International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

A Survey on Authentication Techniques

[1]Mr.Kati Anil, [2]Mr.K.Dayakar
[1,2]Assistant Professor, Department of Computer Science and Engineering.
Jayamukhi Institute of Technological Sciences, Narsampet.

Abstract:

Security refers to all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it and limiting access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters. We have different type's security techniques to protect the information and also our credentials. In this paper we will discuss some of the security techniques. There are different types of security techniques are existed, such as Human Authentication Techniques and Computer Authentication Techniques. The Human Authentication Techniques are Knowledge Base, Token Based, Biometrics and Recognition Based. The Computer Authentication Techniques Textual Passwords Graphical Passwords Biometric schemes.

Keywords: Security, Authentication, Biometrics, Text and Graphics, Palm Vein, Iris Recognition System, OTP, Voice Recognition.

I. INTRODUCTION

AUTHENTICATION is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a username and password. Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:

1. Knowledge Base.
2. Token Based.
3. Biometrics.
4. Recognition Based.

Computer Authentication Techniques are as follows:
1. Textual Passwords
2. Graphical Passwords

II.Human Authentication Techniques

1. Knowledge Base Technique: In this knowledge base technique, we have the remember the password and some other security credentials. It means that consumer or the person have the memory power to know about his details. And also don't share the details to unauthorized persons.

2. Token Based Technique: Token based technique is like communication process between client and server or between knowing persons. In this Technique each and every step in process generated tokens and also applies on that area like where we authenticate our information to others.

Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security token provided by the server. An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. The service validates the security token and processes the user request. After the token is validated by the service, it is used to establish security context for the client, so the service can

make authorization decisions or audit activity for successive user request.

3. Biometrics Based Technique:

The steps in processing a finger image include capture of the image, image processing, feature detection, and matching. The procedures used by different vendors vary in detail, but have a general similarity. This discussion is based primarily on a technical report by Hopkins (1997), but it includes information from several other vendors, as well.

The E-device for capturing a finger image. This device consists of a light source, a prism on which the finger is placed, one or more lenses, and a digital video camera. The user of the sensor places his or her finger on the dark area of the sensor, where the prism is located. The output of the sensor is a digital image, as illustrated in the first pane. Although this technology is typical of the state of the art, other technologies can also be used, including holographic and thermal imaging technology.

4. Recognition Based Technique: In this recognition based technique we have different types of recognition techniques are there that are face recognition, voice recognition, Iris recognition.

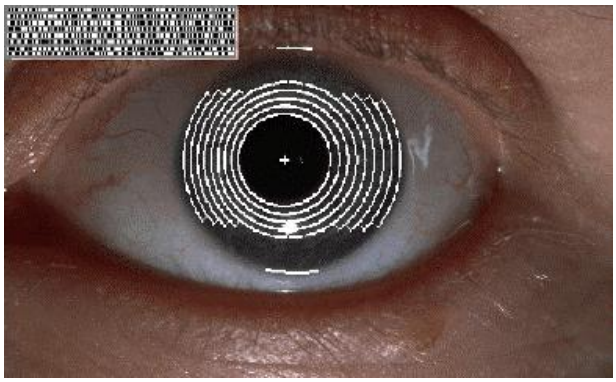
A. Face recognition: One approach to face recognition using visible light uses a neural network as the basis of its face recognition algorithm (Phillips, 1997). Another method, based on a statistical analysis of facial images, is being used to recognize the faces of drivers who are crossing the U.S./Mexico border as a part of a project sponsored by the Immigration and Naturalization Service (INS) to speed up the entry process (Visionics Corporation, 1997).

An alternative approach to facial imaging uses an infrared image measuring temperature differences in the face, rather than a visual image, as the basis for recognition. The temperature is determined by the underlying vascular structure of the face (Beale, 1997).

Such an infrared image, termed a thermo gram, does not look at all like a traditional photographic image. However, this information seems to uniquely identify individuals; even identical twins have different thermo grams.

B.Voice recognition: Voice recognition is often used for controlling access to a building, because it can be conducted at a telephone at the building entrance. This technology requires an individual to enroll by speaking one or more phrases several times. The individual who seeks access will be asked to speak one of the phrases used at enrollment or a different one. For example, one system uses two random digit phrases for enrollment, and two other random digit phrases for verification (Higgins & Nichols, 1994). Using different phrases during the enrollment and verification phases makes the system less vulnerable to attack by a tape recording of the enrollment phrase. However, the identification problem is substantially more difficult when enrollment and verification phrases are different.

C.Iris recognition: The iris of the eye has features that can be used to identify an individual with a level of accuracy that is better than most other biometrics. Like Fingerprints and thermo grams, the patterns in the iris are unique; even between identical twins.



An image of the iris can be taken using a video camera at a distance of up to one meter. The code that is used to represent the iris is represented in the upper left-hand corner of the figure. The advantages of this method include high accuracy, fast identification, and lack of physical contact with the sensor. However, the system cost is currently relatively high, compared to alternative technologies.

III.Computer Authentication Techniques

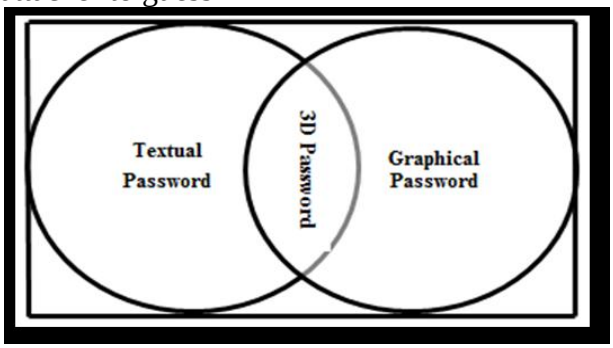
1. Textual and Graphical Passwords Technique:

It can be further divided into two categories: recognition-based and recall-based graphical techniques.

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Main flaw was that password space was small since, the number of images were limited to 30.

2. 3D PASSWORD: Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The 3Dpassword is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. Moreover, user have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more and given the large number of objects and items in the environment, the number of possible 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess



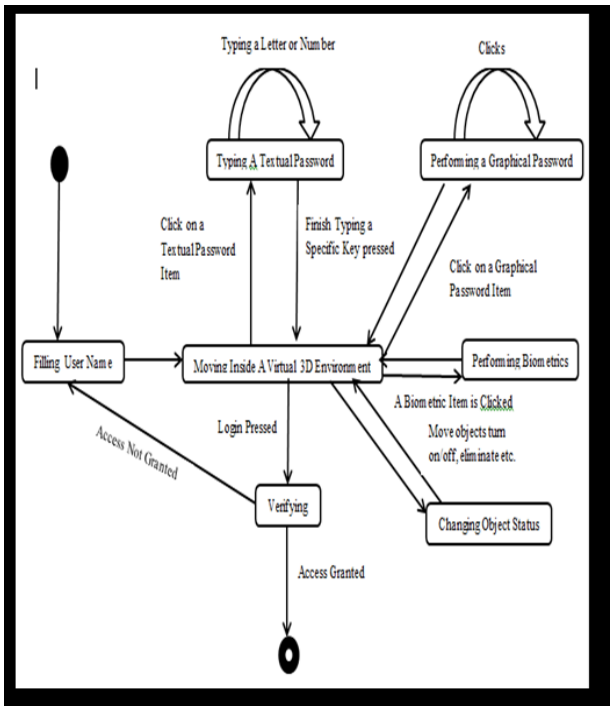


Fig:3D Password and Diagram of Creating 3D Password.

3. 4D PASSWORD: As the 3D authentication scheme suffers from many weaknesses such as shoulder surfing attack, timing attack etc., there is the possibility of hacking the 3D password. The 4-D Password scheme is an attempt to make the existing scheme even more robust and powerful [2]. We propose to add another key to the current scheme, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. This key, what we propose to refer to as the 'FOURTH DIMENSION' would be an encrypted string that encapsulates a gesture that the user is supposed to make with his hands, in front of a webcam, apart from his password.

Consider a web-based repository of research work for scientists, wherein each scientist has his own account which stores his files and folders. This repository employs the 4-D password scheme.

As a new user, I will sign up as follows:

1. Choose a username.
2. I will be redirected to the password generation page.

3. I will enter the 3-D environment.
4. Inside the environment, I will perform certain actions, as have been discussed before.
5. I will exit out of the environment and submit my actions.

6. I will then be asked to perform a gesture in front of the webcam. This gesture, once successfully captured, will be saved. I will be notified of the time that I had taken to perform this gesture this time.

7. I will need to remember it for subsequent attempts at login Sign up process is complete.

IV. Application Areas

1. **Critical Servers:** Many organizations are using critical servers which are protected by a textual password. 4D Password authentication scheme proposes sound re-placement for these textual passwords.
2. **Banking:** Almost all the Indian banks started 3-D password service for security of buyer who wants to buy online or pay online.
3. **Nuclear and military Facilities:** 4D password has a very large password space and since it combines RECOGNITION+RECALL+TOKENS+BIO-METRIC in one authentication system, it can be used for providing security to nuclear and military facilities.
4. **Airplanes and Jet Fighters:** Since airplanes and Jet planes can be misused for religion and political agendas, they should be protected by a powerful Authentication scheme.

5. **ATMs, Desktop and Laptop Logins, Web Authentication.**
6. **The Cloud:** Cloud computing is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. It provides various services over internet such as software, hardware, data storage and infra-structure. The 4D password scheme, if successfully implemented here can make the cloud much safer and reliable.

V. CONCLUSION

In this survey paper we are discussed about different types of security techniques and area applications. In those days most of persons are suffered by the hacker. So by knowing of these techniques such as Human based, Computer based techniques, 3D, and 4DPASSWORD. We will easily save our credential data and any other hacker also couldn't find our information.

REFERENCES

[1] Miss Bhavana Borkar , Miss Shiba Sheikh, Prof. P. D. Kaware,"4D Password Mechanism" ISSN: 2454-1362.
[2]Grover Aman and Narang Winnie, "4D Authentication: Strengthening The Authentication Scene", in International Journal Of Scientific And Engineering Research (IJSER).
[3]Farnaz Towhidi and Maslin Masrom, "A Survey On Recognition-Based Graphical User Authentication Algorithms", in International Journal Of Computer Science And Information Security(IJCSIS).
[4] Harsh Kumar Sarohi and Farhat Ullah Khan, "Graphical Password Authentication Schemes: Current Status and Key Issues", in International Journal Of Computer Science Issues(IJCSI).
[5]Tejal Kongule,Yogundhara Thumbre and Snehal Kongule, "3D Password", in ICACACT.
[6] Duhan Puja, Gupta Shilpi, Sangwan Sujata and Guwati Vinita, "Secured Authentication:3D Password", in International Journal Of Engineering And Management Sciences(IJEMS).