ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

I forget mobile (IFM) web application using persuasive cued click point technique

A. M. Khemnar[1]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

M. S. Padir[2]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

R. S. Walse[3]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Kiran P. Somase[4]
Assistant Professor
Department of Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Abstract: ***We are so dependent on our mobile phones that when we forget them at home it seems we've lost a limb. When this happens, it would be nice to access your mobile from, say, any web browser. An application that used Simple Object Access protocol(SOAP), is a protocol specification for exchanging structured information in the implementation of web services .It relies on XML Information Set for its message format to the web service .An application is used both to access the mobile phone and retrieves all your call log contains the received call ,miscall ,dial call etc and also perform location tracking Using GPS and messages .We can also send the remote messages with help of his web site from your mobile .***

We also used Persuasive Click-Points graphical password scheme for the authentication, including usability and security evaluations, and implementation considerations.. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click point.

Keywords: Simple Object Access protocol, web services, Global Positioning System, International Mobile Equipment Identity.

I. INTRODUCTION

This project is basically an idea to operate through an android mobile and access the data into system only login in functionality. The project consists of the Accessing the data with the help of website or mobile though android SDK. Mobile data backup is the most up-to-date backup solution for the moment being with the Mobile backup service you won't have to worry about your data security, buy hardware and install software to back up your data. Moreover, the software backup saves time. And for the authentication purpose of this web application we use the Graphical authentication technique.

The problems of text-based passwords are well known to us. User often creates memorable passwords that are easy for any unauthorized person to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication in which the system allows user choice while influencing user towards stronger and secure passwords. In our system, the task of selecting weak passwords (which are easy for unauthorized one to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes user to choose a more secure password the path-of-least-resistance. Rather than increasing the burden on users it is easier to follow the system's suggestions for a secure password, a feature lacking in most of the schemes. We applied this approach to create the persuasive click-based graphical password system and compared PCCP scheme to text passwords and two related graphical password systems. Results show that PCCP is effective at reducing hotspots

(areas of the image where users are more likely to select click-points) and avoiding patterns formed by click-points within a password, while still maintaining usability.

II. BACKGROUND

If we forget mobile at home then we can see our mobile details only when back to home. There is no efficient access to see our mobile details like call logs, messages, also we give reply to messages, contact information etc.

There are lots of web security problem occurs. In order to provide security to the web application that we developed i.e. IFM web application we use persuasive cued click point technique. In general, graphical passwords techniques are mainly classified into two main categories : recognition-based technique and recall based technique. In recognition based, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected earlier during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage. Graphical passwords offer another replacement, and are the point of focus in this paper**.**

III. SYSTEM ARCHITECTURE

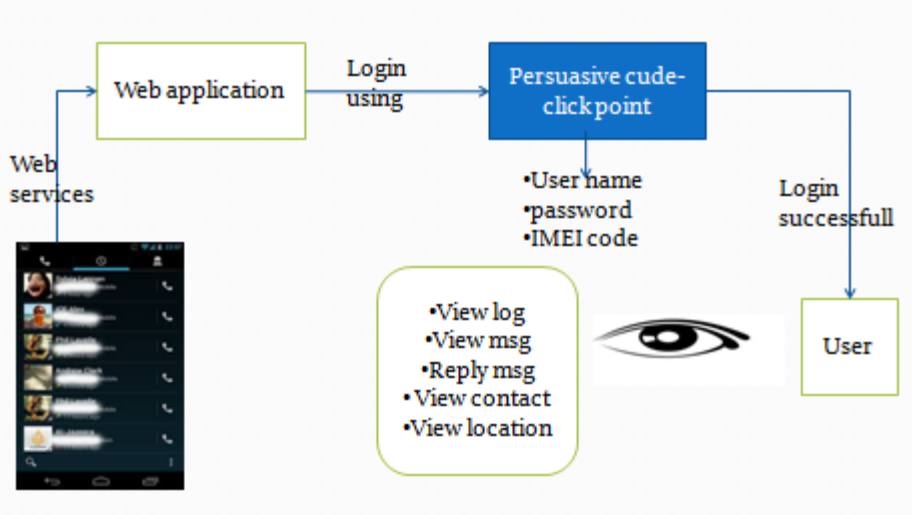

Fig: System architecture

Here we developed the web application, using which user see our mobile details. At the time of registration on the web application user wants to enter user name, password, and IMEI code of mobile. On the web application the user is already register. Here the user mobile and web application where user sees our mobile details both are in network. The architecture for image hot spot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Initially authorized user need to identify the exact hot spot from the image. In earlier algorithm nearly five hot spot is used. Since this process has high probability of finding the password, proposed system with one hot spot password is designed .The user is asked to click the exact point and to confuse the hackers for each hot spot clicked, a duplicate image is generated so that hackers found difficult for accessing the password. Second step is once hot spot is clicked a matrix with list of alphabet is displaced user need to choose the character with intersecting points. To make the process more difficult for hackers each time a new matrix is generated. In this method user created two passwords one is textual password and another one is graphical password. In graphical password particular hot spot is allowed to click by using segmentation algorithm spot from the image is compared and alpha numeric matrix algorithm used. Textual Password allows the user to select password from the matrix this is more advantageous since each time a new matrix is generated.

IV. SYSTEM MODULES

A. PERSUASIVE CUED CLICK-POINT MODULE:

Graphical password scheme for the authentication, including usability and security evaluations, and implementation considerations. We propose is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. The proposed system work merges persuasive cued click points and password guessing resistant protocol. Example systems include Pass Points (PP) and Cued Click-Points (CCP).

Pass Point (PP):

In Pass Points, passwords consist of a sequence of five click-points on an image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although Pass Points is relatively usable security weaknesses make passwords easier for attackers to guess. Hot spots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully predict Pass point passwords. Predictable patterns which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against Pass Point based on image processing techniques and spatial patterns are a threat.

Cued Click-Points (CCP):

A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously selected click-point (figure.3), creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click -point results in a different image sequence.

The claimed advantages are that password entry becomes a true cued-recall scenario based, where in each image triggers the memory of a corresponding click point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP, so pattern-based attacks seem ineffective. Although attackers must perform proportionally.

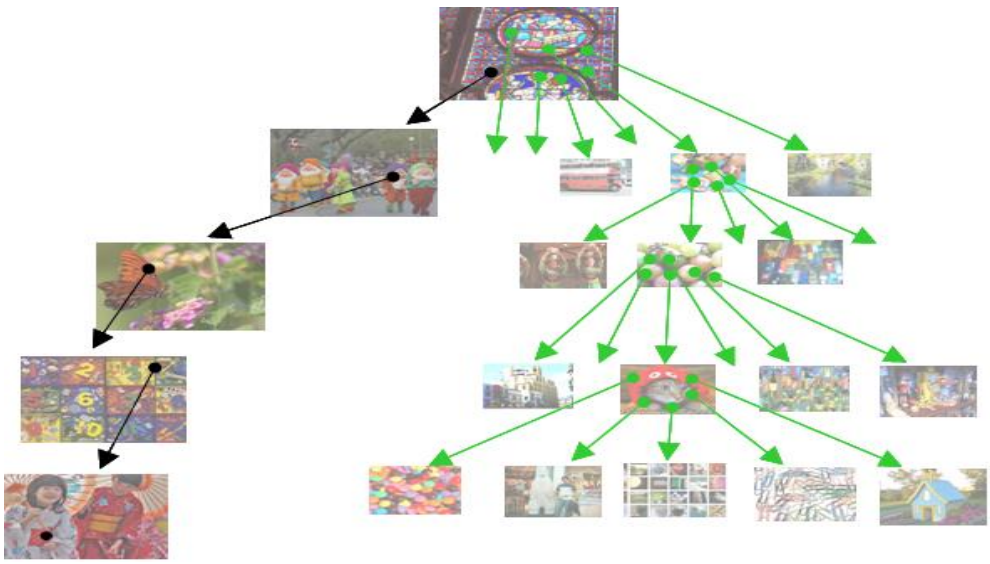

Fig: Cued clique point

B. MOBILE DATA BACKUP MODULE:

Is the most up-to-date backup solution for the moment being? With the Mobile backup service you won't have to worry about your data security, buy hardware, and install software to back up your data. Moreover, the software backup saves time. it contains

- View all mobile logs.
- View SMS
- View Contact

C. MOBILE PHONE TRACKING MODULE:

Refers to the attaining of the current position of a mobile phone, stationary or moving. Handset-based technology requires the installation of client software on the handset to determine its location. This technique determines the location of the handset by computing its location by cell identification, signal strengths of the home and neighboring cells, which is continuously sent to the carrier. In addition, if the handset is also equipped with GPS then significantly more precise location information is then sent from the handset to the carrier.

D. REMOTE SMS MODULE:

We can also send the remote messages with help of his/her web site from your mobile.

E. DATA SECURITY MODULE :

In this module with the help of AES algorithm store the mobile data in cipher text into the database for the purpose of security.

V. CONCLUSION

IFM web application is implemented so that user can see his/her mobile details using web application and it also provide better security using persuasive cued click point technique. Using Web application user can see mobile massages, call logs like received call, dial calls, miss call, provide application for mobile tracking with the help of this user can find lost mobile. In this paper the Persuasive Cued-Click Point graphical password technique is mainly useful for authentication purpose. The advantages of this technique are increasing usability and security by providing password of higher security. The goal of Persuasive cued click point is to encourage and guide user to select better password while still maintaining memorability. Persuasive cued click points increases the workload for attackers and the system's flexibility to increase the overall number of images in the system that allows us to arbitrarily increase this workload. The approach has proven effective at reducing the formation of hotspots, avoiding pattern formations and also provides high security.

References

1. Android a programmer guide Author: J.F.DiMarZio.
2. Professional android application development system
3. MyBookDroidhttp://mybookdroid.blogspot.com/
4. Book Catalogue and Book log. Book Catalogue (by Evan Leybourn)
5. http://wiki.github.com/eleybourn/Book-Catalogue/
6. Beginning android tablet development
7. Professional android 2 application development book review Butler, M.; IEEE Pervasive Computing, "Android: Changing the Mobile Landscape"Volume: 10, Issue: 1, Digital Object Identifier: 10.1109/MPRV.2011.1 PublicationYear: 2011, Page(s): 4 – 7
8. "Sharing Enriched Multimedia Experiences across Heterogeneous Network Infrastructures" IEEE Communications Magazine June 2010.
9. Damianos Gavalas and Daphne Economou, University of the Aegean,"Platformsor mobile Applications: Status and Trends" IEEE SOFTWARE, JANUARY/FEBRUARY 2011
10. "Development of agent-based, peer-to-peer mobile applications on ANDROID withJADE." The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. DOI 10.11.09

AUTHOR(S) PROFILE

Miss. Archana Khemnar, currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). She is also good in programming.

Miss. M. S. Padir, currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). She is also good in presenting the technical topics.

Miss. R. S. Walse, currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). She is good in academic and she is punctual.

Prof. Kiran P. Somase, received the Diploma in Computer Technology from K.B.P. Polytechnic, Kopargaon in 2006, B.E. degree in Computer Engineering from SRES College of Engineering, Kopargaon in 2009 and M.Tech in Computer Science Engineering from Rajasthan Technical University, Kota. He is having 5.1 years of experience in teaching and also presently working as an Assistant Professor at Jaihind College of Engineering, Kuran (Savitibai Pune University, Pune).

