Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6148-6151, 2017
ISSN: 1816-949X
© Medwell Journals, 2017

Secure Password Scheme Using Cryptography, Steganography and Top-K Retrieval Concept

B. Vasudevan and S. Pooja
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal, Karnataka, India

Abstract: The need for security is increasing in the modern digital world. Since, the user information is more vulnerable to attackers it is necessary to protect that information from the hand of hackers. So here arises the need for a strong password. In the digital world password plays a main role and need for a strong password is essential. Password plays an important role in different applications ranging from e-mail to online banking. Most of the present technology makes use of combination of alpha-numeric characters as password. These are more vulnerable to hackers. These can be traced using key loggers or key tracing software's. One alternative is using the virtual keyboard but still the password is alpha-numeric characters. These can be cracked used dictionary attack. Different attempts have been made to overcome these limitations one of the modern approaches in mobile is by using patterns as passwords. In this proposed method, we aim at creating a strong password mechanism using the picture patterns. The traditional alphanumeric password is replaced with the picture patterns. For enhancing the security AES encryption, LSB steganography and Top-k retrieval mechanism are used.

Key words: Password, picture, picture pattern, security, AES encryption, steganography

INTRODUCTION

With rapid growth of internet usage, the need for secure login mechanism is of great importance. Security in digital system has become an area of key concern beginning from 21st century. With easy access to resources, intruders try their level best to compromise on security. It is very essential to build a secure mechanism which is robust, secure and easy to use. With introduction of latest mobile phones it has included pattern lock schemes. But these pattern locks still make use of the alphanumeric characters as password. An attempt to obtain sensitive information by disguising as a trustworthy entity in electronic media is called phishing. Phishing is of many types such as spear phishing, deceptive phishing, content phishing, etc. Different means for capturing the data are as follows.

Keyloggers and screen loggers: These are specific assortment of malware that keep track of user input and send tracked data to the intruder with the help of internet. They are capable of installing themselves into compromised machines as little utility programs known as aide protests that run naturally when the system is started.

Session hijacking: It illustrates an assault when depicts an assault where client's exercise is being observed until they sign into an objective record or exchange and build up their true blue certifications. Later malignant program takes over control and can embrace unintended activities, for example, exchanging reserves without the client's learning.

Hosts file poisoning: At the instance when a client enters a URL to visit a site it should first be converted into an IP address using translation mechanism before it's sent over the internet. The dominant part of PCs running a Microsoft Windows first look for these "host names" in their "hosts" record before making a Domain Name System (DNS) query. By "modifying" the hosts record, program have a false address sent, taking the client without being aware to a fake "carbon copy" site where their data can be compromised.

System reconfiguration attacks: Adjust settings on a client's PC for noxious purposes. For instance: URLs in a top picks document may be changed to direct clients to resemble the other alike sites. For instance: a bank site URL might be changed from "bankofabc.com" to "bancofabc.com".

Corresponding Author: B. Vasudevan, Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal, Karnataka, India

Data theft: In business word, information burglary is a commonly used secret activity. Problem of data theft happens because of storage of sensitive data insecurely in secure servers. Imposters can focus on these secure servers to get access to this sensitive data. By taking secret interchanges, plan reports, lawful assessments, representative related records and so forth, attackers benefit from offering to the individuals who might need to humiliate or cause monetary harm or to contenders.

Access to computers is commonly using alphanumeric passwords. However, users find it difficult to remember passwords that is long and random-appearing. For their ease, they create passwords that are short and simple which in return turn out to be insecure. These passwords have low entropy. These mechanisms are vulnerable to dictionary, shoulder surfing (Shah *et al*., 2015) brute force attacks. By graphical passwords, users click images instead of alphanumeric characters. This makes task of remembering password easier for users. In this study, a secure login mechanism is being proposed that uses a new and more secure graphical password mechanism.

In existing system combination of alpha-numeric characters are more vulnerable to hackers. These can be traced using key loggers or key tracing software's. These can be cracked used dictionary attack. Graphical passwords tend to offer greater security when contrasted with text based passwords. This is on the grounds that many individuals to recall text based passwords, utilize plain words (as opposed to the suggested muddle of characters). The programmer with the help of dictionary search which is tedious but easy to perform operation, can access systems in fractions of seconds. But if there are many images available, a hacker must try every possible combination at random. Thus, offering more security.

Literature review: In traditional approach, passwords are normally text based. These passwords can be generated from a set of 95 characters. It is common human tendency to choose the password that are easy to remember, thus reducing the password entropy. This poses a serious threat to security since, these are vulnerable to different attacks such as dictionary attack, shoulder surfing, key loggers, etc. The main intention behind introduction of graphical passwords was to provide the user the ease of recalling password. Graphical passwords also tend to offer better resistance against different attacks. Studies has found that humans tend to have a significant capability to memorize and to remember graphical images. If users can recall more complicated graphical passwords (i.e., from a larger password space) an attacker will have to build a larger dictionary based on the application context, this would require him to invest more time or deploy system with high configuration to get the same success rate as for textual passwords. This also requires sophisticated mechanism to fill the custom input fields and custom input mechanisms.

Single-image based schemes (Tao, 2006) use one image as a background and user is required to repeat several sequences with an input device such as clicking or dragging, in the same manner as in the signup process. In this mechanism, a user is shown a predefined image on a display and it is essential for him to choose single or multiple predetermined spots on the presented image in order to gain access to resource. Major short coming of this mechanism is that users are not allowed to click randomly on the image. The prevalent difficulties of single-image mechanisms include.

The background picture must be complicated and sufficiently rich that numerous vital focuses are accessible. Because of the low redundancy in content, effective image compression is not possible, hence large files require storage and network bandwidth in much higher quantity.

Since, keyboard is not being used as a device for providing input and if the mouse doesn't work as expected the system does not work as intended. Seeking small focus points in a high content image may be cumbersome and difficult for users with low vision.

In the proposed research, many images are used as a password. In this scheme many images are given and image selection is required to be inputted by user which user had inputted earlier. To enhance the security the input pictures are treated individually and encrypted. Steganography (Singh *et al*., 2007) method is used to hide the encrypted data. A single base image is used for steganography method. The final data is stored in the server using Top-k retrieval method. Top-k retrieval is a scheme proposed by Jiadi *et al*. (2013) where a file is split into multiple pieces and stored in different servers.

MATERIALS AND METHODS

Proposed system

Architectureal design: Figure 1 explains the building blocks of the proposed mechanism.

Picture pattern: A picture pattern corresponds to the sequence of images as chosen by the user to form his password. The sequence of selection should be remembered. An user has to select a set of pictures provided in virtual keyboard during the signup process. The user has to remember the selected pictures and the

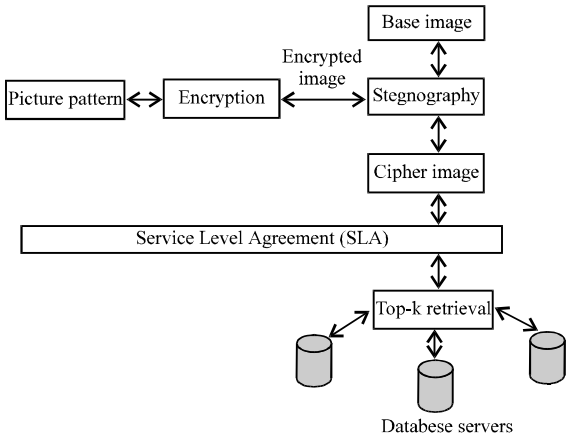

Fig. 1: Proposed system (architectural diagram)

sequence of selection. During the signin process user has to select the pictures from the virtual keyboard in the same sequence. The virtual keyboard will be loaded dynamically and the position of pictures will be changed in each refresh. Minimum length for password is defined as 4 and maximum length is defined as 8.

Encryption: The selected pictures are encrypted using AES encryption algorithm (Sheth and Saxena, 2016). Suppose the user choses 4 pictures as his password all the 4 pictures are encrypted independently to form 4 encrypted images. The selection of AES as an encryption algorithm is mainly because of its proven security. The encryption key is hardcoded and is predefined in the application.

Steganography: The encrypted images are hidden behind a base image using steganography technique. Copies of base images are created based on the length of the password chosen by user. As a result of this step, multiple images are generated with encrypted password hidden in it which appears to be similar. The base image is hardcoded and is predefined in the application. LSB matching technique is used for steganography.

The benefits of LSB are its straight for wardness to install the bits of the message specifically into the LSB plane of cover-picture and numerous procedures utilize these techniques. Tweaking the LSB does not bring about a human-discernible contrast in light of the fact that the adequacy of the change is little. In this way, to the human eye, the subsequent stego-picture will appear to be indistinguishable to the cover-picture. This permits high perceptual straightforwardness of LSB. Another, level of security adds to steganography by utilizing an encryption procedure for encoding message before adding to picture.

Cipher images: The identical images genereted in the previous step is encrypted again using AES encryption algorithm. The encryption key is hardcoded and predefined in the application. At the end of this step, cipher stegonographic images will be genrated based on the length of the password.

Service level agreement: Service level agreement defines the databases and the number of databases used to store the encrypted passwords. It also defines the connection parameters.

Top-k retrieval: This step breaks the cipher images into multiple parts as defined in the service level agreement. The parts are saved in multiple databases which are defined in the SLA. During the signin process the parts are merged again and deciphering process is applied. During login the above said procedure are applied in reverse.

Sequence diagram: Figure 2 explains the sequence diagram of the proposed mechanism. Initially the user creates an account by selecting appropriate username and picture pattern password. The database is checked for availability of the username. If user name is available and password matches the required criteria (minimum length 4 and maximum length 8) the account is created and the password is encrypted using the proposed methodology and stored.

During the login process user provides his credentials. The password is retrieved from the database against his user name and deciphered. The entered password and the retrieved password are compared against each other. If they are found to be matching, the user is taken to his home page.

For this proposed methodology. Net framework 4.5 was used with C#. The database was chosen as Microsoft SQL Server. Since, SQL Server can be easily integrated with windows operating system and C# it provides more versatility for the implementation. Microsoft SQL Server is also proved to be the most secure of any of the major database platforms.

The steganography method that has been used here is “Edge adaptive image steganography based on LSB matching revisited”. Unlike LSB (Sheth and Saxena, 2016) replacement and LSBM which deal with the pixel values independently, Luo *et al.* (2010) proposed a method namely “LSB matching revisited (LSBMR)” Luo *et al.* (2010) that use a pair of pixels as an embedding unit in which the LSB of the first pixel carries one bit of secret message and the relationship (odd-even combination) of the two pixel values carries another bit of secret message.

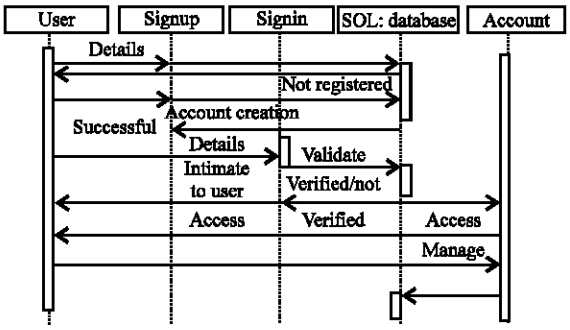

Fig. 2: Sequence diagram of proposed methodology

In such a way, the modification rate of pixels can diminish from 0.5-0.375 bits/pixel (bpp) because a most extreme embedding rate which means less changes to the cover picture at a similar payload contrasted with LSB substitution and LSBM.

RESULTS AND DISCUSSION

Analysis of proposed method: The proposed method has many benefits over the traditional password mechanisms. The benefits are as follows:

Hotspot resistance: A noteworthy issue is that users may record their password as opposed to remembering it. Use of virtual key board and loading images in random location decreases the problem of users remembering the correct location when they review their password and in addition counteracting key-logging spyware. This increases the hot spot resistance of the proposed mechanism (Gyorffy *et al*., 2011).

Password space: Password space is identified by the combination of images possible. The proposed method has a very high password space compared against the traditional password schemes.

Password entropy: For text based passwords, entropy is controlled by the arbitrariness of the alpha numeric characters in an arrangement. The entropy of alph anumeric secret key is very low. To increase the entropy of the password image sequence ought to contain numerous inconsequential pictures. The images in virtual keyboard are chosen in such a way that the selected password has high entropy.

Password communication resistance: A major problem, is that users may note down their password instead of memorizing it. Moreover, an user may orally convey their secret key when they ought not. In the proposed method since, images are used and the sequence is of utmost importance, it's difficult to communicate the password. Though it will not stop the user from communicating their password, it makes it more troublesome when contrasted with text based passwords.

CONCLUSION

In this study, a secure password mechanism using picture pattern, cryptography, steganography and Top-k retrieval has been proposed. This method emphasizes on enhancing the security of the password. It is being demonstrated that despite the fact that content passwords can have an extensive password space, still they have low entropy, since, users chose passwords that could be speculated easily and are vulnerable to dictionary attacks. In addition, users tend to use the same text password that they can recollect instead of making changes to their passwords regularly. Graphical passwords can also face the ill effects of similar low entropy. With the use of virtual keyboard and patterns most of the issues are tried to be addressed in the proposed mechanism.

REFERENCES

Gyorffy, J.C., A.F. Tappenden and J. Miller, 2011. Token-based graphical password authentication. Intl. J. Inf. Secur., 10: 321-336.

Jiadi, Y., L. Peng, Y. Zhu and G. Xue, 2013. Toward secure multikeyword top-K retrieval over encrypted cloud data. IEEE. Trans. Dependable Secure Comput., 10: 239-250.

Luo, W., F. Huang and J. Huang, 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inform. Forensics Secur., 5: 201-214.

Shah, A., P. Ved, A. Deora, A. Jaiswal and M. D'silva, 2015. Shoulder-surfing resistant graphical password system. Procedia Comput. Sci., 45: 477-484.

Sheth, U. and S. Saxena, 2016. Image steganography using AES encryption and least significant nibble. Proceedings of the IEEE International Conference on Communication and Signal Processing (ICCSP), April 6-8, 2016, IEEE, Melmaruvathur, India, ISBN:978-1-4673-8549-7, pp: 0876-0879.

Singh, K.M., L.S. Singh, A.B. Singh and K.S. Devi, 2007. Hiding secret message in edges of the image. Proceedings of the International Conference on Information and Communication Technology, March 7-9, 2007, Dhaka, pp: 238-241. March 7-9, 2007, Dhaka, pp: 238-241.

Tao, H., 2006. Pass-Go: A new graphical password scheme. Master Thesis, University of Ottawa, Ottawa, Ontario.