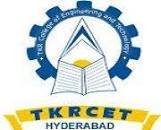
**WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM**



Literature Survey Report submitted in the partial fulfilment of the requirements for the award of the degree of

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE & ENGINEERING**

**by**

**V.Bhavagnya 19K91A05K0**

**V.Likhitha 19K91A05K2**

**S.Swetha 19K91A05H5**

**P.Priyanka 20K95A0534**

**UNDER THE GUIDANCE OF**

**Mrs.N.Chandrakala**

DEPARTMENT OF COMPUTER SCIENCE &ENGINEERING

**TKR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(AUTONOMOUS)**

(Accredited by NBA and NAAC with ‘A’ Grade)

**Medbowli, Meerpet, Saroornagar, Hyderabad-500097**

**CERTIFICATE**

This is to certify that the main project report entitled **WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM**, being submitted by Ms. **V.Bhavagnya**, bearing ROLL.NO:**19K91A05K0**, Ms**.V.Likhitha**, bearing ROLL.NO:**19K91A05K2**, Ms. **S.Swetha**, bearing ROLL.NO:**19K91A05H5**, Ms.**P.Priyanka**, bearing ROLL.NO:.**20K95A0534** in partial fulfilment of requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering, to the TKR College of Engineering and Technology is a record of bonafide work carried out by them under my guidance and supervision.

Name and Signature of the Guide Name and Signature of the HOD

Ms.N.Chandrakala Dr.A. Suresh Rao

**CONTENTS**

**1. INTRODUCTION 4**

**2. LITERATURE SURVEY REPORT 5**

2.1 Comparison Study: An Advanced Information Security System Using

Image Based Graphical Password Scheme

2.2 Click and Session Based—Captcha as Graphical Password Authentication Schemes for Smart Phone and Web

2.3 Evaluating Usability of Three Authentication Methods in Web-Based Application

2.4 Enhancement of Password Authentication System Using Graphical Images

2.5 Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods

2.6 Securing Web Accounts by Graphical Password and Voice Notification

2.7 Random Graphic User Password Authentication Scheme in Mobile Devices

2.8 A Secure Graphical Authentication System Using Watermark Embedding

2.9 Two-way Graphic Password for Mobile User Authentication

2.10 A New Secure Authentication Scheme for Web Login Using BLE Smart Devices

2.11 Authentication by Graphical Passwords Method ‘Hope’

2.12 PassPositions: A Secure and User-Friendly Graphical Password Scheme

2.13Numerical Password via Graphical Input – An Authentication System on Embedded Platform

2.14 Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability

2.15 Directional Based Graphical Authentication Method

with Shoulder Surfing Resistant

**3. REFERENCES 41**

1. **INTRODUCTION**

User Authentication is an interaction that permits a gadget to approve the character of an individual who associates with network assets. Commonly textual passwords are the most used form of authentication for all websites and applications. Textual passwords consist of a string of characters which may also include special characters and numbers. In most cases, users may use only one username and password for multiple accounts. But they are not fully secured. So, we should maintain strong passwords, comprising numbers, uppercase, and lowercase letters. Then these textual passwords are considered strong enough to resist brute force attacks. However, a strong textual password is hard to remember and recall. Along these lines clients will in general pick passwords that are either short or from the word reference, instead of irregular alphanumeric strings. Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication. Shoulder surfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device. A strong textual password is hard to memorize and recollects. To avoiding such problems, we are presenting a secure graphical web-based authentication system that protects users from becoming victims of shoulder surfing attacks.

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words . Also, they should be more resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques . In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or select earlier during the registration stage.

**2. LITERATURE SURVEY REPORT**

**2.1** **An Advanced Information Security System Using**

**Image Based Graphical Password Scheme**

Title: Comparison Study: An Advanced Information Security System Using

Image Based Graphical Password Scheme

Published by:, K.Priya ,T.Venkaiah Naidu ,R.Vamsi Krishna.

Numerous security natives depend on hard scientific issues. Utilizing hard AI issues for security is developing as an energizing new worldview, yet has been under explored. In this Context, It describes another security crude in view of hard AI issues, to be specific, a novel group of graphical secret word frameworks based over Puzzle innovation, It can be called as Puzzle as graphical passwords (Captcha). Captcha is both a Puzzle and a graphical anonymous key arrangement. Captcha watches out for different security issues all things considered, for instance, online estimating attacks, hand-off strikes, and, if joined with two fold view headways, accept surfing surprise attack (Dictionary form). A Captcha riddle word can be discovered only probabilistically through altered on the web. Speculating strikes paying little respect to whether the mystery enter is in the chase set. Captcha likewise offers novel way to deal with address the outstanding picture hotspot issue in prevalent graphical secret key frameworks, for example, Pass Points, that frequently prompts delicate saying decisions. Captcha isn't a panacea, yet it offers sensible security and accommodation and appears to fit well with some effective applications for improving on the web security for example, Pass Points, that frequently prompts delicate saying decisions. Captcha isn't a panacea, yet it offers sensible security and accommodation and appears to fit well with some effective applications for improving on the web security.

**Related Work:**

Cyber-criminals have benefited from on-line banking (OB), regardless of the extensive research on financial cyber-security. To better be prepared for what the future might bring, to predict how hacking tools might evolve. Briefly survey the state-of-the-art tools developed by black-hat hackers and conclude that automation is starting to take place. To demonstrate the feasibility of our predictions and prove that many two-factor authentication schemes can be bypassed, developed three browser rootkits which perform the automated attack on the *client’s computer*. Also, in some banks attempt to be regarded as user-friendly, security has been downgraded, making them vulnerable to exploitation.

Two factor confirmation utilizing cell phones. The proposed technique ensures that validating to administrations, for example, internet managing an account or ATM machines, is done in an extremely secure way. The proposed framework includes utilizing a cell phone as a product token for One Time Password age. The created One Time Password is substantial for just a short client characterized timeframe and is produced by factors that are extraordinary to both, the client and the cell phone itself. Moreover, a SMS-based component is executed as both a reinforcement system for recovering the watchword and as a conceivable mean of synchronization.

Presents another security rough in light of hard AI issues, specifically, a novel gathering of graphical mystery key structures based over Puzzle technology, which call Puzzle as graphical passwords (DSA). Captcha is both a Puzzle and a graphical mystery key arrangement. Captcha keeps an eye on different security issues completely, for instance, electronic guessing ambushes, exchange attacks, and, if joined with dualsee progressions, bear surfing strikes. Prominently, a Captcha mystery key can be found just probabilistically by means of customized online hypothesizing attacks paying little heed to whether the watchword is in the request set. Captcha in like manner offers a novel method to manage address the picture hotspot issue in understood graphical mystery key systems, for instance, Pass Points, that every now and again prompts delicate watchword choices. Captcha isn't a

panacea, yet it offers sensible security and convenience and appears to fit well with some utilitarian applications for improving on the web security. Present excellent Captcha in view of both substance Puzzle and picture affirmation Puzzle. One of them is a substance Captcha wherein a mystery word is a gathering of characters like a substance watchword, however

entered by tapping the right character progression on Captcha pictures. Captcha offers protection against online vocabulary attacks on passwords.

Protection against online lexicon assaults is a more unpretentious issue than it may appear. Puzzle Login(top of Puzzle innovation Using numerical problems).Image Puzzle Solving Using AES Algorithm.

**AES ALGORITHM:**

The Advanced Encryption Standard AES is the most widely used encryption method for securely encrypting data and processing further by using a secure connection.

* National security agencies in many countries inclusive of India recommend using the 256-bit AES encryption algorithm for saving and sending crucial and sensitive data over secure communication channels.
* The military and other government agencies, **for example,** finance ministry, also use 256-bit AES encryption for data storage on day to day basis.
* AES algorithm is used in association with other cryptographic-based algorithms to boost the performance of the encryption process which is deployed for the transition of classified and sensitive information into encrypted form and exchange of the same.

**Examples of AES Algorithm Usage**

* Samsung and other manufacturers of storage devices, which are known as Solid Storage Devices (SSD), use the AES algorithm of 256-bit for saving the data.
* The data we store on Google drive is an example of the usage of the AES algorithm. The cloud on which the user data is stored and visible on Google uses AES encryption method. It deploys a 256-bit encryption method, which is considered a more complex and highly secured method.
* Facebook and WhatsApp messenger uses the AES encryption of 256-bit for securely transmitting and receiving the one-to-one message.
* The Microsoft BitLocker process of encryption, which is by default present in the Windows system, also uses 128-bit and 256-bit AES encryption processes.
* Internet of things (IoT) devices, self-encrypting software, and hard disk drives also use 128-bit and 256-bit AES encryption for the processing of data.

**Features of AES Algorithm**

* AES encryption jumbles plain text information into a kind of cipher code that the unauthorized and third person can’t understand even if they crack it before the information reaches its desired destination. At the receiving end, the receiver has their secret code to unjumble the data back into the original, understandable text.
* In this way, the AES encryption and decryption provisions protect crucial data from being intercepted by some unauthorized person or hacker and can be transmitted over the Internet through secure SSL channels. A fast-running example of exchanging such information is performing banking transactions through smartphones. It will be in encrypted form, and the information is visible to the user only.
* The AES algorithm implementation is very cost-effective, and it is easy to use. In addition to this, there is no copyright issue associated with it. Thus, can be used globally by any person and organization.
* The AES algorithm is easy to implement into software as well as hardware devices. It is very flexible.
* VPN (Virtual Private Networks) deployed in switch for LAN and WAN networks also uses AES encryption by directing the IP address to a secure server located at the far end. This works efficiently for open source networks.\

**CONCLUSION**

The objective of this paper is to give best security framework to online applications through picture confusing framework which can't be hacked through word reference attacks, online guessing attacks, relay assaults and so forth .The product astound might be based upon an information puzzle, it can be coordinated with any current server-side information perplex conspire, and effortlessly sent as the present customer baffle plans do. CAPTCHA is broadly slook into field go about as web rectifier to secure web applications by perceive human from bots. CAPTCHA exhibited which will enhance protection of math analytics CAPTCHA. By utilize, Boolean activities and articulations rather than trigonometric and differential capacity which will help in lessen the intricacy of CAPTCHA and help to accomplish better ease of use and security when contrast with math analytics CAPTCHA. Boolean CAPTCHA can be effectively use by taught client. No need of specialized expertise, by utilizing scholarly personality to fathom this CAPTCHA and help to diminish time many-sided quality.

**2.2 Click and Session Based—Captcha as Graphical Password Authentication Schemes** **for Smart Phone and Web**

Title: Click and Session Based—Captcha as Graphical Password Authentication Schemes for Smart Phone and Web

Published by: Vikas K. Kolekar, MilindKumar B. Vaidya

When we consider the online service or desktop application there is major issue of security breaching. Old password schemes has some drawbacks like hacking of password, shoulder-surfing attack as far as password is concern, online password guessing attack, relay attack. Hence there must be system that provides good solution for such password cracking

attacks. There are many solutions for it and various password schemes available that achieves this. The main drawback of these schemes is users have to deal with complicated and tedious steps as far as registration and login of user is concern as its logic contains some intense AI processes. These complicated AI processes are exhaustive for common user of the system. In this paper we propose authentication schemes which consist of graphical password based captchas. It consists of both a captcha and a graphical password schemes. To boost the security aspect to the next level, we contribute some captcha schemes that provide user high security at time of login. Our system provides choice of various authentication schemes to user at time of login. Along with these schemes session based authentication is also provided which will protect system from unauthorized access. We extend the use of captcha as human present recognition as well as graphical password hence it provides all benefits of captcha and make system more powerful from security point of view.

**Related Work :**

Clicked-based CaRP believe in following equation as far as an automatic guessing attack is concern.

*P(T* = *􀈡*|*T*1*, . . . , Tn-1)* = *P(T* = *􀈡),* 􀗊 *n* (1)

Here, 􀈡 be the password to find, T denote a trial. Whereas, Tn denote the nth trial, and *P*(T 􀈡) be the probability that 􀈡 is tested in trial T. According to equation (1) the chance of finding the password in the present trial always remains the same, no matter how many trials executed previously. Our proposed system adopts this approach. CaRP uses challenge images to guess password in authentication steps. Hence brute force attack and automatic guessing attack possibilities are minimized. To make password guessing more complex and

minimize dictionary attacks, system uses a technique in which for each password guessing trial different challenge images are used every time. As each challenge image has variant

information that keeps above equation (1).To generate CaRP challenge image we used visual

objects such as alphanumerical characters, similar animals. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories

as follows:

*A***. Recognition CaRP**

It requires recognizing a captcha challenge image and using the recognized objects as cues to enter a password by clicking on character objects.

*B***. Recognition-Recall CaRP**

It combines the tasks of both recognition and cued-recall and retains both the recognition-based advantage of being,easy for human memory and the cued-recall advantage of a

large password space.

1. **Basic Concept of CaRP**

There are two basic mode of transaction in CaRP. In one mode of transaction user registers and in another user tries to login both by using CaRP scheme. If validation fails then again user will redirect to login screen else user will get access to panel. Objects in a CaRP challenge image may overlap slightly with neighbouring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object. As a feature of CaRP, each time of login alphabets, characters, special characters and 2D animal images are fetched and randomly arranged and displayed in form of challenge image. Each time user will get different challengeimage containing password letters randomly arranged.

2. **Basic Steps of CaRP Challenge Image Generation:**

Following are the steps to generate random CaRP

challenge image:

**Step 1:** Here, firstly set of alphanumeric characters, special characters or images are defined. While creating CaRP challenge image these alphabets, numbers, images are used. In some cases these letters belongs to the password given by user.

**Step 2:** Create transparent CaRP challenge image with width ‘w’ by height ‘h’ image size.

**Step 3:** Add captcha text over it. For this used android canvas facility. In this, blank canvas is provided to the user. By passing these letters to the canvas function we created challenge image out of it.

**Step 4:** Export the final CaRP challenge image.

3. CaRP Schemes

There are two main categories of CaRP based

schemes.

1. Recognition based schemes.

2. Recognition-Recall CaRP.

ClickText, AnimalGrid and Shuffle

text belongs to recognition based schemes and Textpoints4CR

belong to recognition-recall based scheme.

**Scheme 1: ClickText**

This is a recognition based scheme with CaRP feature.This scheme comprises of randomly arranged characters in CaRP challenge image. Basic thumb rule is that challenge image should not contain any visual confusing characters like as “0” and “O” alphabet.

**Scheme 2: AnimalGrid**

In ClickAnimal scheme [1] user provide password which is sequence of animal names. User will get captcha challenge image in form of 2D animal images overlapped but their core parts are not occluded in order for humans to identify. User clicks on animals with respect to their password sequence. In this process password space is not so large hence based on this advanced AnimalGrid scheme is proposed. This scheme is combination of ClickAnimal and Click-A-Secret. In AnimalGrid scheme user will get CaRP challenge image containing 2D animals of different shape and size on it and number grid of 6X6, which having numbers in between 1to 100 of any combination placed alongside of 2D animal challenge image.

**Scheme 3: TextPoints4CR**

This is a recognition-recall based scheme. In this scheme, to enter a password, a user must trace the click points in a CaRP challenged image, and click the invariant points matching the password. In this case invariant point means a point in particular alphabet that has a fixed relative position in different fonts. User has to provide sequence of such invariant points by selecting particular alphabet at time of registration. When user wants to login then he will get CaRP challenge image containing registered alphabet. User has to trace and click relative positions in alphabet which he used at time of registration.

**CONCLUSION :**

We have used Captcha as a graphical password i.e. CaRP. With the correct use of image processing and AI techniques, we provide solution to online password guessing attack, dictionary attack, relay attack etc. In this system, CaRP challenge images are innovatively designed and their authentication servers are also managed properly. These schemes provide security as well as usability to user. These schemes are robust to shoulder-surfing attack as user will get different independent challenge images and multiple options for every login attempt. Application of existing system is used to offer reasonable security and usability and appears to fit well with some practical systems for improving online security. This concept is also useful for desktop applications. Practically we had applied such login schemes for android based smart phone application interfaces and web. We can apply Captcha as Graphical Password schemes where we have to provide security to extra sensitive data. Overall, we provided smart solutions as far as password security and attacks are concerned with the help of AI.

**2.3 Evaluating Usability of Three Authentication Methods in Web-Based Application**

Title: Evaluating Usability of Three Authentication Methods in Web-Based Application

Published by: Yao Ma and Jinjuan Feng

Effective user authentication is critical for protecting information and system safety. The most common computer authentication method is text password. Previous research suggests that text password can be hard to remember and userstend to create simple text password that is unsecure. Various password strategies and alternative authentication applications have been proposed, such as mnemonic password, graphical password, and biometrics. However, existing research on the usability of these authentication methods are limited. We conducted a longitudinal empirical study to examine the usability of three authentication methods: traditional text password, mnemonic password, and graphical password, in a real life environment. The result suggests that the graphical password took longer time for authentication and demanded higher work load than the text password and the mnemonic password**.**

**Related Work :**

**A. Authentication mechanisms**

Authentication mechanisms can be categorized into three groups: biometric authentication, token based authentication, and knowledge based authentication.

**Biometric authentication**:

It includes behavioral biometrics and physiological characteristics. The first group is based on features such as keystroke latency or signature dynamics. The second one studies physical characteristics such as fingerprint, voice or vein pattern. Although biometrics cannot be easily changed and is easy to manage, it has several flaws. First, existing biometric techniques are still pretty expensive, making it difficult for wide adoption. Second, the technique may not work well when the physical characteristic changes, such as the changed voice when someone catches a cold. Thirdly, biometric techniques are recognition based and recognition

errors may cause authentication problems. Biometric approach is not suitable for web-based authentication because additional devices are needed to read and interpret the biometric data.

**Token based authentication:**

Token based authentication relies on the token possessed by a particular user. An example of token is the bank cash card.Tokens can be easily stolen and used for malicious purposes. Similar to biometrics, they are not convenient for use in the web environment because special devices are needed.

**Knowledge based authentication:**

Knowledge based authentication can be divided into two categories: text based password and graphical password. Text based passwords include un-cued passwords and cued passwords. Un-cued passwords use a random sequence of characters and digits either generated randomly or selected by each user. Cued password relies on the memory of a concept or

a phrase that the user selected. Graphical passwords include recognition based passwords and position based passwords. 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 position based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage .

Due to the limitations of biometric authentication and token based authentication, knowledge based authentication is widely adopted in the web environment. In the following sections, we focus on knowledge-based authentication and discuss in detail recently developed methods, products, and related studies.

**B. Web-based Authentication Products**

Existing web-base authentication products fall into four

Categories

* Un-cued Password
* Cued Passwords
* Recognition based Password
* Position based Password

**Un-cued Password**

Random passwords, passphrase, and mnemonic passwords are un-cued passwords. Even though system assigned password is probably stronger, most systems and websites allow users to choose their own random passwords because users remember passwords better if they choose them . Another problem with random passwords is that users are frequently resort to writing down or sharing random passwords that are difficult to remember. In the most resent research by Richard who works on text password policy found that users are more likely to share and reuse their passwords than to write them down .

**Cued Passwords**

A challenge question asks a user for an answer to a personal question in an attempt to confirm their identity. Challenge questions are commonly used to authenticate users who have lost their passwords. Although challenge questions can also be used for the day-to-day authentication of an individual, it may be inconvenient for day-to-day authentication because it requires more time for authentication and is not as secure as text passwords.

**Graphical Passwords:**

They are the combination of the recognition based and position based passwords.

Both recognition-based password and position-based password are graphical password. Recognition based password requires the user to select target pictures among a set of distracters, which relies solely on visual memory. Position based password requires the user to identify target objects within an individual picture or draw a previously drawn object on a grid, which relies on both visual memory and spatial recall ability.

**C. Evaluation of Authentication Methods**

When considering which authentication methods to adopt, we need to consider both the usability and security aspects. The usability of an authentication method is typically measured by the amount of time required for authentication, the memorability of the password, and ease of use. The security aspect can be evaluated using the difficulty of guessing the password manually, the difficulty of brute force attack, and the difficulty of describing and sharing the key with others by the user. For authentication time, text based authentication is better than graphical based authentication. The authentication time consumed mainly depends on the authentication key size and the number of authentication pages. Images have bigger size than text, the key transfer between server and client will use

more time for graphical based authentication when the network transfer speed rate is certain. it was found that the Passfaces need more authentication time than password.

**Conclusion :**

The result suggests that the login time of the graphical passwords is significantly longer than that of the other two types of passwords. This might be due to two reasons. First, the loading time of the login page for the graphical password is longer due to the image files. Second, the participants needed to browse through the 30 images to find the three password images. Since the image order is always randomized, they have to browse through the images every

time they log in. Regarding login failure rate, the average failure rate of the mnemonic passwords is twice of that of the text passwords and graphical passwords. However, the difference is statistically non-significant probably due to large variance in the data. The higher average failure rate under the mnemonic condition is not consistent with the previous expectation that the mnemonic passwords improve memorabilility. The expected benefit of graphical passwords regarding memorability was not observed in the study because it had

similar average failure rate to that of the text passwords. In order to understand the underlying reason, we studied the text passwords that the participants created and used during the study. We found that most participants used very simple text passwords that were highly vulnerable for dictionary attack Consequently, the passwords were very easy to remember and therefore the login failure rate for text passwords is pretty low at the cost of security. If participants used more randomized text passwords that were more secure, the login failure rate may increase.

**2.4 Enhancement of Password Authentication System Using Graphical Images**

Title: Enhancement of Password Authentication System Using Graphical Images

Published by: Amol Bhand,vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke)

As we all are familiar with web authentication. So initially all the web authentication was done on the basis of text password. Text password was the only system used for authentication system. But as time goes on this system finds many disadvantages to use it. As like this was not trusted as it had always threat of getting hacked. Text password was always tested the memory of the user, so it wasn’t good system. Then invention of biometric authentication system, QR codes and 2 step mobile verification invented to overtake the disadvantages of the text based password. But these systems had also some drawbacks within it, like these systems were expensive and unavailability of its. Then the graphical password authentication system creates the great impact on authentication system, initially pass point and persuasive click point were the systems used as the alternative of the text password. But again those had some disadvantages like hotspot. But the CCP overtake all the disadvantages of the old password authentication system. CCP is nothing but clicking five points from five images as one point per image. It helps to enhance the graphical password authentication system. It also creates best system for user to use and memorable and recognising system.

**Related Work :**

One of the best password authentication systems was text based oral phanumerical based password has several problems. One of the main problem with text based password is it was ridicules to remember several text password for different account. Then introduction of biometric password [3] and token based password was considered as the alternative of the text based password, but it again has several drawbacks like cost and unavailability issue. To overcome the disadvantages of text based password and token based password the invention of graphical password is introduced. Initially there were following graphical password authentication systems:

***A. Pass point****.*

***B. Cued Click Point (CCP).***

**C. *Persuasive* Cued Click Points (PCCP).**

But this system had again disadvantage of hot spot problem. To overcome the disadvantage of hot spot problem invention of cued click point is made.

***A. Pass Point:***

S. Wiedenbeck et al [7], have invented the pass point system for password authentication. The concept of the pass point was as simple as just clicking five point on single image and combination of this point as a password. In this system user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. But the main security problem with this was the HOTSPOT, the area where

the user clicks.

***B. Cued Click point:***

To overcome the disadvantage of the pass point authentication system the cued click point is invented. Cued click point has the same concept as of the pass point but the main difference between them is passing five points on five different image one point per image.

***C. Persuasive-cued click point(PCCP):***

The persuasive cued click point is the addition of the persuasive feature to cued click point. It allows user to select less portable password. It has two more function as shuffle and viewport, when users make a secret word, the images are a little monochromic except for viewport for to avoid known hotspots the viewport. The most useful benefit of PCCP is make complex system to hackers. Users have to choose a clickable area within the area and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport.

**Conclusion :**

This system founds very secure and flexible to use. This system allows very attractive GUI to user so user finds very attractive and convenient to use this type of password. This system also can be used as to provide higher level security to the text based password. This system is very cheap as compared of as biometrics system. As per the study results of the human psychology, the human brain is very efficient to remember the graphical passwords than of the text based passwords. Also the graphical passwords are recognizable to the user. After the successful implementation and results of the proposed system we concluded that the graphical password authentication system is very efficient to use.

**2.5** **Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods**

Title: Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods

Published by: Ali Mohamed Eljetlawi, Norafida Ithnin

This research aims to study the usability features of the recognition base graphical password methods available and extract the usability features of the existing methods. In this paper we study the recognition base graphical password type with the available methods from the usability point of view according to previous studies and surveys. Then we match the usability features (General usability features, existing usability features for existing graphical password methods, and ISO usability features) to the existing graphical password methods and make a comparison study between these methods and the usability features. We have found that there is no method has the most important usability features. Thus, by completing this study a set of usability features is suggested to be in one graphical password system. This set includes the easy of use, memorize, creation, learning and satisfaction. Moreover, this work proposes to build a new system of graphical password system that provides promising usability features.

**Related work:**

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques 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. The existing Graphical password schemes are categorized as based either on Recognition Base or Recall Base.

In recognition based techniques, users are given a set of pictures and they pick and memorize some of them. During authentication, the users need to recognize and identify the pictures they have picked earlier.

**Result and Conclusion :**

In this paper, we have conducted a comprehensive and comparative study of existing recognition base graphical password techniques from the point view of usability features. Even though the main argument for graphical passwords is that humans are better at memorizing graphical passwords than alphanumeric character passwords, the existing user studies are very limited and there is not yet convincing the fact to support this argument. We have found that the existing recognition base graphical passwords schemes does not have attractive usability features for the users which mean that the usability features needed to be studied more and develop more usable systems for the Graphical Password.

**2.6 Securing Web Accounts by Graphical Password and Voice Notification**

Title: Securing Web Accounts by Graphical Password and Voice Notification

Published by: Dr. Viorel LUPU

Internet web services which use and protect valuable data collections must combine high quality services for secure transmission channels of data such as Internet connections with SSL protocol enabled and multi-factor authentication systems. There is no longer a viable option to implement the cheap singlefactor authentication system that rely on text for both user identity and password following the RFC 2196 recommendations because restrictions imposed to the user add some more vulnerabilities . Users do not remember long or complex identifiers and passwords especially in a stressful environment or if they are old or have disabilities. They are thus forced to rely on methods that arise other vulnerabilities such as writing identifiers and passwords in accessible and visible files, store in browsers, using same passwords in multiple websites or predictable graphic passwords . More and more users are using smartphones and they are not satisfied to be forced to remember, read and type text with this kind of terminals and authentication process.

This paper presents a real-time multi-factor authentication system based on images selections guided by voice phone call notification system. Subsequently this paper presents some results and comments upon the implementation decisions and users reactions. The main goal of the presented system is to increase the authentication process quality with minimum impact on user comfort. Other goal is to extend its usability in high stress environments like public hospitals and over elderly people or disabled ones.

**Related Work :**

Internet web services clients are connecting daily from authorized hospitals to report medical events and data to a national authority. There are more than 60 hospitals reporting to the national authority through this web service whenever needed. Some entities have two or more events to report daily. Medical data reporting is performed through public computers in the hospital departments. Although it is mandatory performed only by staff with secondary education. This work pattern has been facilitated by the fact that authorized doctors have received a user name and a password-protected account. Thus, the user name and password were stored in those browsers on computers available to all department staff. In fact, anyone who wanted to access those accounts would have had no technological barrier. This is in contradiction with medical but also with the safe keeping of personal data of patients. It is absolutely necessary to change the working procedures by ensuring switching to a type of authentication with several factors, such as banking authentication systems. Accessibility and affordable high computing power, popularity and wide spread of broadband internet technologies including mobile telephony, more and more aggressive cybercrime reveal the truth that the use of text strings and their associated methods for Internet web user's authentication is an obsolete method [8] and improper for use on mobile terminals Even two-factor authentication with short mobile messaging (SMS) has been compromised since 2005 [8]. Criminal attacks on mobile devices are very complex, being the result of a combination of social engineering and advanced technologies. Intercepting text strings to penetrate the security scheme involves the simplest methods and technologies available today, most often accessible through the Internet. Image-based authentication method is presented as a promising alternative [2][3][4] opposite to text authentication (username and password). In current systems are exposed different methods of user interaction with images on the premise that images are easier to remember and associated with actions [2]. Authentication based on image password is catalogued to be a single factor authentication therefore is as safe as authentication with complex text password, but with some advantages and disadvantages or same level of security offered by a 4 digits personal identification code (PIN).

Using smartphones with incorporated fingerprint readers, cameras and facial recognition systems and / or Near Field Communication (NFC) readers for proximity cards opens up new opportunities to operate Internet web services with relatively cheap implementation methods for multi-factor authentication. Because of small screens and even smaller keyboards it is impractical to use smartphones to type text, tap or draw without error. Displaying images for user's touch is a preferable way to collect user actions even on tablets with larger

screens. Nowadays more than 1.9 billion NFC-enabled mobile phones are already in users’ hand (www.statista.com). These devices offer the ability to use NFC proximity cards, rings, or implants to transfer the web service address and user identifier by a simple gesture of approaching the card to the mobile terminal.

**Conclusion :**

This paper presents a multifactor authentication method for web service users which communicate the random one-timepassword by phone call while simultaneously recording user interactions with the dynamically selected and displayed images. The authentication method presented was implemented for a medical web service that collects medical events and data from hospitals distributed across the country. The classic user name and password text-based authentication system has been migrated to a new system based on the presented authentication method. Results obtained through the implementation of the system are: the authentication quality has considerably increased by introducing new factors of identification; the new authentication mechanism is relatively simple to use and does not require special user training. The new system brings

additional operational costs (e.g. telephone service, NFC cards).

**2.7 Random Graphic User Password Authentication Scheme in Mobile Devices**

Title:Random Graphic User Password Authentication Scheme in Mobile Devices

Published by: Sung-Shiou Shen2,a, Tsai-Hua Kang2,b, Shen-Ho Lin2,c & Wei Chien1,d

Smart mobile terminal are an essential device in our life today. The user usually enters in the related words or draws a simple graphic on the touch screen as passwords for unlocking the screensaver. Although this way can provide users with simple and convenient security mechanism, the process would increase the risk of words or graphic information leakage under the strict security consideration. Usually for this type of keypad lock screen app you can only customize the simple pattern or swipe-to-unlock screen with a static image on a background image that you select to unlock your phone. Therefore, the interested parties could have a chance to eavesdrop the simple graphic pattern information in order to hacking the smart device for stealing the personal information. Due to lack of the proper identity authentication mechanism in the usually keypad lock screen app, this paper proposes a new graphic pattern protection mechanism for enhance authentication level in the keypad lock screen app field. By randomly changing the fixed position of the digital graphics that shows on the touch screen, the user can draw different graphic pattern every time based on the unique or backup PIN password to unlock the screen. Not only added the random graphic pattern authentication method indeed increase the personal secret information being stolen difficulty and complexity, it provides more security level than the traditional graphic pattern authentication in keypad lock screen as well.

**Related Work:**

A smartphone or a mobile phone with an advanced operating system support many useful applications to promote normally work [1]. These applications typically combine the features of a cell phone with those of other popular functions, such as personal digital assistant (PDA), media player and Global Positioning System (GPS). Nowadays, most smartphones can access the Internet. They have a touchscreen user interface and can run third-party apps, music players and are camera phones in the meantime. Therefore, Smartphones run complete operating system software providing a platform for application developers. However, the growing popularity of wireless technology may have finally attracted enough hackers to make the potential for serious security threats a reality [2][3][4]. Furthermore, if you lose your smartphone, there can be outflows of personal and business information. Therefore, authentication scheme is necessary way to identify smartphone’s user and to protect the information saved inside the phone. There are many popular authentication methods with smartphone. Slide Lock is provided on Android and IOS system. Slide Lock is a simple and clean locker with powerful notification features. It is weak for security. Typically, keypad, there are ten numbers since 0 to 9 arrange in two dimension array, is used for anyone who deals with numbers frequently. Keypad scheme require a fixed number as password normally.

**Conclusion :**

Today, many user authentication methods and techniques are available in different mobile devices but each with its own advantages and shortcomings. Using graphic based passwords authentication is a growing interest rather than text passwords. Although the proposed scheme in this paper has the advantage with the lock screen digital sequence of random change, even the constant password condition, each time the total number of digitals and graphic user password patterns are different. Indeed, the proposed mechanism overcomes conventional problems of the shoulder surfing and time-consuming authentication process but it has also some limitations and issues like all other graphical based password. Currently we are working on the implementation and evaluation in user adoptability and usability friendly. In future, some other related parameters like time weight factor, image input time interval and user habits will be considered in the proposed scheme to be more secure, reliable and robust.

**2.8**  **A Secure Graphical Authentication System Using Watermark Embedding**

Title: A Secure Graphical Authentication System Using Watermark Embedding

Published by: SREYA PRAKASH, SREELAKSHMY M K

Nowadays the most popular method for User Authentication is using Textual Password. This method has many drawbacks like dictionary attack, brute force attack etc. A secure text based

password must be made using a combination of uppercase,lowercase, and special characters. Users have a tendency to choose weak text-based passwords, which are short and easy to

remember. To overcome the drawbacks of text-based passwords, many picture-based passwords have been proposed. Picture based password systems often suffer from several problems, one of them is the shoulder surfing attack, ie ,images that users choose as password are both easy for an attacker to watch by snooping over shoulders or by using a camera to record input and also predictable. An authentication system called PassMatrix is used to overcome the shoulder surfing attack. User has to choose images as their password during the

registration phase and choose a pass-square per image. To secure the pass-images from the attackers, Generic Visible Watermark Embedding technique is used to blend a cover image

and a pass-image. This method can be extended to secure web applications by using QR code.

**Related Work:**

* Generic visible watermark embedding technique with a capability of lossless image recovery is proposed. The method is based on the use of deterministic one-to-one compound mappings of image pixel values for overlaying a variety of visible watermarks of arbitrary sizes on cover images. Mapping procedure is reversible. It allows the retrieval of original images from the watermarked images. The mappings may be adjusted to yield pixel values close to those of desired visible watermarks. A two-fold monotonically increasing compound mapping is created and proved to yield more distinctive visible watermarks in the watermarked image.
* A recognition-based graphical authentication system called Select to Spawn was also proposed which is secure, robust and convenient to use. This system allows the user to create a graphical password by first selecting an initial image from a collection of available pictures. The selected image will be opened in a new window in which the picture is further divided into 4x4 grid or 16 rectangular parts.
* A new method which is resistant to shoulder surfing attack was proposed by using a false image in authentication step. Like other authentication methods, the graphical password consisted of two steps, registration and

authentication. In the registration step, users select some images from different categories or produce a graphical image as his password. Later on, in the authentication step, he needs to select the correct images or re-draw the graphical password which is used by him.

**Conclusion :**

Graphical password authentication is the method that usesimages as passwords rather than using alphanumeric characters.They are very attractive because humans have better ability to

remember images better than words. In this project a securegraphical authentication system named PassMatrix is proposed that safeguards the users from becoming victims of shoulder

surfing attacks when inputting passwords in public. User has to choose their password image that they already registered from a collection of shown pictures. To hide the pass-image from the attackers Generic Visible Watermark Embedding algorithm is used to blend a cover image and the password image. It is easy for legitimate users to recognize their password image in the watermarked image. On the other hand, it will be very difficult.

**2.9 Two-way Graphic Password for Mobile User Authentication**

Title: Two-way Graphic Password for Mobile User Authentication

Published by: Ming Jiang, Ai He, Kuangyu Wang, Zhengyi Le

In this mobile era, people cannot live without smart phones. But how smart and trustworthy they are is still a problem. User authentication is one of the most important issues. The

prevalent solutions are simple (4-digit) password, regular textbased password, pattern password and fingerprint. However, all of them are one-way authentication and each of them has its own limitations. This paper proposes a two-way authentication method which fuses knowledge-based secret and personal trait information. Two types of demos are implemented, Android and Web. The experiments and analysis prove our approach is stronger than existing ones.

**BACKGROUND:**

User authentication mechanisms have been slowly evolving for several decades, but the dramatic increase of using mobile devices brings new challenges to this reasearch area. Some

traditional solutions such as PIN code are still alive because of either user habits or system upgrade cost. The following subsections summarize each of most polular user authentication methods, and then the comparison is given.

***A.\_ PIN***

4-digit Personal Identification Number (PIN) is usually used when card is present for POS (Point-of-Sale hardware) payment scenario, and it is still widely adopted in many mobile cases, for example, iPhone 6 simple passcode. Alipay uses 6-digit PIN as their payment passcode for extra security. Bank POS in the U.S. adopts 4-digit PIN while China adopts 6-digit.

***B.\_ Regular Text-based Password***

Regular text-based password is still the dominant user authentication method among most of public websites, from e-Commerce, Banks, to Social Networks. However, different webistes have different password requirements. For example, one website asks for 6 charactors including at least a number and a letter, while another website asks for 8 charctors including atleast three of the following: (1) digits, (2) lowercase letters, (3)uppercase letters, (4) special characters. This increases the difficulties for users to remember each of them. Most of users

reuse passwords on multiple websites. Some users even write down all the passwords in a piece of paper or store it in an electronic file.

***C.\_ Pattern Password***

Another popular password is pattern password (also called gesture password or grid password). Android (80.2% market share, 2014 fourth quarter) is the biggest adopter for this

solution. It lays out 1-9 digits in a 3×3 grid, and asks a user to do continuous strokes on the 3×3 touch screen panel. The path is the password. However, the choices of the “patterns” are “hiddenly” limited. For example, if you choose “1”, the next choice could only be “2”,“5”, or “4” (some systems also support “6” and “8”). But “3”, “9”, “7” are never allowed to be chosen after “1”.

***D.\_ Fingerprint***

Fingerprint authentication is preferred by most of mobile Apps, since it is easy, zero-knowledge, and effortless. However, the major security concern is its ***un-resettable*** nature. Once it is compromised/exposed, you can not reset your fingerprint and you only have ten of them. There are other issues. For example, multiple readings during authentication increase user anxiety. For another example, not all devices have fingerprint scan

sensor embedded.

***E.\_ Token***

Either software or hardware token is still widely used. Blackberry devices use two-factor authentication design to provide additional security. “Two-factor authentication requires

an item that you have (for example, a smart card) and an item that you know (for example, a pass phrase).” [5]. And RSA’s well-established Secure ID is in this category .

**Conclusion :**

There is no such flawless solution which meets all security requirements. Graphic Password allows users to upload their own private pictures and provides two-way authentication

which most of recent solutions do not have. The secrets are easy to remember, fast to input despite complexity, and hard to hack (hard to copy and/or steal). However, our implementation only enables a group of shapes. If more shapes can be incorporated in

the system, it becomes the positive-sample-only problem. The public stage of the art recognition rate is around 80% accuracy. Therefore, we keep it as an open problem and look forward to further collaboration. In summary, our Graphic Password solution offers an easier

and stronger authentication than most commonly used PIN and pattern password.

**2.10** A New Secure Authentication Scheme for Web Login Using BLE Smart Devices

Title: A New Secure Authentication Scheme for Web Login Using BLE Smart Devices

Published by: Gaurav Varshney , Manoj Misra , Pradeep Atrey

Existing user authentication schemes used for login to a website are incapable of handling recent phishing attacks such as real time (RT) / control relay (CR) man in the middle (MITM)

attack and attacks launched via covertly installed malicious browser extensions (MEs). Two factor authentication schemes such as Google 2 Step verification, SAASPASS, QR code,

graphical password and push notification based login schemes can be compromised using RT / CR MITM phishing attacks. Hardware token based schemes are safe but the extra cost of the hardware token makes them unattractive to users. Therefore, there is a need to develop new authentication schemes which are hard for an attacker to compromise but easy for users to understand and utilize. This paper analyzes existing authentication schemes to identify the research gaps and then proposes a secure authentication scheme which uses Bluetooth

Low Energy (BLE, BT 4.0+ version) devices for user identification and which can handle RT/CR MITM phishing attacks, attacks launched via malicious browser extensions and app spoofing via attackers. The proposed scheme is location/client system independent and is secure from Bluetooth address spoofing attacks.

**Related Work :**

Based on the above study we identified that an authentication scheme must have the following design features to handle sophisticated credential stealing attacks launched via malicious insiders/outside attackers through covertly installed ME/apps and via remote desktop relay and monitoring modules to cause RT/CR MITM phishing attacks. In any secure authentication scheme, the user must enter a minimal number of authentication credentials manually, and at least one of the credentials must be acquired automatically in a way which makes it difficult for the attacker to acquire and relay. This is because if all the credentials are entered manually by the user, it becomes easy for the attacker to acquire them with the help of a phishing website. The user identification token such as UNAME should be replaced by a token that is hard to acquire and even if the attacker acquires it, it must be difficult for the attacker to use or relay it. Websites must not receive user credentials through key strokes as the MEs can log key strokes and can perform password sniffing. To address the vulnerabilities of existing schemes, we propose an authentication scheme which uses the Bluetooth hardware address (BTADDR) of BLE (BT 4.0+ version) smart devices (a Smartphone, a BT enabled beacon, a smart wearable, a health monitor etc.) as a use identification token instead of the traditional UNAME. User enters his password on a browser

extension and the use of app id as a secret key for encryption makes the scheme secure from sophisticated phishing attacks or attacks via MEs. The proposed Bluetooth Based Authentication scheme using browser Extensions (BBAE) is discussed in the next section.

**BLUETOOTH BASED AUTHENTICATION VIA BROWSER**

**EXTENSION (BBAE)**

BBAE includes: (1) Web Registration Phase (WRP), (2) Extension Registration Phase (ERP), and (3) Login Phase (LP).

***A. Web Registration Phase (WRP)***

User (U) enters his Name (N), PWD, Email ID (EM) and Phone Number (PN) on the registration page of the website. The U also selects a BLE smart device connected to his PC (SP or a smart wearable) that he wants to register with the website. Once

the user selects the BT device, the BTADDR is fetched by the Web Bluetooth API of the website. Then, information entered by the user along with the BTADDR are sent to the website. The website verifies the user by sending an OTP (SEND\_OTP) to the mobile

phone of the user. Once the correct OTP is returned by the user and is verified (VDB) by the website, the website generates (GENERATE) a 16-character SALT and associates it with the

user account. SALT is generated using AES in CTR mode with count value set to 0 and the current timestamp of the server used as IV.

Also, a unique 16-character string generated using a pseudo random number generator is used as the input secret key. The 16-character string of the yield of one CTR block of operation is

used as the SALT. This SALT is used to encrypt (E) the app instance id (AIDCX) at a later stage. It is assumed that there is no attack during WRP and the system is safe from host based key loggers. Figure 1 shows the message exchanges.

***B. Extension Registration Phase (ERP: one time)***

The legitimate website provides a Chrome Extension (CX) that can be downloaded from the browser extension web stores. During installation, when the user registers the CX with the

website, the registered BT device must be connected to the PC. The user enters his PWD on the CX registration page, and the BTADDR of the connected device and the PWD are verified by website. An OTP is sent to the user registration PN. after the OTP is verified, the server generates an app instance id (GENERATE) for the CX and sends it over the HTTPs session along with the user SALT. The SALT is used in concatenation with the PWD to create a key (PWD+SALT) to encrypt the AIDCX before it is stored on the local browser storage. Server also stores the AIDCX in its database (ADDDB).

the message exchanges.

***C. Login Phase (LP)***

In the login phase, the user enters the PWD on the CX, and

the BTADDR of the selected device connected to the PC is fetched.

The BTADDR and the encrypted AIDCX (stored in the local

browser storage) decrypted using the user PWD are sent to the

website. The initial decryption of encrypted AIDCX with user

PWD thwart attacks via malwares which can steal encrypted

AIDCX from the memory. The website identifies the user based

on the BTADDR. The website encrypts the AIDCX stored in its

database using PWD + SALT and then decrypts it using the

PWD

**Conclusion:**

The proposed scheme can handle RT/CR MITM, MEPA, and other sophisticated credential stealing attacks. The novelty of the scheme is that it uses BLE/BT smart devices as a secure

token for user identification instead of using it as an additional token (as done in the SAASPASS scheme) or as a communication channel for transferring user authentication

information In addition, unlike SAASPASS, it does not require users to install a client side operating system dependent module and secures users from attacks that can occur via BT address spoofing.

**2.11** Authentication by Graphical Passwords Method ‘Hope’

Title: Authentication by Graphical Passwords Method ‘Hope’

Published by: Nikita Zujevs

The security of data and user authentication is an important component of currently deployed security infrastructures. Typical text-based passwords and PIN codes have several drawbacks. Whilst short passwords are easy to remember they are insecure, whereas longer complex passwords are more secure but more difficult to remember. The disadvantage of user authentication systems can be solved by replacing typical alphanumeric passwords with a method using graphical passwords comprising images, which can be easily recognized by the user. A mechanism was developed that makes use of graphically based passwords. A web-based prototype application was implemented that makes use of the new authentication mechanism

One of the weakest places in the authentication process is that of password inputting where Trojan horses, shoulder surfing, Closed Circuit Television (CCTV) can all be used to compromise the user’s passwords. To protect users from password leaking different types of additional security were developed – smartcards; identification by fingerprints, iris or face; SMS with a one-time password to mobile phone, etc. Regardless of the number of different types of authentication, still the most popular text-based passwords consist of different keyboard characters – big or small letters from the Latin alphabet, numbers, and different symbols .

The author decided to move away from text passwords and offer an additional choice in password protection tools. The name of this Graphical Password Locker method is ‘Hope’.

**Related Work :**

III. METHODOLOGY

***A. Programming languages and other software***

To develop the GPL (Graphical Password Locker) Hope a web service was used with PHP and JavaScript, as one of the most popular programming languages . User’s passwords are stored in the MySQL database, which is the most popular of this kind of software .

Because of this popularity, almost all OSs support these languages, and so the GPL Hope can be deployed without any problems on any server.

***B. The main idea of the Hope method***

The method is based on the idea of combining several images in one picture and display few additional pictures with decoy images. In this case, the observer from the side of the person will not be able to understand why this particular picture was chosen from several others, because it shows several symbols and only one of them is the password’s symbol.

***C. The GPL Hope’s basic terms***

The user’s graphical password consists of *symbols*. The symbol can be any picture, with meaning (animal, color, etc.) or without (various points or lines that have no name, etc.) Each symbol belongs to only one array with a specific characteristic (animal, color, digit) and has a unique code. This code is used to store the passwords in the database and to generate images for the graphical passwords.

***D. How the GPL Hope works***

The GPL Hope offers a system where the method for authenticating the user of a computer system – comprising a server A; the computer system operating an access device D (having a display and a means for inputting information) – involves:

(i) storing at least one array (A1, A2, … An) of symbols in the storage unit of the server A, each set of symbols representing a different category of symbols;

(ii) storing the selected password in a storage unit of the server A; the selected password being a graphical password comprising one or more password elements sequentially selected from at least one array (A1, A2, … An) of symbols stored in the storage unit of the server A;

(iii) sending from the access device D to the server A a request for authentication;

(iv) generating by the server A and sending to device D one or more images, each representing a combination of symbols randomly selected from one or more arrays (A1, A2, … An) of symbols;

(v) displaying said images on the display of the access device D;

(vi) sending from the access device D to the server A the image(s) selected by the user using the means for inputting information;

(vii) analysing by the server A whether the received selected image(s) contain the same number as those stored in its storage unit and whether said password elements were obtained in the same sequence as those stored in the storage unit;

(viii) authenticating the user, if the sequentially obtained selected image(s) contains the same number as those stored in the storage unit of the server A and if said password elements were obtained in the same sequence as those stored in the storage unit of the server A.

The access device D can be a tablet, a desktop or laptop computer, a smartphone, a point of sale terminal, or a similar device configured to be connected to a wide area network, personal area network, local area network, or campus area network. The display and means for inputting information may be separate devices that are integrated into each other; or the display and means for inputting information may be one touch sensitive screen.

**Conclusion:**Password protection against shoulder surfing is inversely proportional to brute force protection. The higher the brute-force protection, the fewer passwords the hacker needs to steal to reveal it. The Hope method is best used as a complement to traditional text password authentication. If the users are not sure about the security of the device where the password was entered, they can choose Hope authentication. The author believes that the triple combination is better to use on web resources, and single on mobile devices, since less screen space required.

**A short list of the advantages of the Hope method:**

* No need additional devices.
* Can protect passwords from shoulder surfing.
* Quite easy to learn.
* Can be implemented on any web server or mobile device and even at an ATM.
* Passwords are easier to remember.

**2.12 PassPositions: A Secure and User-Friendly Graphical Password Scheme**

Title: PassPositions: A Secure and User-Friendly Graphical Password Scheme

Published by: Gi-Chul Yang

To solve the problem of text-based password authentication, graphical passwords using images have evolved. Graphical passwords process authentication by selecting the exact

positions on the image shown on the screen. These conventional graphical password schemes cannot be used for recognition if the correct points on the screen cannot be selected in the same order. To solve this problem, a new graphical password scheme called PassPositions was introduced. PassPositions were designed based on universal design, so it is user-friendly for everyone, regardless of their physical abilities. However, in certain cases, PassPositions

does have some weak points. In this paper will identify a problem of PassPositions, and improve the PassPositions.

This chapter describes the researches on graphical passwords and what kind of graphical password systems have been developed since the ideas of graphical passwords coming to the present. Knowing the existing systems will help you to understand what is different between

PassPositions that has a new concept of authentication and existing systems.

Graphical passwords are easy for users to remember, and difficult for others to predict. Graphical password is a user friendly authentication method compared to text-based

authentication techniques . The graphical passwords are rapidly developed as a fast-paced alternative to the text-based authentication since Blonder's idea came out. Graphical

passwords are largely can be classified into recognition based graphical passwords and recall-based graphical passwords. The recognition-based graphical passwords will be described first.

**Related Work :**

Jermyn and his colleagues introduce a system known as DAS (Draw-A-Secret) as recall-based Graphical Passwords. This system is a system that can draw a pattern shown as below.

****

In the DAS system, there are divided areas on the screen, and a pattern is drawn as they pass through the areas. As the pattern is drawn the order of the passing area is remembered,

and the passing order of the areas should be the same for authentication. Therefore, the user should memorize the pattern and reproduce it at the time of authentication.

A system proposed by Syukri and colleagues, the authentication is done by drawing a signature with the mouse in this system. Online signature recognition is another topic and it will not be discussed more in this paper.



By using Syukri and his colleagues system, it is easy to remember the passwords and difficult to use by others because it allows users to use their own signature as a password. However, it has the disadvantages of being difficult to use and the procedure of recognition is complicated. In recent years, the techniques that use graphical passwords and text-based passwords together also had been introduced [16]. Chapter 3, a new concept graphical

password system called PassPositions.

III. PASS POSITIONS

Unlike most existing graphical password schemes, ‘PassPositions’ is a graphical password scheme, which uses relative positions of the click points. If the user uses a thick pointer or a finger, and presses a region instead of a point (at a pixel level), then PassPositions will find the centre point of the region automatically, and use the centre point as the click point. Earlier graphical password schemes than PassPositions (e.g. Pass Points) used absolute coordinates of the click points. For example, a user chose three points, and their (x, y) coordinates values were (100, 650), (430, 330), and (170, 70). These absolute values of coordinates were used as a password for graphical password systems earlier then PassPositions.

**Conclusion :**

This paper studied about graphical password among authentication methods that can replace text based authentication method, and describes PassPositions which is a new concept of graphical password system implementation technique. PassPositions generate the authentication code by taking advantage of the relative positions of the selection points, making it easy for people who cannot select the correct absolute position . PassPositions can be made even more practical when used in mobile devices that operate directly using the touch pad with hands. When using a tool such as a mouse or electronic fan, it is relatively easy to select the narrow area more accurately than when using the hand. PassPositions also allows you to freely select images for your backdrop as you would in the PassPoints system. In other words, the user can use the desired image or photo as the background image, which makes it possible to build a system that meets the user's individuality. It can be used even without any background picture. This feature prevents the password space problem caused by the hot spot which is a problem in the conventional graphical password systems..

**2.13 Numerical Password via Graphical Input – An Authentication System on Embedded Platform**

Title: Numerical Password via Graphical Input – An Authentication System on Embedded Platform

Published by: Siva Janakiraman, Karunya Sri V S, Chathurya Pulluri, Sundararaman Rajagopalan, K Thenmozhi, and Rengarajan Amirtharajan

Graphical systems have been in use in the embedded world for user authentication. Image based systems use image, area or pattern selection process. This paper presents a novel method that employ image recognition at its first level and a modified PassPoint logic with randomization using LFSR at its next level to provide a well secured password authentication system. The proposed real-time authentication scheme for embedded system aims at reducing the password storage space against a similar implementation on embedded platform.

In addition to the conventional text based passwords using computer systems, novel ways of password authentication mechanisms with embedded hardware will certainly improve

the existing security infrastructure Due to the ever increasing number of confidential information storage and transaction over public networks, the existing security infrastructure needs to be strengthened by means of multilevel authentication with the confluence of software and hardware . Janakiraman et al., proposed a two stage Graphical

Authentication Unit (GAU) on ARM-Cortex Intellectual Property (IP) core based embedded System on Chip (SoC). The work was aimed at increasing the password space with smaller

image sizes by utilizing the concept of image magnification.

**METHEDOLOGY**

***A. Embedded hardware for graphical password authentication***

The block diagram of standalone embedded system for graphical password authentication. The embedded hardware is built on OMAP 3530 (Open Multimedia Applications Platform) SoC [13]. The OMAP 3530 integrates an application level hard macro (IP core) sub-chip Cortex-A8 as its Microprocessor Unit (MPU) subsystem. The OMAP

device is supported by 128 MB off–chip NAND – Flash memory through a General-Purpose Memory Controller (GPMC). A mobile DDR2 – SDRAM (Dual Data Rate two Synchronous Dynamic RAM) of 128 MB is also linked via SDRC (Synchronous Dynamic RAM Controller) subsystem module of OMAP 3530.

***B. Password creation***

Identification of legitimate user has been supported by adatabase comprising of passwords created by the authorizedusers of the system. Initially, the new users will have to register

themselves in order to create a new password to access the system. Every new user is first assigned with an ID number. The new user has to select an image as first level password

from a pool of four 100×100 images displayed on the GLCD used for image selection.

***C. Gaining authentication***

In order to gain authentication to access the system, the users have to first get themselves identified as an existing user with their unique ID number. The system denies the password

entry by the user when an invalid ID number is entered. The system has been designed such that it will provide three changes per day for the user to enter a correct password after

which the account gets locked.

**Conclusion :**

The set of 100×100 images used for the initial recognition based authentication phase is sThe 4×4 image matrix obtained next to recognition phase is given in The three image blocks shows the chosen graphical password which in-turn internally registers a three digit

hexadecimal numerical password “6BE”. The pseudo random sequence obtained from the LFSR circuit used to reposition the 4×4 image blocks is presented in Table I. Fig. 4d depicts the randomized form of 4×4 image matrix formed using the LFSR output sequence shows the screenshot of the portable embedded hardware setup used to experiment the proposed

graphical password authentication system. The earlier scheme for graphical password on embedded system proposed by Janakiraman et al., [10]compares the pixel values corresponding to the chosen areas of the magnified image to authenticate the user. Accordingly, storing the pixels corresponds to three 20×20 blocks of grayscale image needs,

1200 Bytes (3×20×20). Alternatively, the technique presented in this paper stores and uses only the three digit hexadecimal numerical password. Thus, the proposed method requires only 3 Bytes for password storage.

**2.14 Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability**

Title: Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability

Published by: Jaffar Abduljalil Jaffar, Ahmed M. Zeki

User Authentication is an important component of security. There are several mechanisms for authentication in use, such as alphanumerical usernames and passwords. However, due

to the well-known weaknesses attached to this method, graphics based passwords were suggested as an alternative. Due to the ability of humans to remember images faster and for a longer period. This study comprises of comprehensive research in the graphical password schemes and evaluates each of the available schemes at two main areas (attack resistance and usability). In the end, it also provides an answer to the question “Are graphical passwords more secure than alphanumerical passwords?”.

**Related works :**

Over recent years, some methods have been applied to predict sales and demand in the practical industry' 1-4 !, and ARIMA, regression, time series, and grey theory are the most frequently used methods, and they all need great amount of training data. Unfortunately, the existing data is usually insufficient, and a rather long training time is expected in above approaches.

Forecasting trend in Tobacco sale is considered complicated, not only because of many factors within the enterprises and that outer circumstances may influence it, but also by the reason that there are no rules during the operation. We want to propose some intelligent recommendation for decision making to tackle the complexity of sale prediction for Chinese tobacco enterprises. In our case, learning and predicting methods based on ε-SVR for intelligent decision support are provided, then, numerical and graphical visualization results describing the tobacco sale prediction are illustrated. Furthermore, the efficiency of ε-SVR is analysed by comparing with the neural network.

**Implementation details:**

**RECOGNITION-BASED SCHEMES**

Generally, in recognition-based graphical passwords, users need to choose a number of correct images from many. Research showed that 90% of users can remember their

password after one or two months . Even though the recognition-based scheme has not been wildly deployed, many schemes were developed to improve this technology.

**A. Passface Scheme**

The Passface scheme is built on the human ability to recognize and remember human faces better than other images Basically, from a list of human faces, users are required to select a single face image.

**B. Déjà Vu Scheme**

Developed in 2000, this scheme allows users to select and recall an image from a larger set of images generated by the system . All abstract images were created using Andrej Bauer’s random art which was introduced to minimize the effect of shoulder surfing within graphical passwords. Nevertheless, this technique shared a similar issue with having complex text passwords that are hard to remember.

**C. Triangle Scheme**

Sobrado and Birget in 2002, suggested a graphical password technique to solve the problem of shoulder-surfing threats known as the “Triangle Scheme”. The user is required to select several objects from a wide range of objects during login.

**D. Moveable Frame Scheme**

In addition to the Triangle Scheme, Sobrado and Birget suggest a second scheme which is the “Moveable Frame”. Users must choose a total number of three images that will be stored within the system and during the authentication process, one of these images will be located into a moveable frame.

**PURE RECALL-BASED SCHEMES**

As the name implies, Pure Recall-based graphical authentications are purely focused on having users recall an outline drawing/ image that they either have drawn or selected

during the registration phase without any hits or cues.

**CUED RECALL-BASED SCHEMES**

Cued recall-based authentication is based on the user’s ability to recognize certain locations within an image. The system, on the other hand, provides hints or reminders.

**Conclusions :**

This study revealed that graphical-based schemes have their benefits and weaknesses. This is not surprising since most of these schemes were designed to overcome the burdens of

remembering textual passwords as it is well known in the security field that there is always a trade-off between usability and security in a way that decreasing one of the two inevitably

increases the other. To date, most schemes are only discussed in laboratories, and successful adaptation of graphical passwords occur mostly within tools that are used as a second

verification to stop bot attacks such as “CAPTCHA”, or user re-authentication such as Facebook account recovery mechanism.

\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized

**2.15 Directional Based Graphical Authentication Method**

**with Shoulder Surfing Resistant**

Title: Directional Based Graphical Authentication Method

with Shoulder Surfing Resistant

Published by: Noor Ashitah Abu Othman, Muhammad Akmal Abdul Rahman, Anis Shobirin Abdullah Sani, Fakariah Hani Mohd Ali.

Authentication has been advanced by implying advancement in security such as cryptography to protect password against data leaking and sniffing; captcha to prevent robot system; Secure Sockets Layer designed to protect users against phishing website and many other solution invented for different types of vulnerabilities. Although there are other methods suggested for preventing shoulder surfing (i.e. exposure of password to nearby observing-person), the techniques still have some drawback. Some of the proposed techniques also required

high computational process with high range of possible answer. This paper proposed a shoulder-surfing-proof graphical based authentication with direction scheme that combines technique adapted from Passfaces scheme and a selection of direction. User is required to choose four faces and one direction to serve as the secret authentication. Besides shoulder surfing, the proposed method also caters security in data transmission storage as hashing is applied along the communication. This technique has been proven to demonstrate the robustness, security strength and the functionality advantages of the system. The result from the security testing shows that image based passwords is more secure because the possibility of the image to be guessed is very low.

**PENETRATION TESTING**

This Directional-based Graphical Authentication was tested against several basic password attack tools in order to certify it fulfill basic requirement of authentication system.

***4.1 Text-based Password Cracking Tools***

The cracking process is done by using software named Cain & Abel. Cain & Abel allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords and more. This software uses Brute Force technique which tries every

combination of ASCII character based on try and error methods that used by application programs to decode encrypted data in order to gain information such as username and passwords. However, the tools were not able to crack the proposed image-based passwords

because the all the password cracking tools and technique is not be able to crack image-based passwords. Even if attacker tries to network sniff the password, they are not being able to crack it because the passwords stored for this study is already being hashed and it is not

in a plain text.

***4.2 Stored Image Security***

The access of the folder in URL was blocked and whenever attacker tries to access into the folder, the permission is denied by the server. In order to block the folder URL, *.htaccess* file were added into the folder. with the content ‘deny from all’.

***4.3 Breaking Hash***

Hash was designed to be secure one-way encryption. The breaking hash process was done by using several online tools such as CRACKSTATION, SHADECRYPT and SHA512 Decrypted. All of the tools give a failed result of reversing the hash.

**PENETRATION TESTING SECURITY**

**CONSIDERATION IN THE PROPOSED METHOD**

Pass-images are combined and implement hashing algorithm before stored in database. This will prevent the data from being sniff during transmission. Other than that, the stored hashed data also become more sturdy against attack that be directed at database. Once the passwords have been hashed, there are no ways it can be reversed because hash is one-way cryptography. This gives another advantage against brute force and other types of password guessing techniques. Images to be display are randomized in every page. Moreover using this proposed method, user will not click on their actual image. Thus, even if a culprit watch a

target victim input their Pass images several times, the probability to get on right sets of pass image is still low.

**CONCLUSION**

Directional Based Graphical Authentication has been proven to be shoulder-surfing-proof authentication system because user will not clicking directly to their images, users clicked into image that satisfies direction of their images. The probability algorithm is used

because the hashed value is irreversible. So, in order to validate the passwords, the algorithm will hold the value of top, bottom, left and right of the clicked images. Then the images will be combined according to their direction and all the value are compared with the hashed value in the database. Together with hashing function, this method is beneficial in securing authentication process. This Directional Graphical Authentication method can be enhanced by increasing the number of direction for authentication to lower the probability of exposure. It is possible by using shape that provides higher number of sides such as hexagon during authentication.

**REFERENCES:**

***2015 Information Processing (ICIP)***

***Vishwakarma Institute of Technology. Dec 16-19, 2015***

15.2018 IEEE , Process and Control (ICSPC 2018), 14–15 December 2018, Melaka, Malaysia

202