International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

3-Level Password Authentication System

Lalu Varghese[1], Nadiya Mathew[2], Sumy Saju[3], Vishnu K Prasad[4]
[1,2,3,4]*Department of Information Technology, Amal Jyothi College of Engineering, Kanjirappally, Kerala, India*

***Abstract*—In the current state there are many authentication schemes and most of these suffer from many weaknesses. Some of them are based on the physical and behavioral properties of the user, and some others are based on knowledge of the user such as textual and graphical passwords. Furthermore, there are other authentication schemes that are based on tokens, such as smart cards i.e., based on what you have. Among the various authentication schemes, the most commonly used schemes are textual password and token-based schemes, or the combination of both. However, both these authentication schemes are vulnerable to certain attacks.**

In this paper, we present a 3-level password authentication scheme, which is a multi-factor authentication system. To be authenticated, this project plans to present a 3-level password system by combining the features of the existing authentication schemes. The three different levels used in the 3-level password authentication scheme are image ordering, color pixels and the one time password (OTP).We use different hash functions such as SHA-1,MD5 for the generation of OTP.

***Keywords*—Authentication, graphical passwords, multifactor, textual passwords, 3-level passwords, image ordering, colour pixel, one time password, SHA-1**

I. INTRODUCTION

In a computer security system human factors are considered as the weakest link. However, there are three major areas where human-computer interaction is important: authentication, developing secure systems and security operations. Here the main focus is given to the authentication problem.

One of the most common computer authentication method is for a user to submit a user name and a text password. But the vulnerabilities of this method is plenty. One of the main problems that could arise is the difficulty of remembering passwords. Studies have shown that users usually tend to pick short passwords so that the passwords are easy to remember. Also, these passwords can also be easily guessed or broken.

The huge increase of computer usage has given rise to many security concerns, out of which the major security concern is authentication. Authentication is a process of validating who you are to whom you claimed to be [1].

Human authentication techniques can be classified as knowledge based i.e., what you know. Knowledge-based authentication can be further classified as :

1) Recall based technique, which require the user to repeat or reproduce a secret that the user created before. One of the common example for recall based authentication scheme is textual passwords. One of the major limitation of textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

2) Recognition bases technique, which is a sub-division of Graphical passwords. Graphical passwords show how the user can recall and recognize pictures better than words. Some of the graphical password schemes requires a long time to be performed. Its major disadvantage is that while the user is performing the graphical password, it can be easily observed and recorded by an intruder and thus it is vulnerable to shoulder surfing attacks.

The 3-level password system is a multifactor authentication scheme. It combine the benefits of existing authentication schemes to form the 3-levels of secure password. The 3-level of password is constructed using the exciting features of the current authentication systems such as image ordering, colour pixels and one time password.

II. OVERVIEW OF THE AUTHENTICATION TECHNIQUES

The currently used authentication schemes can be divided into three main areas:

Token Based Authentication: Token based techniques, use tokens such as key cards, bank cards and smart cards that are widely used by everyone. Most of the token-based authentication systems also use knowledge based techniques to enhance the security of the system. The use of ATM cards together with a PIN number can be stated as an *example*

Biometric Based Authentication: Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted as this approach can be expensive, and the identification process can be slow and often unreliable i.e., it is not reliable since it is time consuming.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

These are the major drawbacks of this approach. However, this type of biometric based authentication techniques provides the highest level of security.

Knowledge Based Authentication: The most widely used authentication technique is the knowledge based techniques and it includes both text-based and picture-based passwords. The picture-based password techniques can be further divided into two different categories: recognition-based technique and recall-based graphical techniques. While using the recognition-based techniques, a user is presented with a sequence of images and the user passes the authentication by recognizing or identifying the images he selected during the registration phase [2]. A user is asked to reproduce something that he or she created or selected earlier during the registration stage, while using the recall-based techniques.

III. 3-Level Password Scheme

In this paper, we propose a multifactor authentication scheme that combines the benefits of the existing authentication schemes and thereby, overcomes the pitfalls of the currently used authentication schemes [1]. Below are some of the requirements we attempted to satisfy:

1) The new scheme stated should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall-based technique, recognition-based technique, image ordering, colour pixel selection and one time password.
2) Users ought to have the freedom to select the first two levels of password i.e. the selection of images and colour pixels in the same order in the first and second levels of password respectively. This freedom of selection is necessary as the users are different and each user may have different requirements. Hence, the user's freedom of selection is important to ensure high user acceptability.
3) The new scheme should provide easy to remember secret keys that are very difficult for intruders to guess.
4) The new scheme should provide secret keys that are difficult to share with others and which are not easy to write down on paper.
5) The new scheme should provide secret keys that can be easily changed or revoked.

Based on the aforementioned requirements, we propose our contribution, i.e., the 3-Level password authentication scheme. The three main levels of the authentication system are described below.

A. *Image Ordering*

The first level i.e., the image ordering simply means the selection of previously set images in the same order. From a sequence of images, the user can select few images at random. The images provided are commonly used, user friendly and easy to remember images. For example, we can set a count, say three. So the maximum limit of image selection will be set to three images. During authentication phase, the sequence of images will be given in a shuffled order, from which the user selects the same set of images chosen during registration phase in the same order. In case of any invalid selection of images, the system will be locked automatically after few trials based on the count given.

Fig 1: Image Ordering

B. *Colour Pixels*

After image ordering, we move to the second level i.e., the selection of colour pixels. The user can select a single colour pixel from the different blocks of colours provided. For example, we can set a count, say one. So the maximum limit of colour pixel selection will be set to one. During authentication phase, the previously set images should be chosen in the first level and then the user will be redirected to the second level i.e. the colour pixel selection, where the user selects the same colour pixel chosen in the registration phase. In case of any invalid selection of images or colour pixel the system will be locked automatically after few trials based on the count given.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

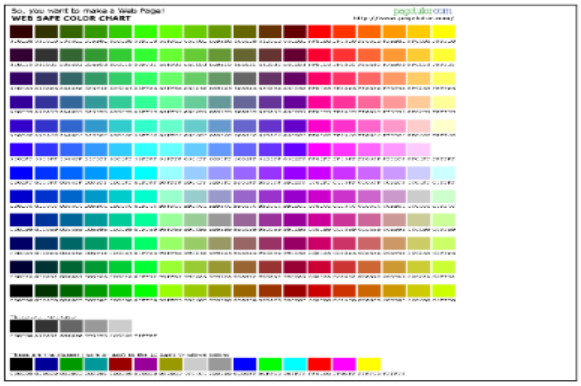

Fig 2: Colour Pixel

C. One Time Password

In the Third level, we make use of one time password (OTP) that is a password which is valid for a single session. We securely generate and verify the OTP using Smartphone. The generated OTP can be send to a mobile phone in the form of SMS as SMS messaging has a high potential to reach all the customers with a low total cost of ownership or Smartphone can be used as token or platform for creating OTP [3]. Thus we can call it SMS OTP or OTP generated through Smartphone the OTP generated will be valid only for a short period of time and it is generated and verified using Hash Functions and Secured Cryptographic Algorithm such as SHA-1. The system we proposed been implemented and tested successfully.

Security is one of the major concerns today in almost all sectors such as banks, governmental applications, military organization, educational institutions, etc. The passwords are the commonly found weak links when it comes to security concerns in these numerous and varying industries as it is the most common type of credential used today. So to avoid the tedious task of remembering difficult and lengthy passwords, users often use weak passwords which are easy to remember. Such passwords will have security issues such as management security concerns. Users commonly use easy-to-guess passwords, and they also tend to use the same password in multiple accounts etc. Moreover, the hackers use many techniques such as shoulder surfing, snooping, guessing, sniffing, etc. to steal passwords. Furthermore, these passwords can be written down, forgotten and stolen or even guessed deliberately being told to others.

At present several proper strategies has been proposed for using different kinds of passwords. Out of which, some of them are very difficult to use and some might not meet the necessary security concerns.

Some solutions have been developed to help the users to create and manage their passwords. A more secure solution would be giving the user a hardware token such as a Smartphone for generating one-time-passwords, i.e. passwords that are valid for a single session or transaction. Moreover, there are many disadvantages in using tokens due to some factors like the cost of purchasing, issuing, and managing of these tokens. The customer might also find it difficult to carry multiple tokens since it could be lost or stolen.

In this paper, the proposed OTP is generated by providing the necessary inputs which is encrypted and appended as a single string. Then we use popular hash functions such as SHA-1, MD5 to generate a secure hidden OTP in the web part. At the application side, the same input is provided so as to get the same output i.e., generated OTP in the web part. If the OTP generated in the web part matches with OTP generated in application side i.e., if it is valid, the generated OTP will be sent as an SMS to the users Smartphone with which he logins. If the OTP generated is not valid i.e., if the hidden OTP does not match with the OTP generated at the application side, the session will be dismissed. The major advantage of the system is that, different OTP is generated each time the user tries to login.

The generated OTP must be difficult-to-guess, retrieve or trace by hackers so as to make the system more secure. So we should develop secure OTP generating algorithm which can use several factors to generate hard to guess passwords. Hence we propose a Secured Cryptographic algorithm since the users tend to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments.

Hash Functions

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any accidental or intentional change to the data with very high probability will change the hash value. The data to be encoded are often called the message, and the hash values are sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main properties:

1) It is easy to compute the hash value for any given message
2) It is infeasible to generate a message that has a given hash
3) it is infeasible to modify a message without changing the hash

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

4) It is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called digital fingerprints, checksums, or just hash values.

Most cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length hash value. A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. At a minimum, it must have the following properties:

- *Pre-image resistance*

Given a hash *h* it should be difficult to find any message *m* such that h = hash(m). This concept is related to that of one-way function. Functions that lack this property are vulnerable to pre-image attacks.

- *Second pre-image resistance*

Given an input m_1 it should be difficult to find another input m_2 such that $m_1 \neq m_2$ and $hash(m_1) = hash(m_2)$. Functions that lack this property are vulnerable to second pre-image attacks.

- *Collision resistance*

It should be difficult to find two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for pre-image resistance; otherwise collisions may be found by a birthday attack.

These properties imply that a malicious adversary cannot replace or modify the input data without changing its digest. Thus, if two strings have the same digest, one can be very confident that they are identical. A function meeting these criteria may still have undesirable properties. Currently popular cryptographic hash functions are vulnerable to length-extension attacks: given hash(m) and len(m) but, by choosing a suitable m' an attacker can calculate hash(m || m') where || denotes concatenation. This property can be used to break naive authentication schemes based on hash functions.

One of the major applications of hash functions is verifying the integrity of files or messages i.e., an important application of secure hashes is the verification of message integrity by ddetermining whether any changes have been made to a message For this reason, most digital signature algorithms only confirm the authenticity of a hashed digest of the message to be "signed". Verifying the authenticity of a hashed digest of the message is considered proof that the message itself is authentic.

A hash function must be able to process an arbitrary-length message into a fixed-length output. This can be achieved by breaking the input up into a series of equal-sized blocks, and operating on them in sequence using a one-way compression function. The compression function can either be specially designed for hashing or be built from a block cipher. A hash function built with the Merkle–Damgård construction is as resistant to collisions as is its compression function; any collision for the full hash function can be traced back to a collision in the compression function. The last block processed should also be unambiguously length padded; this is crucial to the security of this construction. This construction is called the Merkle–Damgård construction. The construction has certain inherent flaws, including length-extension and generate-and-paste attacks, and cannot be parallelized.

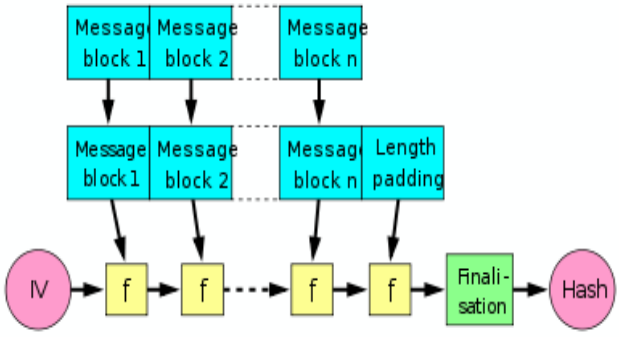

Fig 3: Merkle–Damgard hash construction.[4]

SHA-1

This standard specifies a Secure Hash Algorithm (SHA), which is necessary to ensure the security of the Digital Signature Algorithm (DSA). When a message of any length $< 2^{64}$ bits is input, the SHA produces a 160-bit output called a message digest. The message digest is then input to the DSA, which computes the signature for the message.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

Signing the message digest rather than the message often improves the efficiency of the process, because the message digest is usually much smaller than the message. The same message digest should be obtained by the verifier of the signature when the received version of the message is used as input to SHA. The SHA is called secure because it is designed to be computationally infeasible to recover a message corresponding to the message digest. Any change to the message in transit will, with a very high probability, result in a different message digest, and the signature will fail to verify.

IV. Conclusion And Future Work

In the current state there are many authentication schemes. Some of the schemes are based on the physical and behavioral properties of the user, and some other authentication schemes are based on the knowledge of the user such as textual and graphical passwords. Also, there are other authentication schemes that are based on tokens such as smart cards i.e., based on what you have [1]. Among the various authentication schemes, the most commonly used schemes are textual password and token-based schemes, or the combination of both.

The 3-level password is a multifactor authentication scheme that combines the features of various authentication schemes. The first level is the image ordering, where the user selects the same images in the same order as selected in the registration phase. The second level is the colour pixel selection, where the user selects a single colour pixel.

The most secure level is the third level, which is the generation of one time passwords. The hidden OTP generated in the web part is compared with the OTP generated in the application side and if they are valid i.e., if both the OTPs generated are same , then the generated OTP will be sent to the smartphone of the user as an SMS, with which the user logs on to the system.

One of the future works will be gathering attackers from different backgrounds to break the system which will lead to system improvement and will prove the complexity of breaking the system. But still the attackers will acquire the knowledge about the system and will try to launch their attacks. Shoulder surfing attacks is a limitation against the 3-level password system. Therefore, a field of research would be a proper solution.

REFERENCES

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE 2008 Three-Dimensional Password for More Secure Authentication

[2] X. Suo, Y. Zhu, and G. S. Owen, “Graphical passwords: A survey,” in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Sagar Acharya1, Apoorva Polawar2, P.Y.Pawar. Student, Information Technology, Sinhgad Academy Of Engineering/ University of Pune. Two Factor Authentication Using Smartphone Generated One Time Password

[4] http://en.wikipedia.org/wiki/File:Merkle-Damgard_hash_big.svg