Volume 3, Issue III, March 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Authentication using RFID and PCCP Application for Mobile Devices

Sayli Pradhan[1], Prachi Pandya[2], Rinita Nair[3]

[1]Dept. of Computer Engineering,
K.J.Somaiya College of Engineering, Mumbai 400077
sayli.p@somaiya.edu
[2]Dept. of Computer Engineering,
K.J.Somaiya College of Engineering, Mumbai 400077
prachi.p@somaiya.edu
[3]Dept. of Computer Engineering,
K.J.Somaiya College of Engineering, Mumbai 400077
rinita.nair@somaiya.edu

Abstract: *In the contemporary world, where in we have explored the universe of computing, there have been rising concerns about the security of the data under usage. It is far more imperative to protect this data from the so called, 'nefarious people'. This paper aims at satiating the growing needs of security not only through the use of a Byzantine application but also integrating it with hardware. There by, introducing the user with a whole new dynamic domain of security. The paper touches upon the potential application domain of the proposed system.*
Keywords: *Au - Ring, Mob – Reader, RFID, CCP, PCCP, IDE, ADT, SDK, UI, UML.*

1. INTRODUCTION

Authentication has been perceived as that process of a system which enables it to substantiate a user trying to gain access to the system. This complex age of computing has brought about a massive revolution in the authentication systems. We have delved in three major categories of authentication systems viz. Biometric Based Authentication (BBA), Knowledge Based Authentication (KBA) and Token Based Authentication (TBA). BBA deals with finger prints, palm prints, iris recognition, voice recognition, retina recognition. Known for its accuracy but the very foundation of this authentication is use of complex and very expensive technologies. Thus the triads of CIA (Confidentiality, Integrity and Availability) are difficult to achieve in the day to day lives of common people. KBA, a popular method of securing data through text and graphical passwords [2], but with this comes into picture the privacy issues of the customer in consideration. Largely based on the fact of, 'Something you know' is always going to be dangerous if the victim is well known to the attacker.

In this paper, we intend to integrate KBAM [6] and TBA, which we would refer as, 'Squared Authentication'

2. PROPOSED SYSTEM

The proposed system is aiming at bringing about a whole new perspective of visualizing the authentication process through 'Squared Authentication'.

The system can be represented with the help of Fig. 01 as shown below. The initialization of this proposed system starts with pressing the power button or the unlock button of the mobile device under consideration and then connecting the Au - Ring, a RFID chip integrated ring, with the rear side of the mobile device, where a Mob- Reader, a RFID reader in – built in a mobile device, will verify the user.

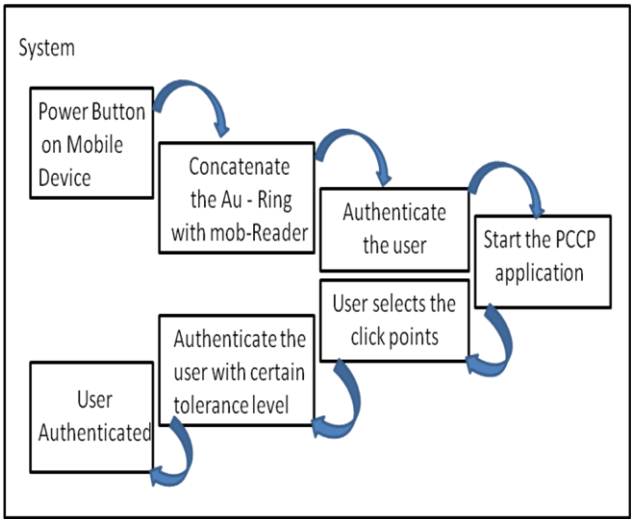

Fig. 01: Block Diagram of the Proposed System

Once, the user is substantiated, an application starts, known as PCCP (Persuasive Cued Click Points) application [1]. PCCP application has its roots engrained in Cued Recall [3] Based Techniques one of the Knowledge Based Authentication techniques.

When the user is signing up for the first time to the PCCP application, he or she is asked to select five images or it could be made dynamic by asking users the number of images, which can be imported from the gallery or camera and for each and every image selected he or she has to select one click point.

This click point will be saved in a database that consists of the image and the corresponding co - ordinates. A dynamically induced viewport [7] is present which will be used to help user get a precision over selection of the click points in the entire image. Since, it is likely that a user will

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

always select guessable click points. Thus a predefined rectangle will always be present to help user click on selective portion of the image only. If the user finds the portion to be more complex there is a shuffle button that dynamically and randomly changes the position of the rectangle.

The beauty of the system lies in the smartness of tricking the attacker with continuing the system even if the choices made during the selection of the click points was wrong. The order in which the user during sign up selected images appears only if the choices during the logging in the system are perfect. If at any point during login process does the attacker by mistake clicks the wrong click point, the system starts drifting away from the sequence of correct images without any notification of the error caused in selection process during runtime. It is only after the five images selected appear that the user will come to know if the login was successful or unsuccessful.

This leaves the attacker without any clue as to where he or she goes wrong in the entire hacking process.

Another impressive feature to this system is the actively involving the day to day sturdiness of the usage that common person faces. A specific tolerance level is associated with each click point. A slight variation in selecting the click point is considered and treated with respect. Any authentication system can easily thus consider 'Squared Authentication' as an epitome technology.

2.1 Overview *of the components*

The proposed system consists of the following hardware and software components:

1) Mobile Device: An android OS enabled mobile device is considered for running the entire system
2) RFID enabled Au – Ring: This ring will have an embedded RFID chip which will be helpful in the initial stages of authentication
3) Mob – Reader: The mob – reader will send EMR Radiations to the Au – Ring and then verify the user.
4) Android SDK and Eclipse: A software development kit and IDE respectively required for the coding of entire PCCP application.
5) Database: A database would be required to store the information about the images and their co- ordinates.

Proposed Implementation:

The Fig. 02 shows the flow of the implementation of the system under consideration.

The entire process of the 'Squared Authentication' can be visualized as Authentication by Au – Ring, followed by the Authentication of the user using the PCCP software application.

The flow gives the feel of entire process right from the word 'go', wherein we find the user registering for the system and then using the system in the subsequent endeavors.

Soon after the registration, it is evident that the user is automatically signed off. Thus, after registration it is important that the user does sign in again to use the device under consideration.

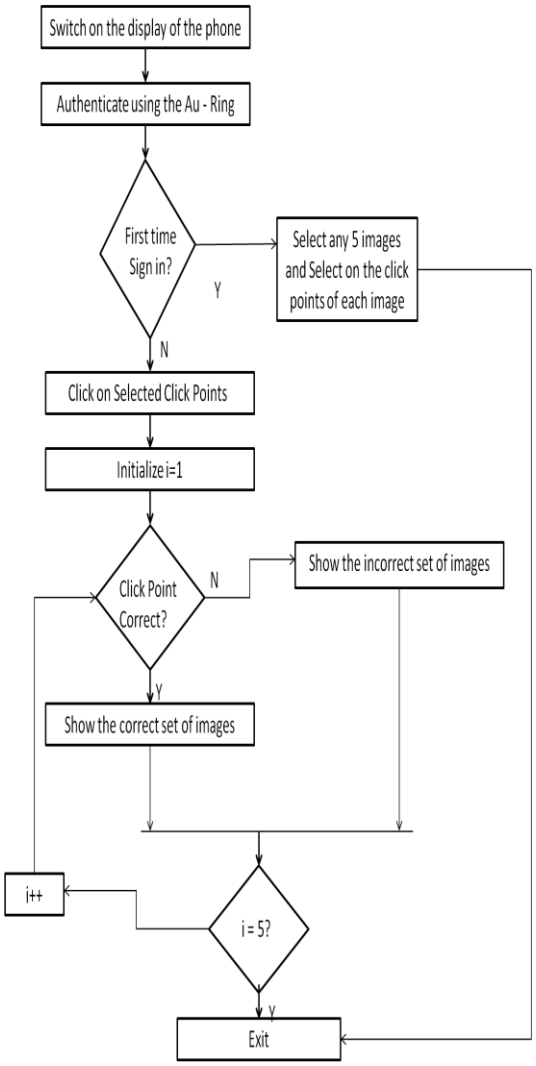

Fig. 02: Flow – chart of 'Squared Automation'

3. LITERATURE SURVEY

The current scenario of authentication systems in recall based algorithms basically consists of Pass point, Pass map, Cued Click Points, Persuasive Cued Click Points.

Pass Points: S. Wiedenbeck proposed pass-point graphical password scheme in which password consists of a sequence of 5 different click points on a given image. During password creation user can select any pixel in the image as a click-points and during authentication the user has to repeat the same sequence of clicks in correct order within a system defined tolerance square of original click-points. Pass-point used the robust discreatization [5] technique.

Pass Maps: Main problem with passwords is that good passwords are long and hard to remember and the one which are easy to remember are too short and simple making it less secure. It is relatively easy to remember landmarks or road on a well-known journey. In pass-map, a user can select different places that he wants to visit or the places he likes as click-points.

Cued Click Points: Cued click points (CCP) technique was proposed by S. Chaisson. CCP reduces the HOTSPOT and

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

pattern formation attack. In CCP user chooses one click point on five different images instead of five click-points on one image. The next image to be displayed is based on previous click-point. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For legitimate users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point. CCP also used the robust discreatization technique.

PCCP: In this scheme when the image is displayed the randomly selected block called the viewport only clearly seen out. All the other parts of the image are shaded, so that the user can click only inside the viewport. This is how the PCCP [1], [4] influence the user to select the position of the click point. The viewports are selected by the system randomly for each image to create a graphical password. It will be very hard for the attackers to guess the click point in all the images.

4. APPLICATION

The system has been created by a fusion of two extremely different domains of authentication (Knowledge Based Authentication and Token Based Authentication) which indeed in absolute blessing in disguise for the massive fields of mobile computing, laptops and every digital gadget where in huge volumes of data are stored and processed.

Not only is it going to be beneficial in the terms of computing but also where sensitive data is involved like the strategic military formations in army, air – force, navy during sudden or anticipated attacks in bellicose circumstances.

5. CONCLUSION

Just the way, camera enabled mobile phones have dramatically reframed the way we look at lives around us, similarly such a fusion is going to have a huge impact in terms of safety, security of every confidential information available. There by, providing an impetus to a digitally safe and sound world. There would be particularly tremendous potentials of securing data against such '*nefarious people'*.

REFERENCES

[1] S.Chiasson, E.Stobert, A.Forget, R.Biddle and P.C. van Oorschot, "Persuasive Cued Click-Points: Design Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Transactions on Dependable and Secure Computing, VOL. 9, NO. 2, 2012,pp. 222-235.

[2] M.S. Umar, M.Q Rafiq and J.A. Ansari, "Graphical User Authentication: A Time Interval Based Approach", IEEE International Conference 2012.

[3] A. H. Lashkari, F. Towhidi, Dr. R. Saleh and S. Farmand , "A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms", 2009 Second International Conference on Computer and Electrical Engineering, pp.527-532.

[4] Smita Chaturvedi and Rekha Sharma, "Securing Image Password by using Persuasive Cued Click Points with AES Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014.

[5] http://link.springer.com/chapter/10.1007/978-3-540-74835-9_24

[6] Uma D. Yadav, Prakash S. Mohod, "Adding Persuasive features in Graphical Password to increase the capacity of KBAM", IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology 2013

[7] Iranna A M, Pankaja Patil, "Graphical Password Authentication Using Persuasive Cued Click Point", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.