International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 04, April 2017
www.ijates.com
ijates
ISSN 2348 - 7550

A SURVEY ON VARIOUS AUTHENTICATION TECHNIQUES AND GRAPHICAL PASSWORDS

Tushar R. Mahore[1], Prof. A.V.Deorankar[2]

[1]*Computer Science and Engineering, Government College of Engineering, Amravati, (India)*

[2]*Computer Science and Engineering, Government College of Engineering, Amravati, (India)*

ABSTRACT

In last few decades various applications have been developed in various fields, where authentication is the main process of granting access to the particular application. Authentication is the process, in which an individual is identified on the basis of username and password. In authentication username and text-based passwords are the most commonly used techniques. In conventional systems usually the text-based passwords are the combination of alphanumeric characters, which includes text, numbers and special characters. On the other hand in graphical password systems images are used for authentication. Biometrics are the another technique where the authentication has been done by using physiological or behavioral concept of particular user. In this paper we have done a survey on various authentication techniques that are currently in use. The authentication techniques discussed in this paper are different from each other. This paper mainly focuses on various characteristics of every technique and how they are different form each other, what are their pros and cons.

Keywords :Graphical Password Authentication; Draw-a-Secrete (DAS); PassMatrix; Biometric Authentication

I INTRODUCTION

Authentication schemes are one of important part of computer field, everywhere in the world of computer authentication plays an important role in identifying an individual. For the identification, the individual is supposed to be inputting some credentials proving to the computer system that the one trying to access the service or any other thing is a valid individual. The difficult part in authentication is that, the process of authentication is supposed to simple for the users, while it provides high security which protects the privacy of the users. Lots of work has been done in the way of providing security by keeping the authentication process simple, one of the most common process is, in which the user has to create text-based password using alphanumeric combination.

Various Human Authentication Techniques are present in Computer World, they are:

1. What you know (Knowledge base authentication)
2. What you have (Token base authentication)

3. What you are (Biometrics base authentication)

The above mentioned authentication processes are currently in use, in different ways at different places. Each and every of them have some advantages and disadvantages.

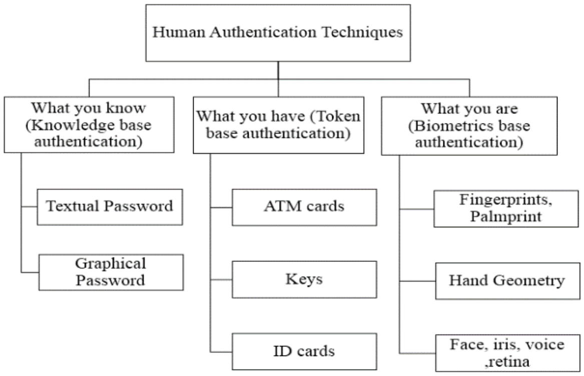

Human Authentication Techniques
What you know (Knowledge base authentication)
What you have (Token base authentication)
What you are (Biometrics base authentication)
Textual Password
Graphical Password
ATM cards
Keys
ID cards
Fingerprints, Palmprint
Hand Geometry
Face, iris, voice ,retina

Fig. 1. Taxonomy of Human Authentication Techniques

Every day researchers are doing something new in the way of providing more security for the authentication techniques. Various advancements are made in the field of authentication, such as new techniques are evolved in graphical authentication scheme, now which can be used on any platform, such as mobile devices as well as web applications and desktop applications.

The paper is arranged in the following sections, section II discusses the various types of human authentication schemes, section III discusses how graphical passwords are more trustworthy, and finally section IV concludes the paper.

II HUMAN AUTHENTICATION SCHEMES

2.1. Knowledge Based Authentication

Knowledge based authentication also known as the KBA is the most widely used authentication technique. Near about every web application we see uses the KBA. As the name indicates the KBA requires knowledge of the private information of the individual to show that the person providing the information is the one who is the owner of the identity. In KBA the user has to answer at least one “secrete” question. There are some criteria for the good question in KBA, (a) the question should be appropriate for the large segment of population, (b) the answer is supposed to be easy for remembrance, (c) the question must have only one answer, (d) the answer should be difficult to crack or guess.

KBA is further classified into two types, (i) Textual Passwords and (ii) Graphical Passwords.

2.2. Textual Passwords

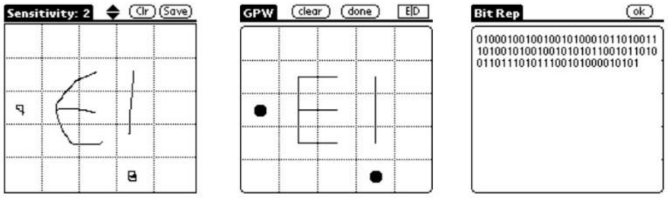
Textual passwords are the most commonly used authentication technique in computer field. In text based password authentication, the user is supposed to select username and the alphanumeric password, and remember both of them. At the time of authentication, user inputs the username and the password in the given fields, and on the basis of that authentication has been done. The main difficulty in the text-based passwords, which has been pointed out by the users is the selection of the alphanumeric passwords. These passwords are difficult to remember, especially for those users who do not belong to computer field [1]. According to Ofcom's "Adults Media Use and Attitudes Report 2013" report, a poll of 1805 adults aged 16 and over discovered that 55% of them used the same password for most websites [2].

While selecting the passwords the instructions for selecting a perfect password is always given such as, use the combination of uppercase and lowercase letters, then use at least one number and special character. Such kind of passwords are strong against attacks, but the problem is faced by the user. These kind of alphanumeric passwords are difficult to remember. So the users goes for the easy way and selects easy passwords, which are very easy to crack for attackers, leading to the problem of losing the privacy of the data, and an unauthorized access.

2.1.2. Graphical Password's

Graphical passwords are much more popular in mobile devices. Lots of graphical authentication schemes are developed in last few decades. Some of them are very popular among users, such as PIN authentication. Various graphical authentication schemes [3], [4], [5], [6] are present in the world, these schemes are developed to overcome the problems associated with text based passwords. In the early days of graphical authentication there are some restrictions, due to the low pixel quality of the devices. The first idea of the graphical password has been given by Blonder in 1996.

Since then various types of methods have been developed few of them are very popular. Draw-a-Secrete (DAS) [5] is one of the technique in which the user is supposed to draw a set of gestures for authentication. The drawing is then mapped to the coordinate pair used to draw the password and recorded in the sequence. Another most studied graphical authentication scheme is PassFaces [6]. The reason behind the popularity of the PassFaces scheme is that it is simple and easy for implementation. A set of faces is presented to the user at the time of login, and form that the user has to select those faces belonging to his/her set.



```
010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101
```

Fig. 2. Draw-a-Secrete (DAS)

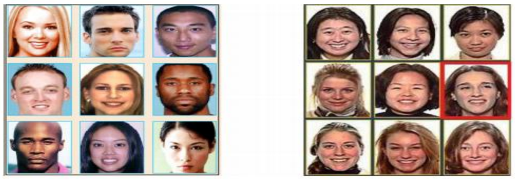


Fig. 3. Passfaces System [7][8]

PassPoints [9] is one another technique which is popular in graphical authentication techniques. This technique is introduced in 2005 by Susan Wiedenbeck et al. In this scheme the user has to click on the set of predefined pixels on the predestined photo, as shown in Figure 4, with the correct sequence and within their tolerant squares during the login stage.

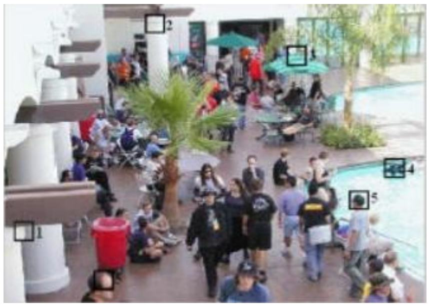


Fig. 4. PassPoints Technique [9]

Recently the new technique has been proposed in 2016 as a shoulder surfing resistant scheme is proposed by Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng known as PassMatrix [10]. This Scheme is based on PassPoints, in this scheme the user has to select the pass image from the given image, and at the time of authentication the user is provided with the login indicator, which is to be set on the given scroll bars. This scheme shows promising results against shoulder surfing attacks.

Like all the above graphical authentication schemes, there are some other schemes are present, which are not as much popular as the above techniques, such as discussed in [11], [12], [13], [14], [15].

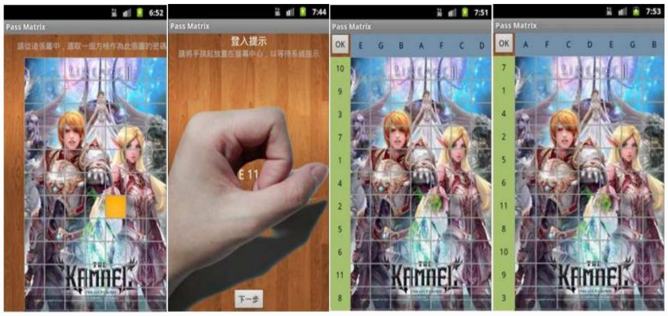


Fig. 5. (a) Select pass image, (b) Generated login indicator, (c) Scroll bars setting, (d) After setting login indicator and pass image coordinate at same positions [10]

2.3. Token Based Password

In token base authentication system, security tokens are used to prove one’s identity electronically. The token is used in the addition or at the place of passwords to identify the particular user. The tokens acts like electronic key to access something. Various types of tokens are available in the market, which are used for the authentication process. Some of them may consists cryptographic keys, some may have biometric data such as fingerprint, and some of them may possess passwords.

All of the tokens used contains some secrete information, there are four different ways in which this information is used.

- Static password token. The device contains a password which is physically hidden (not visible to the possessor), but which is transmitted for each authentication.
- Synchronous dynamic password token. A timer is used to rotate through various combinations produced by a cryptographic algorithm. The token and the authentication server must have synchronized clocks.
- Asynchronous password token. A one-time password is generated without the use of a clock, either from a one-time pad or cryptographic algorithm.
- Challenge response token. Using public key cryptography, it is possible to prove possession of a private key without revealing that key. The authentication server encrypts a challenge (typically a random number, or at least data with some random parts) with a public key; the device proves it possesses a copy of the matching private key by providing the decrypted challenge. [17]

ATM cards are the basic example of the token base authentication, it comes under the connected tokens smart card technology. Smart cards can be very cheap and contain proven security mechanism. Similar to the ATM identity cards and keys are also the example of the token based authentication. ID cards are the most commonly used authentication technique in any organization. ID cards are most popular in these sectors, they contains RFID tags, which at the time of inserting authenticates on the unique tag number.

2.4. Biometrics Based Authentication

Biometrics based authentication is again most common in some of the organizations. Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. Most commonly used characteristics for authentication include fingerprint, face, and iris. A conventional biometric authentication system works in two phases: enrollment and verification (Fig 6). In the enrollment phase, a biometric feature set is extracted from user's biometric data and a template is created and stored in the database. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication.

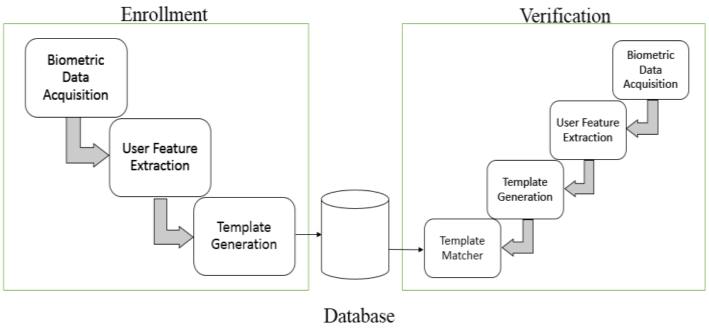


Fig. 5. Enrollment and Verification in Biometric Authentication

Various biometrics authentication techniques are present in the market, such as (a) Fingerprint or Palm-print, (b) Hand Geometry, (c) Face, Iris, Voice, Retina Detection.

All of these techniques are developed in various ways, the development in this field leads to the more secured Authentication schemes. Among these techniques fingerprint is the most popular technique, which uses fingerprint scanner for authentication.

III WHY GRAPHICAL PASSWORDS

Among all of the above discussed authentication schemes, each and every technique has their own advantages and disadvantages. Most widely used authentication technique is the text based password. Then on the organizational level token based authentication and biometric authentication is also popular.

In all these techniques graphical authentication techniques shows most promising results. It can be used on large scale, and cheap as well as easy for implementation. On the other side biometric authentication provides more security but cannot be used on large scale, because of its high cost and difficult of implementation. Graphical passwords are easy to remember for users and difficult to crack by attackers.

In graphical authentication recent development of PassMatrix technique can be possibly implemented on the web platform.

IV CONCLUSION

From this survey we have reached to the conclusion that how the authentication security is important, but at the time of focusing on the security we also have to consider the ease of use, by the user perspective. From this survey we can say that in future graphical authentication is going to be more popular. So for making the authentication more secure, by keeping in mind that the schemes are supposed to be easy for the user, lots of work can be done in this area. Also the graphical authentication schemes are not going to be limited for the handheld devices, but it can be easily implemented on various platforms.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, “Cryptanalysis of password authentication schemes: Current status and key issues,” in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] “55% of net users use the same password for most, if not all, websites. When will they learn?” https://nakedsecurity.sophos.com/2013/04/23/users-same-password most-websites/

[3] R. Dhamija and A. Perrig, “Deja vu: A user study using images for authentication,” in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[4] “Realuser,” http://www.realuser.com/.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[6] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[7] Passfaces Corporation. The science behind Passfaces. White paper, http://www.passfaces.com/ enterprise/resources/white_papers.htm, accessed July 2009.

[8] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.

[9] P. Dunphy, J. Nicholson, and P. Olivier. Securing Passfaces for description. In 4th ACM Symposium on Usable Privacy and Security (SOUPS), July 2008.

[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[11] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng "A Shoulder Surfing Resistant Graphical Authentication System" IEEE Transactions on Dependable and Secure Computing 2015.

[12] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[13] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.

[14] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.

[15] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.

[16] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.

[17] "Security token" https://en.wikipedia.org/wiki/Security_token