Project title

Control techniques for the common password attacks.

List of group members - Group #14

Agarwal, Mridul
Deshpande, Omkar
Prakash, Shivam
Sunkesula Bhaskar, Nikhil
Talasila, Madhu Meghana

Introduction

Background and Motivation

An astute and decisive information system is the need of the hour. In the recent past, some of the IT giants have faced the issue of password leak because of social engineering. Passwords are the basic means of authentication and authorization. It is not necessary that a technically advanced system is fully secured. Typically the passwords are alphanumeric i.e. combination of letters and digits. These types of passwords are difficult to remember. So we land up selecting weak passwords which are vulnerable to dictionary attacks and brute force attacks. To overcome such type of problem, the researchers have proposed a graphical password mechanism. The next big thing related to the password security are the phishing attacks. PhishTank(2009) provided a list of active phishing sites which show that 70% of the sites are designed to retrieve user name and passwords. If the phisher obtains this data he can easily login and can further obtain sensitive information which could cause irreparable harm. A solution to this type of attack could be by performing the user authentication via one-time passwords(OTP) which is delivered through a reliable secondary communication channel on demand. The next and popular cause related to the password security breach is the hacking attack. And one of the solutions which is robust against any hacking attack is the noisy password technique. The noisy password consists of several parts - the actual password and the noisy part. It has been proven that the noisy parts have been robust against all type of hacking attacks. This all motivated us to survey, identify and outline the solutions for avoiding the password attacks.

Goal and scope of study

The scope of our study involves survey of different papers that propose solutions for the following scenarios of password security breach.
Cause 1: Hacking attack
Cause 2: Phishing attack
Cause 3: Weak passwords

And then present a thorough analysis of present and new techniques/solutions to prevent these attacks. Thereby evaluating the identified techniques to control these causes.

Results

Agarwal, Mridul

Tasks completed

a) Analyzed the one time password mechanism to reduce the number of password phishing attacks.
b) Security analysis of the mechanism.

Description

Phishing is a malicious activity whereby an attacker (phisher) tries to trick Internet users into providing confidential information (Dhamija et al., 2006).PhishTank(2009) provided a list of active phishing sites which show that 70% of the sites are designed to retrieve user name and passwords. If the phisher obtains this data he can easily login and can further obtain sensitive information which could cause irreparable harm. A solution to this type of attack could be by performing the user authentication via one-time passwords(OTP) which is delivered through a reliable secondary communication channel on demand.

Mechanism

Here, the author considers an instant messaging(IM) service as the secondary communication channel. And also the primary channel, i.e. the HTTP protocol is secure. The advantages of using IM service are: delivers messages in real time, they are almost ubiquitous, cost effective, infrastructure is already available on the internet, and downloading the client side program and obtaining a user account are free of charge. The disadvantage is that it is not fully secured but with proper configuration and design, it can be utilized efficiently.

This mechanism involves two processes:

I. a registration process, and
II. a login process.

We use OTP in both of these processes, and the life span and the no. of attempts to enter the password is limited to reduce the chance that it could be guessed. The steps in the registration process are identical to the conventional registration except that the users are not asked to choose a login password. Instead, the user is required to complete an extra IM account registration. After the successful registration, user can login to the system using the OTP assigned by the website.

Security Analysis

Here, we briefly describe the strengths and weaknesses pertaining to security.

As far as *mutual authentication* is concerned, by the proposed mechanism a website(server) authenticates user(client) by asking to enter the OTP which is already assigned by the website. As only the user knows about the IM account which is used to obtain the OTP, other users cannot guess the correct OTP.

There are three components related to the proposed solution, they are - user's website account, the website's IM account and the user's IM account. Hence, to compromise the proposed solution the attacker needs to get hold of the unrevealed relationship between these three components. It might be a possibility that a phisher might acquire the user's account name, but to compromise the given solution he needs to get hold of the IM account details as well. But we can enhance the security of the IM services by: *encrypting the instant messages*, by having a *customized interpretation of authentication messages* or we can simply *block messages from unknown users*.

This mechanism also provides security when we are accessing the website in an *untrustworthy environment*. In such cases user must have some trusted secondary device which is connected to the internet. In such a situation he might access the IM account through the trusted device to obtain the OTP and could use a publicly shared computer to log in to the website by entering the OTP received via the trusted device.

Now let's analyze the proposed solution with respect to the *Man In The Middle* attack. We have already made an assumption before that the primary channel used to deliver user's login name is secured; therefore, an OTP cannot be associated with the user's web account name by any eavesdropper. If at all the OTP is discovered then also it will be of no use as it will not be sent via the user's machine, which is identified by the IP address. Thus, by MITM attack an attacker can only retrieve optional security question and its answer. Another solution to this problem could be re-authentication of the user in case of a critical transaction.

Other kind of popular attack is the *IP-spoofing* attack, but is difficult to occur with the given mechanism, since primary communication channel is encrypted. So, to perform such an attack the attacker will have to first breakdown the primary communication channel. And secondly either the attacker has to be someone using the same IP or some sort of man in the middle. We have already discussed about MITM, as far as attacker using the same IP concurrently is concerned, it can be detected easily. And more over the lifespan of the OTP and the session token is of few seconds. Therefore this type of attack is very difficult to perform.

Tasks to be completed

a) A more comprehensive and detailed security analysis of the one-time password mechanism.
b) Examining the security related strengths and weaknesses of the given mechanism.
c) Identifying possible improvements for the above identified weaknesses.
d) Preparing a detailed collaborated report.

Deshpande, Omkar

Tasks Completed

a) Brief description of Hacking attacks on passwords and existing security techniques.
b) Understanding the Noisy Password technique with OTP to make system robust against hacking attacks.
c) Security Analysis of Noisy Password technique with OTP.

Hacking attacks on passwords

There are many types of hacking attacks on password namely hijacking or impersonation, password theft, dictionary attack, shoulder surfing, video recording etc. Password based user authentication can counter dictionary attacks if one opts for strong password. However humans are not experts in memorizing complex strings. The biometric technique for authentication is considered to be highly secured for authentication. But such techniques are costly and can result in lot of false rejections. For example, the system may not allow access to a legitimate user because of a cut on his/her fingers. Token based authentication techniques like using ATM cards, are prone to theft attacks. One time password technique (OTP) uses different password every time the user tries to sign in. OTP mainly uses the mathematical algorithms or time synchronization for generating one time passwords. The One time passwords that use time synchronization are expensive for large system. And the one time passwords, that are not time synchronized, are highly prone to hacking attacks. Therefore authors have proposed a new technique which combines Noisy password technique with OTP to make system robust against hacking attacks.

Noisy Password technique with OTP

Noisy password comprises of actual password along with few extra characters or noise. As oppose to normal static password, it cannot be used directly for authentication. Instead it has to go through the software which extracts the actual password and forwards it for regular authentication. Noisy password can be divided into four parts- a fixed alphanumeric F, a variable alphanumeric V, a terminator X and a safeguard S. It can be defined in ordered quadruplets as follows-

$P=<T_S, V, X, F>$

F is defined by the user and it's an alphanumeric text with length of 4 to 8 alphanumeric characters. It forms the fixed part of the noisy password and it represents the actual password. It can be represented as follows-

$F= \{f_1, f_2, f_3 \ldots f_i \text{ where } 4<=i<=8\}$

V is the variable length of the alphanumeric text that user enters between each of the character of the actual password F until hit by a terminator. It can be represented as follows-

$V= \{v_1, v_3, v_3 \ldots v_i \text{where } 0<=i<= n_j\}$

There are few restrictions applied on V. The character that v_k that belongs to V should not be equal to the any character x_i that belongs to X. This restriction can be stated by the following equation-

(v_k *belongsto* V_i) != (x_i *belongsto* X)

X is a character set that acts as a terminator. X can be represented as follows-

X= {x_1, x_2, x_3… x_i 4<=i<=8}

User is requested to enter an alphanumeric text T_s of length S, after each f_i, where S is called as safeguard number.

As oppose to the normal static password, user has to remember two things- fixed part of the noisy password and the terminator. Example of noisy password-

F = 2, 5, 7, 9

S = 5

X = 1, 3, 6, 8

V = any subset of alphanumeric character set.

User can enter the following variable length password-

24592125492359456754289

The system will now look for the terminators-

24592**1**25492**3**5945**6**7542**8**9

The system will now extract the characters that are located immediately after the terminators-

24592**12**5492**35**945**67**542**89**

Analysis of the technique

This algorithm may prove robust to hacking attacks as compared to other algorithms, if it used by experts who have basic knowledge about the algorithm. The variable length of the password can be as large as required and does not need to be same every time. This will eliminate the use of weak passwords and hence shield the password against dictionary attacks. Shoulder surfing will be extremely difficult because user will enter different password every time with only the fixed part F and terminator X being the same. However, its strong point can prove its weak point. It will fail if F and X are comprised and hence it is extremely important to protect F and X. It can also prove robust against video recording attack because every time user will enter a long and different password making it extremely difficult, almost impossible, to study the typing pattern.

However, this technique can prove to be tedious for some users as compared to the simple static password authentication technique. Due to lack of experience in using the noisy password technique, users may also take considerable time in choosing and inputting the password. Choosing a password may take time because of the strict conditions imposed on variable length of the password, as stated above. Also there can beasignificant error rate in choosing the valid password. This all factors make this

technique more usable in an environment where security is more important than time. The major issue associated with this technique is implementing it on regular basis with the users that have low or no prior knowledge about this algorithm. Authors have proposed a modified technique that will ease the utilization with low error rates in the succeeding paper.

Task to be completed

a) Getting detail insight of the modified noisy password security technique that will ease the utilization with low error rates.
b) Security Analysis of the modified noisy password security technique.
c) Compare both the techniques and prepare a detailed collaborated report.

Prakash, Shivam

Tasks Completed

A. Analyzed various password phishing techniques.
B. Studied counter measure to prevent these attacks.

Background Study:

With the drastic increase in use of internet by users for performing financial transactions, hacking for password has grown to prominence. Most of the attacks seek to get the information of user's credentials like credit card details etc. Some of the trivial attacks against password are Brute-Force attack, Dictionary attack and Guessing attack. These attacks can be deterred by using strong password.

Passwords also become vulnerable when user uses a single password for every website. Hacker can break into one of those vulnerable sites and can use the retrieved password on some other important websites. Moreover, adversaries now try to phish user directly by falsely claiming to be some legitimate enterprise and trying to allure user to enter there password and other credentials on their fraudulent website.

Fundamental Approach:

To deal with this security issue, many researcher and developers tried to finda solution. Theybasic idea was-Hashing the master password using the domain names as keys. In this way, user may use same password for every website but since it is hashed with the domain name of the website, a unique password will be generated for each site. So even if a hacker creates a web page and somehow tries to misguide user to enter the password then also he will receive a password hashed with its domain name. It is very difficult to decrypt using common attacks like Brute force, Dictionary attack etc. Some of the examples of such applications are- Password Composer, Magic Password Generator, Password Hasher, Password Generator, PwdHash.

PwdHash++:

V. Reddy, V. Radha and M. Jindal in their paper, 'Client Side protection from Phishing Attack', compared these various anti-phishing tools. They evaluated thesetoolson the basis of certain factors like application type, hashing algorithm, password strength, spoof proof, visibility to web page, visibility to user, and concluded Pwdhash as the most secure tool for passwords protection. Though it was a good tool which provided a decent way to secure password, they identified some shortcomings like invisibility of running app to user, visibility of the activation of app to webpage, password filling as plaintext, easily spoof-able, effects on JavaScript's of other web pages.

To overcome these shortcomings, they provided a solution which addressed to these problems and named their new tool as PwdHash++ [1].It followed a sequence of steps which laid the authenticity of website and the browser plug-in.The extension was activated when user hits special prefix(@@) on the password field of the web page. This popup window contains the identity key (asked at the time of installation from user) which makes sure that the extension popped up is genuine. Apart from this it also have a background, which is a site specific custom image which user assigns to trusted website. So if user tries to open a trusted web site and this image is not displayed then it can be figured out that the website which user is working on is a malicious one. These measure validated the authenticity of the website. After this user is supposed to enter the password through this extension. This password is hashed with the domain name of the site. The algorithm used for hashing is MD5 which is non reversible. This solution improved the efficiency of Pwdhash and made it able to counter JavaScript Attack.

Hashing with a Salt value:

Another defense mechanism to protect password from phishing was proposed by researchers S. Khayal, A. Khan, N. Bibi and T. Ashraf [2]. In this paper they suggested an improvement for password hashing technique by using a salt value for hashing, which were basically current parameters of the system like Date, Time and some special characters. The algorithm used here for hashing was SHA-1. The advantage of using salt value will be that even if the hacker populates a table of hashes corresponding to each value, then also he will not be able to get to know the password of the user since the hash value is calculated after including the salt in the user's password. So even he decodes the hashed password then also he will not come to know the master password.

Tasks to be completed

1. Comparison of MD5 and SHA-1 algorithms.
2. Analysis of other password anti-phishing techniques.
3. Comparative study among these techniques and their performance in the real world.

Nikhil SB

Tasks Completed

Understood various techniques that have been proposed to secure the password system.Analyzed the strengths and weakness of each approach. Read as to why the current solutions are not fully effective in securing passwords. Most of them still are vulnerable against MITM, replay &spoofing attacks. And read the need for new techniques for password security.

Although many systems use complex techniques to secure the system, Password security is the most common method adopted as a first line of defense in various systems. Most of the personal and sensitive information are secured with passwords. The Challenge here is to design a technique/scheme which has lessdrawbacks.

We researched various papers and one of such a paper was "DPASS – Dynamic Password Authentication and Security System using Grid Analysis" by Balaji R and Roopak V. In this paper they discuss the conventional password system and its security problems. They reference a technique called One Time Password, where the user enters new password every time to login to the system. They propose a new technique which is dynamic and also uses the feature of OTP. The proposed system makes use of a grid which is generated dynamically every time. The grid is made up of alphabets, numbers and special characters included multiple times. User tries to enter his password/pattern by selecting the cells of the grid. The user enters a complex character at i'th position to make the pattern complex. Since the grid generation is dynamic the pattern entered by user also varies countering the replay attack. This method also counters Brute force attack efficiently as cracking the password takes years even for a 6 character password in a 9*9 Grid.

Justin Cappos also proposes a system which is difficult to crack the passwords even though you manage to get the password files. This paper discusses the approach to keep passwords secure with a different type of storage mechanism. It uses a secure hash with salt to store the passwords. The hashed passwords are split and stored across different servers. Salt already has an advantage as it makes impossible for user to guess the password from its hash and PolyHashing adds to the security.

Another defense mechanism is mentioned in the paper proposed by researchers. V. Reddy, V. Radha and M. Jindal in'Client Side protection from Phishing Attack' paper. They perform comparative study among existing tools explain the shortcomings. A solution tool is proposed which overcomes the shortcomings.

Tasks to be completed

1. Learn more methods to secure the password authentication/security.
2. Select few techniques which provide a better security to passwords.
3. Compare and discuss advantages and drawbacks/ issues related to all of the selected techniques and present an efficient &feasible solution.
4. A comprehensive report to be developed.

Talasila, Madhu Meghana

Tasks completed

a) Studied different authentication methods and causes of weak passwords
b) Analyzed categories in graphical passwords.
c) Identified hybrid scheme in graphical passwords as better alternative for weak passwords

Background

Authentication, the process of identifying an individual based on username and password, the weakest link of computer security system. The authentication methods can be broadly divided into three categories namely token based, biometric and knowledge based. The problem of weak passwords is because of two conflicting requirements of passwords, 1. Easy to remember and authentication protocol should be followed, 2. Hard to guess. While choosing alpha numeric passwords (min. of 8 characters and combination of lowercase, uppercase, digits and special characters) user tends to compromise one of the requirements which results in weak passwords. Some of the reasons why users tend to compromise are limitations to human's long term memory - each user might be having a number of accounts, user might not be using account from long time and some accounts need password to be changed periodically for the sake of security. Weak passwords are prone to dictionary attack, brute force attack and soon. Other methods like PIN No. (Choosing a pin or one time password) and Biometrics (using thumb impression/ iris scan/ face scan to authenticate) are not always feasible and involves high operational cost. Graphical based password scheme, using images or graphics to authenticate, is a better alternative because according to psychological studies humans remember pictures better than text and in most of the graphical based password techniques are less prone to dictionary attack.

Graphical based Password Scheme

In **Recognition based techniques**, user has to identify the image which he has seen/ chosen before during registration phase. It is easy for user to recognize than to enter something purely based on memory. Example: Passfaces: user select n faces in the registration phase. During password authentication, user has to recognize the selected n faces among several other faces in n steps. Disadvantages with recognition based techniques is that limited number of faces are available and is vulnerable to brute force attack. In **Pure Recall based methods**, user has to redraw something which he draw previously. Example: Grid Selection: User has to select or draw a line connecting a number of grids during the registration phase. While authenticating, user has to redraw the shape connecting same grids in same order. Disadvantage with this method is that users are finding it more difficult to remember than alphanumeric passwords. For **cued-recall based methods**, user has to select an image based on the hint that he kept in registration phase. Example: Passpoints: User has to select n distinct points in an image

while registering to the system. During logging in user has to select the same point with some error of 0.25 pixels and in same order. Problem with cued-recall based method is that users are taking more time to learn the password and is taking more time to authenticate than alpha numeric passwords.

Graphical based password schemes too have drawbacks. 1) People with poor vision and color blindness might find difficulties in using graphical password. 2) People who are less equipped with or having some problem to handle devices like stylus, pen etc., may not use graphical passwords effectively. 3) Images occupy more space to be stored in the database. Considering difficulties of graphical passwords a new mechanism was proposed, **hybrid system** which is a mixture of recognition and recall based schemes.

Working of Hybrid System

This system comprises of 9 steps. Steps1-3 are registration steps and steps 4-9 are the authentication steps. The first step is to type the user name and a textual password which is stored in the database. During authentication the user has to give that specific user name and textual password in order to log in. In second step objects are displayed to the user and he/she selects minimum of three objects from the set and there is no limit for maximum number of objects. This is done by using one of the recognition based schemes. The selected objects are then drawn by the user, which are stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. In third step during authentication, the user draws pre-selected objects as his password on a touch sensitive screen (or according to the environment) with a mouse or a stylus. This will be done using the pure recall based methods. In fourth step, the system performs pre-processing. In fifth step, the system gets the input from the user and merges the strokes in the user drawn sketch. In sixth step, after stroke merging, the system constructs the hierarchy. Seventh step is the sketch simplification. In the eighth step three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching [3a].

Tasks to be completed

a) Comparing chosen mechanism with other methods w.r.t security analysis
b) Examining the strengths and weaknesses of the given mechanism.
c) Preparing a detailed collaborated report.

Timetable

NAME	MILESTONE
Agarwal, Mridul	Week 1:Read materials related to phishing attacks and how passwords are compromised via this type of attack. Week 2: Analyzed the OTP mechanism and how it works. Week 3: Did a brief security analysis of the OTP mechanism.

Deshpande, Omkar	Week 1: Brief study of hacking attacks on password and existing security techniques. Week 2: Read paper on Noisy Password Scheme with OTP. Week 3: Security Analysis of Noisy Password Scheme with OTP.
Prakash, Shivam	Week 1: Study of phishing attacks for passwordtheft. Week 2: Analyzing different anti-phishing techniques. Week 3: Comparing and Contrasting the studied techniques.
SunkesulaBhaskar, Nikhil	Week 1:Brief study on the need for password security ,causes and existing security techniques. Week 2: Study of Dynamic password authentication and security system using grid analysis Week 3: Analyzing different techniques like dynamic passwords ,OTP & the PolyPassHash scheme
Talasila, Madhu Meghana	Week 1: Brief study on authentication techniques and causes of weak passwords. Week 2: Analyzing different graphical passwords techniques Week 3: Study of hybrid system for authentication

References

Agarwal, Mridul

Read

[1] Chun-Ying Huang; Shang-PinMa; Kuan-TaChen, Using one-time passwords to prevent password phishing attacks. Journal of Network and Computer Applications 34(2011)1292–1301

[2] Ahmad Alamgir Khan, Preventing Phishing Attacks using One Time Password and User Machine Identification. International Journal of Computer Applications (0975–8887) Volume 68– No.3, April 2013

[3] PhishTank.PhishTank:jointhefightagainstphishing,2009.[online] /http://www.phishtank.com/S. URL:/http://www.phishtank.com/S.

[4] DhamijaR,TygarJD,Hearst M. Why phishing works.In:CHI'06:proceedings of the SIGCHI conference on Human factors in computing systems. NewYork,NY, USA: ACM;2006.p.581–90.

To be read

[1] Yun Huang; Zheng Huang; Haoran Zhao; Xuejia Lai, A new One-time Password Method. 2013 International Conference on Electronic Engineering and Computer Science. IERI Procedia 4(2013):32–37

[2] K.Aravindhan; R.R.Karthiga, One-time Password: A Survey. International Journal of Emerging Trends in Engineering and Development. Issue 3, Vol.1 (January 2013). ISSN 2249-6149

Deshpande, Omkar

Read

[1] Khaled Alghathbar (ghathbar@coeia.edu.sa),Hanan A. Mahmoud (hanan.hosni@coeia.edu.sa) , Noisy Password Scheme: A New One Time Password System, Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia [2010].

[2] Minakshi Bhardwaj, G.P Singh, Types of Hacking Attack and their Counter Measures, International Journal of Education Planing& Administration, Volume 1, Number 1 (2011), pp. 43-53, Research India publications, http://www/ripublication.com/ijepa.htm

[3] Adeka, M.; Shepherd, S. ;Abd-Alhameed, R., "Resolving the password security purgatory in thecontexts of technology, security and human factors", Computer Applications Technology (ICCAT), 2013International Conference on DOI: 10.1109/ICCAT.2013.6522044, Publication Year: 2013 , Page(s): 1-7

To be read

[1] Khaled Alghathbar (ghathbar@coeia.edu.sa), Hanan A. Mahmoud (hanan.hosni@coeia.edu.sa) , Noisy Password Security Technique, Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia [2010].

[2] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd "Reducing Shoulder-surfing by Using Gaze-based Password Entry," Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

Prakash, Shivam

Read

[1] Reddy, V.P.; Radha, V.; Jindal, M. Client Side Protection from Phishing attack. International Journal for Advanced Engineering Sciences and Technologies 3.1(2011):39-45

[2]Khayal, S.H.; Khan, A; Bibi, N.; Ashraf, T.Analysis of password login phishing based protocols for security improvements. *Emerging Technologies, 2009. ICET 2009. International* Conference, Serbia, 19-20 Oct. 2009.

[3] Ross, Blake, Collin Jackson, Nick Miyake, Dan Boneh, and John C. Mitchell. "Stronger Password Authentication Using Browser Extensions." 14th USENIX Security Symposium —Technical Paper. N.p., n.d. Web. 13 Oct. 2014.

[4]Luca A. D., Frauendienst B., Maurer M., Seifert J., Hausen D., Kammerer N., Hussmann H,. 2011. Does MoodyBoard make internet use more secure?: evaluating an ambient security visualization tool. In Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11). ACM, New York, NY, USA, 887-890.

To be read

[1] Agarwal, V. K.; Bharti, B. T.; Parihar, B. Password Authentication with Secured Login Interface at Application Layer. International Journal of Computer Science and Network Security 14.9(2014):82-85.

[2] Zeydan, H. Z.; Selamat, A.; Salleh, M. Study on Protection against Password Phishing. World Applied Sciences Journal 35:5 (2014):797-801.

[3] Gouda, M.G., Liu, A.X., Leung, L.M., Alam, M.A.: SPP: An anti-phishing singlepassword protocol. Computer Networks 51(13), 3715–3726 (2007).

[4] Wu, Y.; Zhao, Z. "Enhancing the security of Online Transaction with CAPTCHA Keyboard". Information Security and Privacy Research 376(2012):531-536.

SunkesulaBhaskar, Nikhil

Read

[1] Balaji. R, Roopak. V, "DPASS: Dynamic password authentication and security system using grid analysis", Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.2, no., pp.250-253, 8-10 April 2011

[2] Reddy, V. P.; Radha, V.; Jindal, M. Client Side Protection from Phishing attack. International Journal for Advanced Engineering Sciences and Technologies 3.1(2011):39-45.

[3]Cappos, Justin PolyPassHash: Protecting Passwords In The Event Of A Password File Disclosure - https://password-hashing.net/submissions/specs/PolyPassHash-v0.pdf

[4] Rainbow Table – Wikipedia. http://en.wikipedia.org/wiki/Rainbow_table

To Be read

[1] Agarwal, V. K.; Bharti, B. T.; Parihar, B. Password Authentication with Secured Login Interface at Application Layer. International Journal of Computer Science and Network Security 14.9(2014):82-85

[2] Wu, Y.; Zhao, Z. "Enhancing the security of Online Transaction with CAPTCHA Keyboard". Information Security and Privacy Research 376(2012):531-536.

Talasila, Madhu Meghana

Read

[1] Ahmad Almulhem, "A Graphical Password Authentication System", World Congress on Internet Security (WorldCIS-2011), London, UK, February 21-23, 2011.

[2] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", 2010 International Conference on CyberWorlds, Singapore, 20-22 October 2010.

[3a] Wazir Zada Khan, Mohammed Y Aalsalemand Yang Xiang. " A Graphical Password Based System for Small Mobile Devices"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[4] Elizabeth Stobert, Robert Biddle, “The Password Life Cycle:User Behavior in Managing Passwords”.

To be read

[1] Wei Hu,Xiaoping Wu, GuohengWei, “The Security Analysis of Graphical Passwords” International Conference on Communications & Intelligence Information Security, 2010.
[2] MohdJali, Steven Furnell, and Paul Dowland, “Quantifying the Effect of Graphical Password Guidelinesfor Better Security”
[3] http://arxiv.org/ftp/arxiv/papers/1001/1001.1962.pdf