IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-6 E-ISSN: 2347-2693

Secure Server Authentication Using Graphical and Session Password

Smruti Bhosale, Shradha Botre, Gayatri Chandnani*, Nikita Kamble

[1,2,3,4]MAEER's Maharashtra Institute of Technology College of Engineering,
Kothrud, Pune-411038,India

www.ijcseonline.org

Received: May/16/2016 Revised: May/30/2016 Accepted: Jun/18/2016 Published: Jun/30/ 2016

Abstract- With today's technology enhancement, it is possible to store your whole life on your hard drive. But at the same time it increases the risk of information theft. Human generally create passwords that are easy to remember. There are many techniques used to crack passwords like Eves dropping, shoulder surfing, social engineering, etc. To make hacking difficult, we should find out techniques that will increase the security level. So this paper proposes a combination of textual session password and graphical passwords. Session passwords enhance security as they are valid only for certain period of time. Graphical passwords on the other hand are easy to memorize and are better resistant to hacking. Algorithms like Pair based algorithm and Cued Click Point algorithm are used to facilitate the combination.

Keywords- SSA, GSP, Security, Authentication

1. Introduction

While leaving your house for work in the morning, you surely take steps to protect it from theft. The same principle can be applied to information. Steps must be taken to protect the information. If it is left unprotected, it can be accessed by unauthorised person. When data is not protected properly there are chances of losing the data and this is known as information breach. The consequences of an information breach are severe.

Computer security is concerned with four main areas: Confidentiality, Availability, Integrity, and Authentication.

Computer security is essential in today's communications since many of our day to day actions depend on the security of the data. The most widely used attacks against a computer system are trap doors, worms, social networking and eves dropping (Man-In-The-Middle attack).Also popular are DoS / DDoS attacks, which can be used to disrupt services. Often insiders i.e. authorised users are directly involved in data theft and misuse too. If proper measures are taken, such attacks can be prevented.

Authentication is the first step of information security. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during login-in time. Current authentication methods can be divided into three main areas:

- Knowledge-based authentication: These are most widely used and include text based and picture passwords. Textual passwords are the first choice for authentication by humans.
- Token-based authentication: Most token-based authentication systems also use knowledge based authentication to prevent impersonation through theft or loss of token. An example is ATM authentication, which requires a combination of a token (a bank card) and a secret knowledge (a PIN).
- Biometric-based authentication: These techniques include figure prints, iris scan, face recognition. These techniques are not widely adapted because they are expensive and identification process is slow. However this technique provides greater level of security.

Due to limitation of human memory, users generally choose the password which is easy to remember. The strength of password depends on size of memorable password space rather than full password space. The tradition password schemes are vulnerable to many attacks.

2. Existing System

Existing system generally uses Textual password or Graphical password individually. Textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing[4]. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. Most cases of stolen information occur by the hacker guessing the victim's password.

There are a lot of techniques being used to steal passwords. Some of the most common include:

- ***Guessing*** :There are a number of programs designed to guess a user's password based on information found online about the user, such as names, birth dates, names of friends or significant others, pet names or license plate numbers[4].

- ***Dictionary-based attack***: These are generally used for textual passwords. In this attack, the hacker makes use of a dictionary words. Hacking is done by trial and error method by using one word at a time[4].

- ***Brute Force attacks*:** This attack method refers to trying every conceivable combination of key strokes in tandem with a user name to find the password[3].

- ***Shoulder surfing:*** hackers watch people enter their user names and passwords[4].

- ***Spyware:*** It is software that tries to gather information about people or an organisation without their consent. This information is then send to another entity. Spyware is classified in four categories: 1.System Monitors 2. Trojans 3.Adware 4.Tracking Cookies[4].

- ***Keylogger:*** It is hardware or a small program that monitors the keystrokes that user types using a keyboard.

- ***Social Engineering***: It aims to obtain users' information by manipulating the user to give up secret information like pins, passwords, bank account numbers, etc[4].

To overcome these vulnerabilities, we need to enhance the security level.

3. Proposed System

Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this project, two techniques are combined to enhance the level of security. Textual passwords support the use of virtual keyboard [2] to generate a session password and image authentication use the concept of Cued Click Points (CCP)[1].

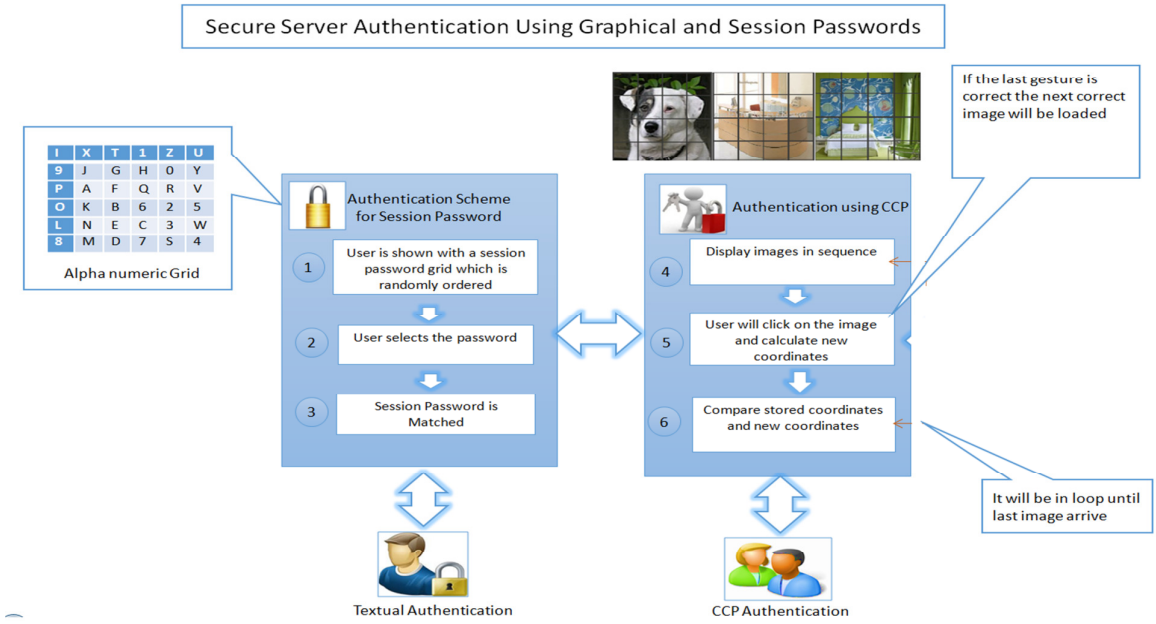

Fig 1. Block Diagram of the system

3.2 ALGORITHMS

Pair-Based Authentication Algorithm

- During registration user submits his password. Maximum length of the password is 8 and it can be called as secret pass[2].
- 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.
- The session password consists of alphabets and digits. User has to enter the password depending upon the secret pass.

Cued-Click Point Algorithm

- At the time of registration, user will select images(max 5) which he/she want as a credentials at the time of user login and user will also enter number of splits. Number of splits will indicate the size of matrix in which the image is going to divide.
- Then user will give check- point for each image i.e. for example for a particular image split is 3 then that image will get divided into a 3x3 matrix and then check point can be combination of row and column e.g. (1,2),(2,2) etc. Images and respective checkpoint is stored in database.

4. System Design

The proposed system using new Authentication technique consists of 3 phases i.e. registration phase, login phase, verification phase.

a) Registration phase

- The user selects a textual password of his choice (also called as the secret pass).
- Selects certain number of images along with the number of splits of the image.
- Selects the click points on the corresponding image i.e. a cell from the corresponding image.

b) Login phase

- User first login by textual Login id and password. However, user does not enter textual password using the keyboard he/she enter using number grid which is show on the login screen.
- Session passwords are generated based on this secret pass[2].
- At the time of CCP login[1], will select the check point (which is given at the time of registration) then system will check into the database using **CCP**, if checkpoint for each image matches with checkpoints stored in database then user logs in successfully.

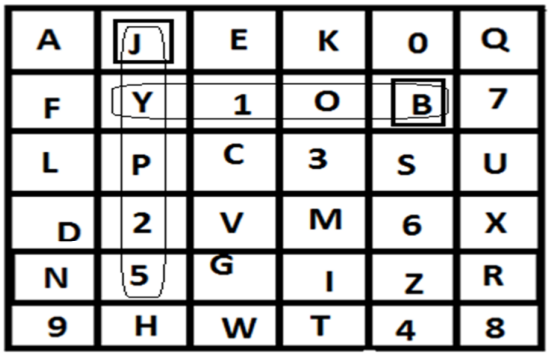

Fig. 1 Pair-based authentication grid

Fig 3. CCP Authentication

5. Conclusion

Password possesses many useful properties and used in various security applications. Unfortunately today's standard methods for password input are subject to variety of attacks based on observation, casual eavesdropping, to more exotic methods. There are various applications that require high security, for this purpose we have tried to enhance the level of security by combining two techniques. Through the technique of pair-based authentication the use of session password is advocated. This technique uses a grid for generating a session password similar to OTP. The second technique i.e. CCP (Cued Click Point) authentication is an alternative and has advantages over pass-point algorithm. There is growing interest for graphical passwords because people are better at memorizing graphics rather than text. This project makes its best efforts to avoid the various attacks like the shoulder surfing, eavesdropping. However, the system accepts a textual password of only eight characters. This could be considered as an improvement in future.

References

[1] J. Kanagarag and K. Noel Binny, "*A safe and powerful technique for visual based (secret word) password confirmation*", International journal of advance research in computer science and management studies, Vol. 2, Issue 11, November 2014.

[2] M Shreelatha,M Shashi,M Anirudh,MD Sultan Ahamer,V Manoj kumar, "*Authentication schemes for session password using color and images*", International journal of network security and applications, Vol. 3, No.3, May 2011.

[3] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000. Real User Corporation: Passfaces. *www.passfaces.com*.

[4] R. Nithya,"Graphical password", International journal of computer science and information technology research, Vol. 2, Issue 3, September 2014

