Survey on Authentication Password Techniques

Priti Jadhao, Lalit Dole

Abstract - ***Authentication is process of determining whether someone or something is ,in fact who or what to be declared. For authentication mostly textual passwords are used. Passwords are the most commonly used method for identifying users in computer and communication systems. Typically, passwords are strings of letters and digits, i.e., they are alpha-numeric. Such passwords have the disadvantage of being hard to remember. Graphical passwords, which consist of some actions that the user performs on an image. Such passwords are easier to remember, but are vulnerable to shoulder surfing (which consists of simply watching a user login). We present a few graphical password schemes that offer resistance to shoulder surfing.***

Keywords — Graphical Password , Session Password, Textual Password.

I. INTRODUCTION

Authentication is any protocol or process that permits one entity to establish the identity of another entity. The old methods of authentication are based on the realities of our physical world; basic human authentication is done by identifying unique physical characteristics of other human being. In some cases, such methods are insufficient, particularly when authentication must be accomplished by a person who does not personally know the person to be authenticated. Authentication protocol are capable of simply authenticating the connecting party or authenticating the connecting as well as authenticating itself to connecting party.

Password are mostly widely used form of authentication. Commonly used methods for authentication are as follows :

- Authenticate Using UserName and Password.
- Authenticate Using a Certificate deployed to the mobile device.
- Authenticate using one-time password or security tokens.
- Authenticate using Smart Card.

As above password can be used this way or any other techniques will see next . Authentication is more essential for the security purpose. Upto this password can be easily guessed by any third person.

Authentication is direct need of each and every person's / organization; it is essential for a person's/organization not because it copes with security threats, the reasons it deals with develops policies, procedure and mechanisms that provide administrative, physical and logical security. Different organizations have different authentication requirements and so they set different authentication according to their requirement type.

The main goal of authentication to secure their data / system from third (unknown) person. Authentication being used increasingly in military and government agencies, hospital and other business settings[7].

Manuscript received on May, 2013.

Priti Jadhao, CSE Dept, G.H.Raisoni College of Engineering, , Nagpur, India.
Lalit Dole, CSE Dept, G.H.Raisoni College of Engineering, , Nagpur, India.
Third Author name, His Department Name, University/ College/ Organization Name, City Name, India.

II. LITERATURE REVIEW ON PASSWORD

The paper survey, most of the paper searched are used passwords for authentication by using textual password, alpha-numeric password and graphical password this password techniques are used but having drawback like shoulder surfing brute force attack. Watermarking techniques is also used , but not for the passwords authentication. Two authentication techniques are based on text and colors proposed for PDA in this they generate the session passwords and resistant to dictionary attack[2].Drawback of this paper is that every time they generate the session password and it is difficult to remember new password to the user.

Two new authentication schemes authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. But in this same problem is occur that every time user has to enter password again and again. It is too hard to remember password and as it is the session password it is for the particular time only[1].

To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing .Here text was combine with image and color to generate the session password and every time user wants to enter new password as session ends . Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Same problem is here too as previously comes. Drawbacks associated with the textual passwords such as brute-force and dictionary attacks and same this problem held with graphical passwords which includes shoulder-surfing and are very expensive to implement. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords [3].

III. PASSWORD TECHNIQUES

A. *Alpha-numeric passwords:*

Alpha numeric password were first introduced in the 1960s for security purpose that secure the confidential data .In alpha numeric password the password are :

- The password should be at least 8 characters long.
- The password should not be easy to relate to the user.
- The password should not be a word that can be found in

dictionary or public dictionary.

- Ideally, the user should combine upper and lower case letters and digits.

Drawbacks:

Alpha-numeric password is the dictionary attack. Passwords are used by user are mostly common words or phone no. , name etc. This type of passwords are easily guessed or crack by third person.

B. Graphical Passwords:

Because human beings live and interact in an environment where the sense of sight is predominant for most activities, our brains are capable of processing and storing large amounts of graphical information with ease. While we may find it very hard to remember a string of fifty characters, we are able easily to remember faces of people, places we visited, and things we have seen. These graphical data represent millions of bytes of information and thus provide large password spaces. Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security **[4][6].**

Advantages of graphical passwords:

Dictionary attacks are infeasible, partly because of the large password space, but mainly because there are no pre-existing searchable dictionaries for graphical information. It is also difficult to devise automated attacks. Whereas we can recognize a person's face in less than a second, computers spend a considerable amount of time processing millions of bytes of information regardless of whether the image is a face, a landscape, or a meaningless shape[5].

Drawbacks :

Perhaps the biggest drawback for current graphical passwords is the shoulder surfing problem. Although graphical passwords are hard to guess, a person who gets to observe a few login sessions could, depending on the scheme, eventually figure out the password. The above example reveals the password to anybody watching the login session.

The shoulder surfing problem :

As the name implies, shoulder surfing is watching over people's shoulders as they process information. Examples include observing the keyboard as a person types his or her password, enters a PIN number, or views personal information. Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing. Most of the existing schemes simply circumvent the problem by stating that graphical passwords should only be used with handheld devices or workstations set up in such a way that only one person can see the screen at the time of login.

While it is usually possible to ensure that there are no people looking over one's shoulder at the time of login, the value of graphical passwords as an alternative to alpha-numeric passwords diminishes somewhat if they can only be used in environments set up to prevent shoulder surfing.

IV. CONCLUSION

In this paper, authentication password techniques used for security purpose .As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. Authentication needs more powerful authentication techniques which remove all drawback of as mentioned above in authentication password techniques.

V. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

[1] GAJBHIYE S.K.1* AND ULHE P.2 -Authentication Schemes for Session Passwords Using color and gray-scale images(2012).

[2] Bin Hu, Qi Xie, Yang Li- Automatic verification of password based authentication protocols using smart card (2011).

[3] 1S.Balaji, 2Lakshmi.A, 3V.Revanth, 4M.Saragini, 5 V.Venkateswara Reddy-Authentication Techniques for Engendering Session Passwords With Colors and Text. (2012).

[4] L.Sobrado and J.C. Birget, “Graphical Passwords”, The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002,

[5] Hai tao, ***“Pass-Go, a New Graphical Password Scheme”***, Master Thesis, University of Ottawa Canada, June 2006.

[6] G. E. Blonder. Graphical passwords. *United States Patent5559961*, 1996.

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

Priti Jadhao, B.E.(CSE) Pursing M.E.(Mobile Technology)

Lalit Dole M.Tech.(IT)