Authentication Scheme” ,4th International conference on network security and its applications CNSA 2011, Springer LNCS-CCIS 196, pp. 239–248