ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Uncontrollable Cybercrime with Artificial Intelligence Admeasure with Unpredictable Password Mechanism

Yelakapati Estheru Rani
Persuing M.Tech,
Department of Computer Science &Engineering,
A1 Global Institute of Engineering & Technology,
Markapur, Prakasham District.

PatanYasdhani Khan
Professor,
Department of Computer Science &Engineering,
A1 Global Institute of Engineering & Technology,
Markapur, Prakasham District.

Abstract:

Cyber-crime is regarded as most serious problem for any technological development and new application sustainment. The hackers are day to day increasing their strengths with different kinds of attacks to record possible damage to the corporate customers as well as individual sensitive information. Predominantly the artificial Intelligence assistance has been taken by Cyber-Criminals to break any kind of textual passwords and eavesdropping the sensitive and confidential information from the application servers. To admeasure the attitude and stealing behavior the present project has given solution with unpredictable click points on photo images selected as the passwords for the application.

Key words:

Textual Passwords, Graphical Passwords, Cued Click Points as passwords, Guessing Attacks.

Introduction:

Guessing attacks predominantly affected the business of B2B. The financial transactions of the banks should be kept online. So that the business of the banks will get improved. To keep the financial transactions a strong online security mechanism should be developed. The need of a security mechanism for financial transactions conducted by the financial institutions is very high. The security mechanism should act against the guessing attacks. Guessing attacks are more powerful and breaking the passwords of the online financial transactions and stealing the data. The present proposed project is development of a security mechanism against the guessing attacks.

The proposed project is also creating a security layer for the financial transactions and obstructs the intruders into the financial online applications. The project is developed to cater the security needs for online applications. The stakeholders of the project are online application users. The application is developed in the field of security domain. The application is replicating the novel concept of graphical password authentications with persuasive click points. The sphere of the project is wide and used universally and shows a solution for guessing attacks, Brute Force Attacks and Dictionary attacks.In this mechanism the user perception and creativity is going to play a high security implementation to the application. The user click points will be stored in the database with x axes and y axes points. The user has to select random click points on the image.

The number of click points also limited and restricted by the application. The selected click points are stored in the application with x axis and y axis parameters. When the user login to the application second time and repeatedly the application will ask the user to select the image with click point. The user has to select the previously selected image and give clicks on the image with appropriate click points which have already given on the image. The points will be verified and tallied with the stored click points. If the points are tallied, then the application will allow the user into the application. This has given revolutionary change in the field of web application security.

Project Contribution:

The present report is on A New Authentication Mechanism Based on Graphical Password. The project is a novel piece of work in the field of online application security and system security.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The project is defining the new way of defining the passwords to operate an online application. The project is going to give a novel methodology for implementing new password system to online users. By using this novel concept of using graphical passwords with persuasive cued click points the passwords will be preserved with great privacy and can't be guessed by any attacker of online application. The project will be contributing well to the field of security authentication and application security. The project method is novel and paved the way to restrict the guessing attacks, Brute Force Attacks and Dictionary attacks.

Literature Review:

Authentication is a process, to distinguish the identity of the user to access the specific application. This identification process can be incorporated with the user name and password storage and verification methods. The attackers guess the password according to the name, environment, working culture, qualification and other standard memorable events of the person. The human brain generally remember the events and objects which are mostly acquainted to the person. This phenomena can be adopted by the hackers and apply guessing attacks, Brute Force Attacks and Dictionary attacks. In this technology an advancement has been generated in the form of Persuasive Cued Click Points.

This technology has removed the fears from guessing attacks. This mechanism will set the password of the user with high security and privacy with the help of image cued click points position viewport.'Gloriya Mathew [2013] The security to the online application or desktop application will be incorporated by the passwords. The password was generated from text based characters. Then it has been advised to mix special characters. Then the knowledge based passwords have come into the practice. Similarly in token based passwords are distinguished as tokens for identification, smart card identification, keys identification and finally chip impulsive identification.

The biometric identification is classified as finger print identification, palm prints identification, Hand geometry identification, face recognition, voice recognition, Iris recognition, retina recognition. All these biometric impressions are stored in the database at the first registration and then the verification process will be done when the person is log in into the system.

In Image recognition password system Hong's method is predominant. In this method the user will pass-object variants will be used for graphical password scheme. 'Chippy.T and R.Nagendran' [2012]The alternative mechanism for textual passwords has been successfully implemented to arrest the guessing attacks on online applications. The textual passwords can be cracked by the intruders and eavesdroppers. The graphical passwords with persuasive cued click points are easy to remember for online users and difficult to crack the passwords for online intruders. This graphical password is providing increasing security to the online applications. G.ManiMayuri, et.al [2013]

Research Approach:

Research approach reveals how the project work will be developed and how the required knowledge can be acquired. To design and develop the project the domain knowledge is required. The functionality has to be understood. The technology to develop this project is mastered. The proficiency development in the technology required for the project development is essential. The present project is Defenses against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points. To design and develop the project the predominant research methods have been implemented. These are Quantitative Research Method, Qualitative Research method, Experimental Research Method, case study method and Action research method. The research methods have been understood and adopted for doing the dissertation work. Saunders et.al [2006].

Description of the project:

The project is developed to demonstrate the persuasive click points usage to prevent the guessing attacks for online applications. This project is designed to demonstrate the web application which will be operated with a login page to insert the persuasive click points on an image along with user name and password to enter into the application.

Module specification:

The following modules are present in the project.

1.User
2.Administrator

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

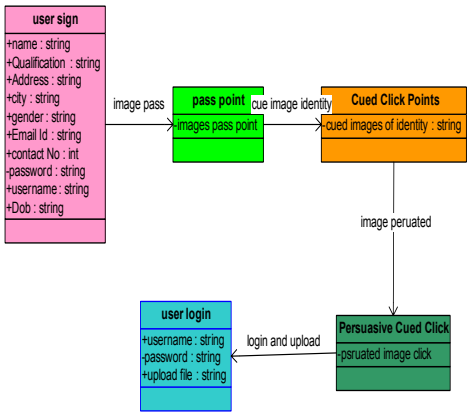
Functionality of the Modules:

User module is used to select an image for identification of persuasive cued click points on it. The user is designed to enter the user name and password for login to the application. The user has to register with the application to give all details of the user. The user has to select the image for his password authentication. The persuasive cued clicks have to be defined for every login operation. Administrator module is designed to keep variety of images for user. The administrator will create a database to restore the user name and password into the database. The administrator will view the number of users logged into the application.

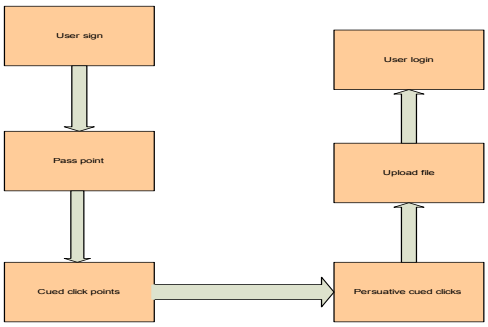
Functionality of the project:

The project is designed to demonstrate the highest grade of security provision for online applications. The security is given against the guessing attacks. This has been incorporated with the persuasive cued click points on an image selected by the user along with the user name and password. The present project security mechanism is combined with textual passwords along with the image passwords with persuasive cued click points. The project is an online application with security mechanism to protect the application from guessing attacks. The project is predominantly highlighting the security mechanism with image passwords, textual passwords and persuasive cued click points.

Class diagram



Data flow diagram



Code behind the technique:

The most important and critical issues have to be encountered are in developing the code behind the technique. The code behind the technique is developed with ADO. Net controls, ADO.Net classes, C#.Net codes and stored procedures. The project is a web based application so that the ASP.Net application screens have to be connected with the database server tables. Each table and the attributes of the table are to be connected with the respective user interface screens. The connection strings and connection mechanism is developed with the C#.Net code and ADO.Net statements and classes. The development of code behind the technique is difficult. This has been achieved with the help of experimental research methodology until the connection is properly established. This trial and error mechanism has given the clear connection with the database.

Conclusion:

The revolutionary experimental research work has been done in incorporating the security with encrypted mechanism. The revolutionary changes and innovative changes have been done in deploying advanced digital encryption standards. The digital encryption standards have been deployed to hide the real password of the user and tried to protect the interest of online financial application users. All the trails have become in vain. Even digital encrypted textual passwords also decrypted with the wise characteristics of hackers and intruders.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The hackers again started looting the valuable data of the financial organizations. The hackers and attackers have adopted sophisticated cracking techniques for textual passwords and intrude into the applications and caused irrevocable damage to the application storing data.The online applications are enriched with the security by introducing the persuasive click points on the image. The user is given clear instructions to select the click points very casually on the image at non attractive and not significant points. This selection of image and selection of normal and casual points on the image has highly reduced the guessing capability of the hackers and intruders. This mechanism has drastically reduced the guessing attacks on the online applications.In this mechanism the user perception and creativity is going to play a high security implementation to the application. The user click points will be stored in the database with x axes and y axes points. The user has to select random click points on the image. The number of click points also limited and restricted by the application. The selected click points are stored in the application with x axis and y axis parameters.

References

Books

9.1.1. Persuasive Advertising - Author : J.Scott Armstrong
9.1.2. Picture password authentication using cued click points - Author : Harikrishnan Nair
9.1.3. Graphical User Authentication (GUA): Graphical Password Algorithms and Analysis Published in – December 3, 2010 by ArashHabibiLashkari (Author) , FarnazTowhidi (Author)
9.1.4. A Calculus to Detect Guessing Attacks by BogdanGroza, Marius Minea Published in 2009.

Articles

» S Chiasson - 2012 - Cited by 29 - Related articles on Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication
» May 10, 2012 - home • articles ... Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism ... users to select more random, and hence more difficult to guess, click-points.
» essays, articles and other content including Persuasive Cued Click-Points: ... Posts from DIGG that contains the high definition-digital video disc

Previous Research Published Papers

1.Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE [2011] Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism downloaded from http://hotsoft.carleton.ca /~sonia/content/ Chiasson_tdsc_pccp_author_copy.pdf

2.D.AnuRadha [2013] A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks Published by: PIONEER RESEARCH & DEVELOPMENT GROUP(www.prdg.org) IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791

3.Gloriya Mathew, Shiney Thomas [2013] "A Novel Multifactor Authentication System Ensuring Usability And Security" - Published In Computer Science Journal

4.Chippy.T and R.Nagendran [2012] DEFENSES AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS BY USING PERSUASIVE CLICK POINTS published in International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012

5.Ms. Resmipriya M G Ms. Sangeetha N [2013] "An Efficient Approach for Preventing Online Password Guessing Attacks" International Journal of Computer Science and Management Research Vol 2 Issue 3 March 2013

6.Seth Thigpen [2005]Authentication Methods Used for Banking Published in East Carolina University articles

7.DharmendraChoukseUmesh Kumar Singh Deepak SukhejaRekhaShahapurkar [2010] Implementing New-age Authentication Techniques using OpenID for Security Automation International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010

8.Hafiz ZahidUllah Khan [2010] Comparative Study of Authentication Techniques International Journal of Video& Image Processing and Network Security IJVIPNS-IJENS Vol:10 No:04 9 103304-2929 IJVIPNS-IJENS © August 2010 IJENS I J E N S

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

9.G.ManiMayuri, S.Vineela Krishna, M.Tech[2013] Graphical based Secure Authentication System for Online Applications published in International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 8–August 2013

10.Wayne Jansen,SerbanGavrila, VladKorolev, Rick Ayers, Ryan Swanstrom [2003]Picture Password: A Visual Login Technique for Mobile Devices published at Information Technology Laboratory, National Institute of Standards and Technology

11.Serena [2007] An IntroductIon to AgIle Software development.

12.Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. van Oorschot [2012]Persuasive Cued Click-Points:Design, implementation, and evaluation of a knowledge-based authentication mechanism.

13.Iranna A M1,PankajaPatil [2013] Graphical Password Authentication Using Persuasive Cued Click Point. Published in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.

14.Kailas I Patil, JaiprakashShimpi [2013] A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devicespublished in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013 155.

15.Head of W3C Greece Office, Associate Researcher, Institute of Computer Science-FORTH

16.Glenford J. Myers (2013)The Art of Software Testing, Second Edition Revised and Updated by Tom Badgett and Todd M. Thomas with Corey Sandler