ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 3; July-August-2015; Page No. 25-29

Comparative Study of 3-D Password and Textual Password

Surbhi Sharma[1], Manya Singhal[2], Sumitra Yadav[3]

Research scholar Computer Science & Engineering, Jyoti Vidyapeeth Women's, University, Jaipur, Rajasthan, India

surbhisharmass1992@gmail.com [1] manya95366@gmail.com [2] sumitra.mukesh27@gmail.com [3]

ARTICLE INFO

Received: 30 May 2015
Accepted 08 July 2015

Corresponding Author:

Surbhi Sharma

Department of Computer
Science and Engineering,
Jayoti Vidyapeeth Women's
University, Jaipur

Email:
surbhisharmass1992@gmail.com

Keywords: Cryptography, Authentication, biometrics, graphical passwords, multifactor, textual passwords, 3-D password, 3-D virtual environment.

ABSTRACT

Now days, authentication system have many problems such as textual passwords can be easily identified either by using brute force technique or by choosing meaningful words from dictionaries. To achieve this limitation many graphical password are available which take less memory space as compared to textual password. Also biometric system is used which may automate the identification or verification of an individual by identifying human characteristics. Multi factor authentication scheme is called 3-D password which represents the 3-D virtual environment of the various virtual objects. Interaction with objects takes place by the user through this environment. In 3-D virtual environment there is a sequence and combination of user interaction which is defined as 3-D password. 3-D password key space is defined by the design of 3-D virtual environment and type of objects selected.

INTRODUCTION

The security demand increases as the increment of computer usage. Authentication is the best method to validate the user to maintain the security. In this process we authorized the user to access the information. Major passwords like textual passwords, biometric scanning, tokens or cards (ATM) etc are provided for users. Encryption and decryption algorithms are used to secure the textual passwords. User validity can be proved by cards or tokens and identified by "natural" signature which is biometric scanning. Most of time textual passwords are kept in simple manner for ex-pet names, girlfriend names, phone no. which can be easily cracked. Long and random appearing password is difficult to remember for a user that's why they create simple, small and insecure passwords that can be easily hacked. Using graphical passwords makes the fact that user can easily recognized or remember pictorial data rather than words.3-D passwords not easily guessed by any attacker. To increase the security we use very interesting and more customizable authentication technique i.e. 3-D password. Human memory is the basic component in which the passwords depend. 3-D passwords are mainly used when there is need of high security.3-D stands for three domains which are defined as-

1. Acquirer Domain.
2. Issuer Domain.
3. Interpretability Domain.

When we access any secure site, the 3-D password GUI opens up.

An additional textual password security also implemented on this on which a user will go through the first authentication and then 3-D virtual room will open the screen. The choice of the 3-D password is totally depend on the user. It means the technique only the user choose is applicable for their password either it is face recognition, iris recognition or anything it totally depend on the choice of the user. Graphical passwords may go through a many number of complications. Execution time of some graphical passwords is high. Importantly when the users go through the process of authentication, passwords can easily be noted or observed by anyone and may suffer from attacks. For further enrichments and usability studies, many graphical passwords are still under research and development before they can be deployed in markets.

- **Graphical passwords**

Memorable location of image is chosen by the user in graphical password technique. Nature of the image and specific sequence of click locations may affect memory location. Human factors criteria are memory of passwords and their input's efficiency. Memory of passwords has two features:

How the password can be choosed and encoded by the user.

At the time of retrieving that password what the course of action has been done.

User will be represented at the time of retrieval either by recognition task or recall task depend on the graphical password system.

- **Multifactor**

To verify the validity of a transaction, this system requires more than one form of authentication. The primary objective of multifactor system is to create a defensive layer and make the situation worst for an unauthorized people to access the secret information. It develops two layers of authentication through which if one layer may be broke up then attacker has one more layer of authentication.

- **Textual passwords**

This authentication scheme is widely spread all over the world to verify the validity of the user. This protection is generally used on the internet or remote services. The most unsafe to attack scheme is textual password scheme. For ex- if someone implement a hidden camera or try to surf your password standing behind your shoulder then your password can be easily hacked.

Authentication

Authentication is the method in which we identify the identity of the user. In this procedure we confirm the identity of the person by validating their identity documents, verifying the validity of website through the digital signature, tracing the age of ruin by carbon dating, or the claim of packaging and labeling also ensured in it. In short, it includes verification of validity of at least one form of identification.

It is the task to verify the reality of the user's data or entity. In this procedure username and passwords are used to recognize an individual. It only ensures who is the user claims to be, but not says about their rights. Logon passwords are mainly used to complete this process.

Authentication techniques can be classified into 3 categories:

Knowledge based means what you know.

Token based means what you have.

Biometrics means what you are.

Knowledge-based authentication also divided into two types:

i) Recall based techniques in which a user repeat or recall a secret message that can be used before. For ex- Textual password.

ii) Recognition based techniques in which user can identify and recognize the secret message or a part of it that the user selected before. For ex- Face recognition, finger print.

Token based system depends on that in which a user has something to confirm individual identity. This system is commonly used by the banks as the use of credit or debit or ATM cards held by the user to access their accounts.

Biometric system depends on which a user is itself involved in the authentication process. An individual organ or whole body is included in authentication process.

Biometrics

It is the authentication scheme which is used to identify the characteristics or behavior of human beings. It can be used as an access control and identification form. These have different characteristics which may identify the individuals. These are classified into two categories which include Physiological and behavioral. Variety of different aspects encapsulated in biometric functionality. Selection of biometric system depends on some factors: 1) Universality: Trait can be accessed by everyone.

2) Uniqueness: The trait that should be used by the system must be unique to each individual.

3) Permanent: Constant trait should be used.

4) Measurability (Collectability): Measurement of the trait should be easier.

5) Performance: Accuracy, speed and robustness of the technology is calculated.

6) Acceptability: It depends on the individual's requirement.

7) Circumvention: It calculates that how easy a biometric factor followed.

Some biometrics schemes are- fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition. Each of them has its own pros and cons based on above factors. The main drawback of this system is that to authenticate user, it require a special scanning device which cannot be used for remote end internet users.

Two modes can be managed by this system:

Verification mode captured biometric compares by the biometric database template to authenticate the user successfully.

Identification mode, biometric database enforce one-to-many comparisons such that a new identity can be generated.

Accessing the system by the user for first time is known as enrollment. In this procedure, individual's information is captured and saved. Information that can be stored at the time of enrollment, detected and matched when the system used another time. Robustness of security in biometric system is essential during storage and retrieval of data. The coupling of 3-D passwords with biometric system can provide a higher level of security.

3-D passwords

3-D password is a new authentication technique which is more securable than textual, biometric, verification related methods. It is generally multifactor authentication scheme for assigning a password in which a virtual world is provided to the user where 3d objects should be adjusted. It mainly works on single 3-D virtual environment.

Fig 1- login process in a system

It can combine textual, recognition, recall, token and biometric systems into a single authentication scheme. Interaction and navigation is done by the user of the objects through this environment. The combination and sequence of user interactions occur in 3-D virtual environment is referred to as 3-D passwords. Objects that request to be recalling of information, reorganization of information, presentation of tokens and verification of biometrical data contained by designing a 3-D virtual environment.

Any object that can be encounter in real life is called virtual objects. Virtual objects in the virtual 3-D environment can perform actions and interaction towards the real life objects. In the 3-D virtual environment, any user input can be consider as a part of 3-D password such as speaking in a specific location. Some of the virtual objects can be described as:

The user's computer through which the user can type.

A fingerprint reader.

Biometric recognition device.

A white board or paper on which user an write, sign or draw.

Automated teller machine that reads tokens.

A light that can be switched on/off.

A television or radio.

A staple .

9) A car that can be driven;

10) A book that can be moved from one place to another;

11) Any graphical password scheme;

12) Any real-life object;

13) Any upcoming authentication scheme.

It is a procedure which is based on combination of multiple sets of factors. The design of the 3-D virtual environment and the nature of objects selected required for creation of 3-D password key space. It provides the high security to user because it combines the many authentication system. There are some requirements for particular authentication scheme:

Only recall or recognition is not ued in this scheme but it is a collaboration of many authentication schemes such as recall, recognition and biometrics.

2) Specification of the 3-D password should be freely chosen by the user. We have to consider that every individual has different needs, such as they don't want to carry cards or to present biometric system or may other have less memory which makes its greater acceptability.

3) The scheme is simple to the intended user to remember but complex to the attacker technique that should contain secrets.

Advantages 3-D passwords

Guessing of password is complex: Easy to remember for the user but not easy to guess for the hacker.

Paper writing is complex: writing password on paper is not easy that are provided to keep a secret in 3-D format.

Changes are easier: Scheme provided to keep a secret can be easily changed.

No sharing: Sharing of passwords with others is difficult.

Flexibility: Due to multifactor authentication it is more flexible.

Strength: There should be unlimited password provided in this scenario.

Privacy: Users privacy can also be held in selection of authentication by organizers.

3-D Password Applications

1 Critical server: Textual passwords are used to protect critical servers in many organizations. Textual passwords can be replaced by a sound proposed by 3-D authentication. To protect the entrance of locations and protect the usage of servers 3-D password authentication scheme is used.

2. Nuclear and military facilities: In these services, there is maximum need of security which can achieve

by the most powerful authentication systems. 3-D passwords contain probably high password space which is a good choice to increase the level of security based on knowledge-based system.

3. Airplanes and jetfighters: To avoid the miss usage of airplanes and jetfighters for religion or political agendas, we used a powerful authentication system. 3-D passwords became a very good choice for these systems.

Instead it only uses in critical system, it uses in simple systems also. It can be designed to implement into any type of systems such as ATMs, Personal digital assistants, Desktop computers and computer login, web etc. authentication.

3-D virtual environment

Fig2- A view of real virtual environment

It can include many objects and items to which the user may interact. Variation in interaction type from one to another item. Observing the actions and interaction of user and by observing the sequences of action can be used to develop a 3-D password. Usability, effectiveness and acceptability affected by the designing of well-studied 3-D virtual environment in 3-D password system. Administration and security requirements reflected by the designing of 3-D virtual environment to create a 3-D password system.

Designing can be done by using the following guidelines:

Similar to real life: The reality visualization of people is affected by the 3-D virtual environment. Virtual objects relatively similar to real life objects such as scaled sized in virtual environment. Real life situations reflection should be done by possible actions and interactions towards virtual objects and these object response maximaly real. User can interact with 3-D virtual environment by using common sense is the major objective of this system.

Distinction and soleness of object: Every object or item in 3-D virtual environment has its own uniqueness and different from other virtual object or items. Uniqueness refers to as every object has its own properties for ex- size, position etc. So, the user perspective on object1 interaction is equal to the object2 interaction. For ex- an organization is having 20 computers in place may confuse the user. So, the every object is different from other object during the designing of 3-D virtual environment. In simple the numbering of homes that look like each other and if not numbered would be difficult to distinguish which house was visited a month ago is the real life example. In this way, during the designing of 3-D virtual environment, the navigation and distinguishing between the objects should be easy. Recognition, usability of objects highly improved by distinguishing factor.

Size of 3-D virtual environment: City or even the world can be depicted by the 3-D virtual environment. Also, Space as focused as single room and office is also depicted by 3-D environment. There should be greater need to carefully study of size of 3-D environment. The requirement of time to perform a 3-D password by the user increased by the large 3-D virtual environment. Large number of virtual objects contained by large 3-D virtual environment. It can be space broadens. Only few objects can be contained by small 3-D virtual environment and also take less time while performing 3-D password.

Number of objects: Designing of 3-D virtual environment include identifying the types of objects and how many types' objects are included in this environment. Response of objects determines the type of objects. Textual password or a fingerprint considered as an object response type for making it simple. Password space of 3-D password affected by the selection of types and number of objects.

Importance of system: The type of system which protected by the 3-D password should be considerable for 3-D virtual environment. Importance of system measured by the types and number of objects used in 3-D virtual environment.

Conclusion

Increment of codeword length or aut5hentication key's length in virtual 3-D environment due to number of series of action and interaction in 3-D password system. The memory required for 3-D passwords is high as compared to textual password but it is more secure than textual password. A special training is required to user for using this system. In today's time there is high demand of security. According to user's preferences and requirements we need to choose the authentication system. An individual make prior choices to remember a password which may be textual or graphical instead of 3-D password. Choosing of smart cards as their 3-D passwords because it may difficult to user to recall textual passwords. To construct preferred 3-D password there is need to user's choice and decision.

References

1. IEEE-Three Dimensional Object Used for Data Security (Ms. Vidya Mhaske-Dhamdhere , Prof. G. A. Patil).
2. IEEE-Three-Dimensional Password for More Secure Authentication (Fawaz A. Alsulaiman and Abdulmotaleb El Saddik).
3. ijater- 3d password: minimal utilization of space and vast security coupled with biometrics for secure authentication (ms. nidhi maria paul, ms. monisha shanmugham)
4. I.J.E.M.S.- SECURED AUTHENTICATION: 3D PASSWORD (Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita)
5. http://www.slideshare.net/saddam12345/3d-password-23-mar-14