Authentication Using Three Phase Password

Hajisha1, Kanika Jain2, Meenu K.M.3, Mumthas K.P.4, Harikrishnan G.R.5
1,2,3,4Student, Department of Computer Science, MES College of Engineering, Kuttippuram, INDIA
2Assistant Professor, Department of Computer Science, MES College of Engineering, Kuttippuram, INDIA

ABSTRACT
Authentication is necessary in any system as it provides more security to that system. Current authentication techniques such as textual passwords, biometrics and graphical passwords have several limitations and disadvantages. To overcome the drawbacks of these techniques, we propose a new improved technique is used called the Three-Phase Password. Three Phase password is a multifactor authentication scheme. In this technique, we implement the password as a combination of textual password, graphical password and the co-ordinate position. Three-Phase Password is an advanced authentication scheme and is more secure than other authentication techniques. This paper presents the working and implementation of Three-Phase Password and also shows how this technique is more secure than the existing authentication scheme.

Keywords— Three-Phase Password, textual password, graphical password, co-ordinate position.

I. INTRODUCTION

Authentication is the process of confirming the identity of a user. It might involve confirming the identity of a person by validating their identity documents or verifying the validity of a Website with a digital certificate and labeling claim to be. In other words, authentication generally involves verifying the validity of at least one form of identification.

The advancement of technology, the Internet, and information sharing has both positive and negative impacts. One of the negative impacts was the large increase in new “information” threats. Many of the computer incidents exploited confidential information being stored by companies in a variety of different industries. The ability to carry out threats against information systems has been made easier due to the sharp increase in system vulnerabilities. Unauthorized access to confidential information was also the result of weak or non-existent information security practices. Not identifying and mitigating risks is a leading cause of unauthorized access and the exploitation of vulnerabilities.

Traditionally, computer facilities have been physically protected for three reasons:
• To prevent theft of or damage to the hardware
• To prevent theft of or damage to the information
• To prevent disruption of service

Security of a system is its ability to protect information and system resources in terms of their confidentiality and integrity. Human factors are considered the weakest link in a computer security system. Generally there are three major areas where the interaction between human and computer is important: authentication, security operations, and developing secure systems. The most common computer authentication method used is when a user submits the username and the password. One of the main problems is the difficulty in remembering the passwords.

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource, which should be kept secret from those not allowed access. Generally, the human authentication techniques [1] can be classified as knowledge based, token based, and biometrics. Knowledge based authentication techniques can further be divided into classes namely the recall based techniques and the recognition based techniques.

Token based technique means what you have. This may include ATM cards, credit cards, smart cards etc. Biometric based technique refers to what you are. This may include fingerprints, face recognition, iris scan, voice recognition etc. Knowledge based technique means what you know and it is the most widely used authentication technique which includes both textual passwords and graphical passwords. In the Recall based technique, the user repeats or reproduces the secret that has been created in the registration phase, e.g. textual password. In the Recognition based techniques, the user identifies and recognizes the secret or part of it that the user has selected during the registration phase, e.g. graphical password. Textual password which is the most commonly used authentication method has several vulnerabilities including the dictionary attacks, shoulder surfing attacks, eyes dropping etc. Users
tend to pick short passwords or passwords that are easy to remember, but unfortunately these can be guessed or broken [2]. Most organizations specify password policy that sets requirements for the composition and usage of passwords, typically dictating minimum length, required categories, prohibited elements. Graphical passwords are based on the idea that users can remember images better than words. Some graphical password schemes require long time for their completion. Most of the graphical passwords can be easily observed or recorded while the authorized user is performing a graphical password.

Based on our study, we conclude that the existing authentication schemes have certain limitations or drawbacks. We have introduced a new authentication technique which is based on the previously existing authentication techniques to overcome their limitations.

Combination of the above mentioned schemes is called the Three-Phase Password scheme or the multifactor scheme. In this scheme, the password is constructed as a combination of the textual password, graphical password and the coordinate position. The more number of password schemes used by the user will ensure greater security. Therefore, it becomes much more difficult to guess the user’s password for the attacker.

The contributions of this work are
1. Related work in this field.
2. System model which includes proposed system and its architecture.
3. Implementation of the proposed authentication scheme in the system.
4. System analysis which focuses on how the system overcomes the different attacks.
5. Discussion which shows the results of the survey.
6. Conclusion and the future work.

II. RELATED WORKS

Different authentication schemes have come into existence today. They are classified into knowledge based, token based and biometrics.

In knowledge based scheme, most commonly used method is textual password. Security of this comes from the fact that, they can be lengthy and random. But so far these passwords can be easily guessed when they are too short. As a result, it can be easily subjected to eavesdropping, shoulder surfing, social engineering etc. Token based scheme consists of something that user owns, which can be ATM cards, credit cards etc. Biometrics mainly include iris scan, thumb.

Dhamija and Perrig [3] proposed a graphical authentication scheme. In this technique, the user needs to choose a certain number of images from a set of random pictures during registration. At the time of login the user needs to recognize the image that has been chosen before.

Another recognition-based graphical password technique is Passfaces [4]. This technique works by having the user select a subgroup of $k$ faces from a group of $n$ faces. To ensure authentication, the system shows $m$ faces and any one of the faces belongs to the subgroup $k$. The user has to perform the selection several times in order to complete the authentication process.

Another scheme is the Story scheme [5], in which the user has to select pictures or objects (people, cars, foods, airplanes, sightseeing etc.) to form a story line.

Jermyn et al. [6] introduced a technique known as Draw-a-Secret (DAS) which is highly vulnerable to shoulder surfing. In this, the user needs to re-draw the picture that has been defined before on a 2D grid. The user becomes authenticated when the drawing touches the same grid in same sequence.

Haichang designed a new technique that enables user to draw a curve across their password images orderly instead of clicking on them directly. This scheme prevents shoulder surfing to some extent.

Goldberg introduced a technique named as “passdoodle” [7][8]. This is a graphical password authentication scheme that enables user to draw handwritten design or text with a stylus onto a touch sensitive screen.

Blonder [9] developed a new graphical passwords scheme where the user can select touch regions of the image which was defined before. As a result graphical password can be generated from the sequence and location of the touched place.

Syukri designed a technique for authentication in which the user draws his signature by mouse. It consists of two phases, registration and verification phase. During the registration stage the portion of the user signature previously drawn will be extracted. In the verification phase, user signature is taken as input and performs normalization and then extracts the parameters of the signature.

III. SYSTEM MODEL

A. PROPOSED SYSTEM

The Three-Phase Password authentication scheme can combine the different existing authentication schemes into a single environment. Which type of authentication techniques will be part of the user’s choice. Moreover, giving user the freedom of choice as to what type of authentication schemes will be part of their Three-Phase password increases the usability of the system.

Three-Phase password technique is the combination of recall based (i.e. textual password, etc.) recognition based (i.e. graphical password [10] etc.), so that multifactor and multi password are the another names for Three-Phase password authentication scheme. Token based schemes are vulnerable to theft and loss as well as to other attacks. Biometric scheme is efficient over shoulder surfing attack but is not resistant to certain other attacks.

It is very difficult for the intruders to guess the Three-Phase password and also it is difficult to observe the password while user is providing it, as user clicks on some images in a definite sequence or choses the coordinates of an image. So it is not easy for observer who wants to hack the user’s account to observe the whole sequence of Three-Phase password. If we assume that observer somehow gets known about some clicks of the password, still he or she can’t get access to user’s account because if the attacker is not able to guess the correct password in certain number of
trials, the account gets locked. In this way, the intruder cannot access the user’s account in any way.

Proposed system helps different types of users to store their data according to the security they need. For highly confidential data, the user can use combination of all the 3 techniques. For other data, user can use the authentication scheme that the user finds appropriate in order to ensure security to the data.

Some of the objectives of proposed system are:
- To provide a more secure authentication scheme to the system than the existing one.
- To give user the freedom of selecting more than one password scheme in a single system.
- To develop a more user friendly authentication scheme.
- To design a system that overcomes the limitations of the existing authentication schemes.

**B. SYSTEM ARCHITECTURE**

In this section, we will see how to create Three-Phase password and what are different schemes used to form a complete Three-Phase password. As we know, Three-Phase password is multifactor and multi password authentication scheme, many password schemes like textual password, graphical password can be used as a part of Three-Phase password. Choosing one of the schemes from different authentication schemes is based on category of the user who is going to the system. Fig. 1 shows the state diagram of creation of Three-Phase password.

As illustrated in the figure, the user initially enters the textual password. If the textual password is correct, the user enters the environment. If the user has registered the graphical password, the user enters the graphical password by selecting a sequence of images in a certain order. If the user has entered the position based password, he is asked to enter the select co-ordinates. If both these passwords are correct, the user is granted access to the account. In case if any one of these passwords is incorrect, the user is redirected to the login page.

![State diagram of Three-Phase Password creation](image)

**IV. SYSTEM IMPLEMENTATION**

Three-Phase password key space is determined by the design of the environment and the sequence of images and the co-ordinate position selected. To create his or her account user has to fill up his or her profile details like user name, textual password, email ID etc. After giving the profile information, user moves in environment.

In the case of graphical password, user enters into an art gallery. The art gallery consists of many images. User has to select a set of images in a certain order from the art gallery as in fig 2. The sequence in which user has selected the images is stored in database in the encrypted form. In this way the graphical password is set or created for the particular user. Next time when the user wants to access his or her account, he/ she has to select all the images which the user has entered at the time of creating password in the correct sequence. This sequence is then compared with the sequence which is stored in the database.
In the case of creating the position based password, the user is asked to select a pair of \((x, y)\) co-ordinates from an image as in fig 3. Next time when the user has to access his/her account, the user has to select the same co-ordinates. These co-ordinates are compared with the co-ordinates which is stored in the database. Access is thus granted to the authorized user if authentication gets successful.

Working of Three-Phase password is shown in fig. 4 which depicts the flowchart for Three-Phase password creation and authentication process.

When the user logs in with his/her credentials, an environment is displayed to the user and the user can interact with it. When the user interacts with the environment, an interaction sequence is generated. This sequence is registered with the user ID with which the user logs in. The user credentials are accepted and stored in the database. This interaction sequence is compared with the interaction sequence generated by the corresponding user at the time of registration. If this comparison is successful, authentication is verified and the user is granted access to different applications such as emails, files etc.

Using this system, different types of users can store their data in a secure manner. The authentication schemes used for creating the password depends on the user’s preference to ensure security. If the user has to store a highly confidential data, the user can use combination of all the schemes for password. If the user does not need high security for storing the data, he/she can use either the graphical password or the position based password.
V. SYSTEM ANALYSIS

To analyse and study how secure a system is, we need to consider how hard it is for the attacker to break the system. On the basis of the information content of a password space, a possible measurement can be done.

A. SECURITY ATTACKS AND COUNTERMEASURES

We have to consider all possible attack methods to realize and understand how far an authentication scheme is secure. In this section, we try to cover most possible attacks and whether the attacks are valid or not. Moreover, we try to propose countermeasures for such attacks that prevent such attacks. [11].

1. DICTIONARY ATTACK: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems, because user have to select the correct graphical and object based password in every login session.

2. SHOULDER SURFING ATTACK: The attacker uses camera to record the user’s Three-Phase password or tries to watch the legitimate user while the Three-phase password is being performed in this kind of attack. In this case, even if the user is successful in obtaining one password, the user cannot still access the account unless all the passwords match [12] [13].

3. BRUTE FORCE ATTACK: The attacker has to try all the possibilities of Three-Phase passwords in this kind of attacks. So it is hard to break our system by guessing the passwords.

4. WELL STUDIED ATTACK: The attacker has to study whole password scheme in this kind of attack. The attacker tries combination of different attacks on scheme after studied about scheme. As Three-Phase password authentication scheme is multifactor and multi password scheme, so attacker fails to study whole schemes. This attack is also not much effective against Three-Phase password scheme.

5. TIMING ATTACK: The attacker observes how much time is required for completion of successful login by the authorized user using the Three-Phase password scheme in this type of attack. Timing attacks can be effective if the scheme used for authentication is poorly designed. This kind of attacks is not easily possible on Three-Phase password scheme, because the Three-Phase password scheme is designed more securely.

6. KEY LOGGER: In this kind of attack, attacker installs software called key logger on the system where authentication scheme is used. This software stores the text entered through keyboard and this text is stored in text file. This attack is more effective only in the case of textual password scheme. Hence this attack is not much effective in Three-Phase Password scheme because Three-Phase password is a multi password authentication scheme.
Overall, we believe it is more difficult to break our system using the traditional attack methods like brute force search, dictionary attack, and shoulder surfing attack[14].

**B. APPLICATIONS**

Three-Phase password can be used in many areas where more security is needed to the system, as Three-Phase password authentication scheme is more useful and more secure than the existing authentication schemes. Three-Phase password’s main application domains are protecting critical systems and resources, because Three-Phase passwords can have a password space which is very large as compared to the other authentication schemes.

1. **NETWORKING:** Networking involves many areas of computer networks like critical servers, etc. Three-Phase password can be used to provide more security to the server. To ensure that the data or other important files are more secure from unauthorized users, it is an efficient and a secure way.

2. **NUCLEAR and MILITARY AREAS:** We can use Three-Phase password scheme in the areas for providing more secure authentication as nuclear and military areas of a country are the most important areas where security must be ensured. Three-Phase password scheme can protect data or secrete information about these areas. Three-Phase password authentication scheme is a good choice for high level security locations.

3. **OTHER AREAS:** The Three-Phase password authentication scheme has wide areas of application. We can use Three-Phase password authentication scheme in areas like ATMs, cyber cafes, in industries for data security, web services and much more.

**VI. DISCUSSION**

We conducted a survey and the study produced some distinct results. We observed the following regarding textual passwords, Three-Phase passwords, and other authentication schemes.

1) Most users who use textual passwords of 9–12 character lengths or random characters as password have only one to three unique passwords.

2) More than 50% user’s textual passwords are eight characters or less.

Three) About 25% of the users use meaningful words as their textual passwords.

4) 75% of users use meaningful words or partially meaningful words as their textual passwords. Only 25% of users use random characters and letters as textual passwords.

5) 95% of users on which the study has been performed, have never used any graphical password scheme as means for authentication.

**VII. CONCLUSION**

In this paper we proposed three authentication techniques that are based on text, images and co-ordinate positions for PDAs. There are many authentication schemes available in current state. But as we discussed before, these existing authentication techniques are vulnerable to certain attacks. The Three-phase password is a multifactor authentication scheme that combines benefits of various authentication schemes into a single environment. It does not require any special type of registration during login time. We are mainly focusing on user’s purpose and user’s needs, so it is 90% user friendly system. Shoulder surfing attack is still possible so how to overcome that is the field of research and development.

**REFERENCES**


