International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:6, 2016

Hybrid Authentication System Using QR Code with OTP

Salim Istyaq

***Abstract*—**As we know, number of Internet users are increasing drastically. Now, people are using different online services provided by banks, colleges/schools, hospitals, online utility, bill payment and online shopping sites. To access online services, text-based authentication system is in use. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. The core element of computational trust is identity. The aim of the paper is to make the system more compliable for the imposters and more reliable for the users, by using the graphical authentication approach. In this paper, we are using the more powerful tool of encoding the options in graphical QR format and also there will be the acknowledgment which will send to the user's mobile for final verification. The main methodology depends upon the encryption option and final verification by confirming a set of pass phrase on the legal users, the outcome of the result is very powerful as it only gives the result at once when the process is successfully done. All processes are cross linked serially as the output of the 1st process, is the input of the 2nd and so on. The system is a combination of recognition and pure recall based technique. Presented scheme is useful for devices like PDAs, iPod, phone etc. which are more handy and convenient to use than traditional desktop computer systems.

***Keywords*—**Graphical Password, OTP, QR Codes, Recognition based graphical user authentication, usability and security.

I. Introduction

ONE of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. Psychology studies have revealed that the human brain is better at recognizing and recalling graphical images than text. Computer security systems must also consider the human factors such as ease of use and accessibility [15]. Current secure systems suffer because these mostly ignore the importance of human factors in security [1]. An ideal security system considers security, reliability, usability, and human factors. All current security systems have flaws which make them specific for well trained and skilled users only.

A password is a secret that is shared by the verifier and the customer. "Passwords are simply secrets that are provided by the user upon request by a recipient". They are often stored on a server in an encrypted form so that penetration of the file system does not reveal password lists [2]. Passwords are the most common means of authentication because these do not require any special hardware. Typically, passwords are strings of letters and digits, i.e. these are alphanumeric. Such passwords have the disadvantage of being hard to remember. Weak passwords are vulnerable to dictionary attacks and brute force attacks, whereas strong passwords are harder to remember.

Salim Istyaq is with the Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, Aligarh Muslim University, Aligarh-202002, U.P., India (phone: +919412563748; e-mail: saleemishtiyak@gmail.com).

A. Methods of Authentication

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication [4]. Currently, the authentication methods can be broadly divided into three main areas Fig. 1

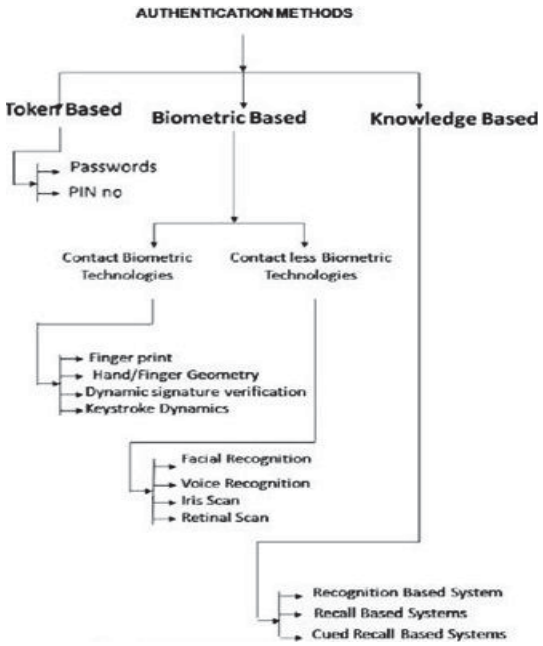

Fig. 1 Classification of Authentication Methods

B. Classification of Current Authentication Methods

Token based techniques [8] such as keycards, bank cards and smart cards are widely used for security purposes. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques [9] such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. Such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques [8], [9] are the most widely used authentication techniques which include both text and picture based passwords. The picture-based techniques can be further divided into two categories recognition-based and recall based graphical technique [14].

II. Related Work

Graphical passwords were originally described by Blonder [7]. In his description, an image will appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked, the user would be authenticated. Graphical password is an authentication system that works when the user selects from images, in a specific order, presented in a graphical user interface (GUI). Graphical user authentication (GUA) is the term used for graphical password that contains authentication method via graphical interface. Many techniques have been designed in the field of graphical password since 1996 [7].

Today, authentication technology is the main measure to guarantee information security [9], and the most common and convenient authentication method is alphanumeric password. GUA is a promising alternative to replace the traditional alphanumeric password way of authentication. The main motivation lies with the fact that the human brain is capable of remembering graphical or pictorial objects better than texts. Even psychological studies support such assumptions [16]. Also with the advancement of technology, we are now moving forward to use touch based devices such as mobile phones, tablets, and even touch screen monitors. So with this, the alphanumeric method is much more inconvenient in such devices. So, the graphical method would allow the user to just touch the various regions in screen and get authenticated. It is slightly too much difficult to crack graphical password [6]. Jansen [8] proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numeral [12].

Pass face [10] techniques supported by the fact that human brain can quickly recognize familiar faces. During registration user has to select 4 faces. The registration is completed if the user correctly identifies 4 pass faces two times consecutively. During login, user is presented with a login screen consisting of grid of faces. User has to select 4 faces: one face from each of 4 grids of 9 faces. Pass faces can be predictable as they are affected by race, gender and attractiveness.

Syukri et al. [11] propose a system where authentication is conducted by having the user drawing their signature using a mouse. There are techniques included two stages, registration and verification. During the registration stage: The user will first be asked to draw their signature with a mouse, and then the system will extract the signature area and either enlarge or scale-down the signature, and rotate if needed (also known as normalizing). The information will be saved later into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. After that the system conducts verification using geometric average means and a dynamic update of the database. According to the paper, the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize ones' signature and signatures are hard to fake.

Dhamija and Perrig [12] proposed a graphical authentication scheme based on the Hash Visualization technique. In their authentication system, user selects a certain number of images from a set of program generated random pictures. For a user to be authenticated, he or she would have to identify the preselected images. One weakness of their system is that the server needs to store the seeds of the selected images of each user in plain text. Also, it is a bit time consuming and tedious for the users to select images from the database.

III. Proposed Work

The graphical password [3] is not widely deployed in real systems due to the problem of shoulder surfing. The other vulnerabilities of graphical passwords are still not fully understood. In this paper, we define a way of protecting the information from shoulder surfing attack that is combining QR based graphical authentication scheme with One Time Password scheme which is implemented in the authentication [13] system to avoid shoulder surfing.

Steps for proposed authentication system:

(a) First the user has to register with the website application or service etc. Then user will go through a first time user registration process.
(b) At the time of registration process, the user will be asked to select the QR code which will be easy to remember. The code will read by QR scanner or any other application in devices, which are used to read QR codes.
(c) Any time authentication is required; the user will enter his/her User_ID/Login_ID (a unique identity to be allocated). Then he clicks validate user button. For a valid user a Secure One-Time Password (numeric) will be sent to his/her registered Mobile/E-mail.
(d) The user is also presented with a randomly generated grid of QR images as shown in Fig. 3. The pictures that appear are different every time, but the user will always look for their same categories. Each picture is randomly paired with a different alphanumeric character. In this way the system generates a unique, one-time password every time. Yet the user only needs to remember their few categories.
(e) The user authenticates by identifying which QR on the grid fit their secret authentication categories. They can simply click on the appropriate QR images, or type the alphanumeric characters that appear on the correct QR to form a one-time password (Graphical).

(f) Also the user will have to give the One Time Password (numeric) sent to his/her mobile/E-mail as shown in Fig. 2.

Fig. 2 OTP Login

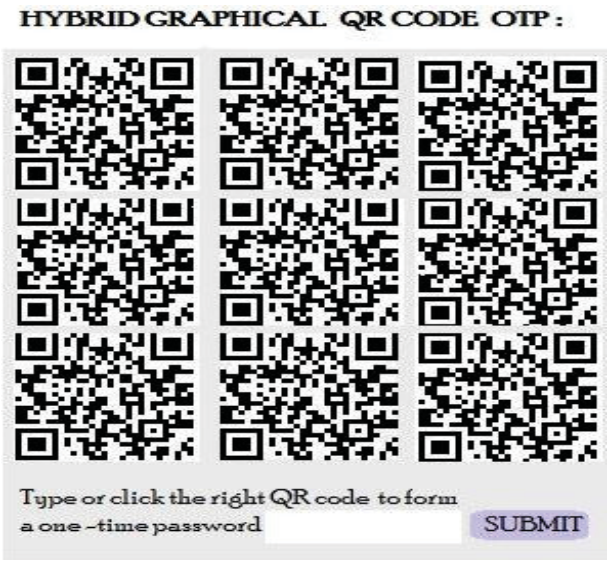

Fig. 3 QR Login Interface

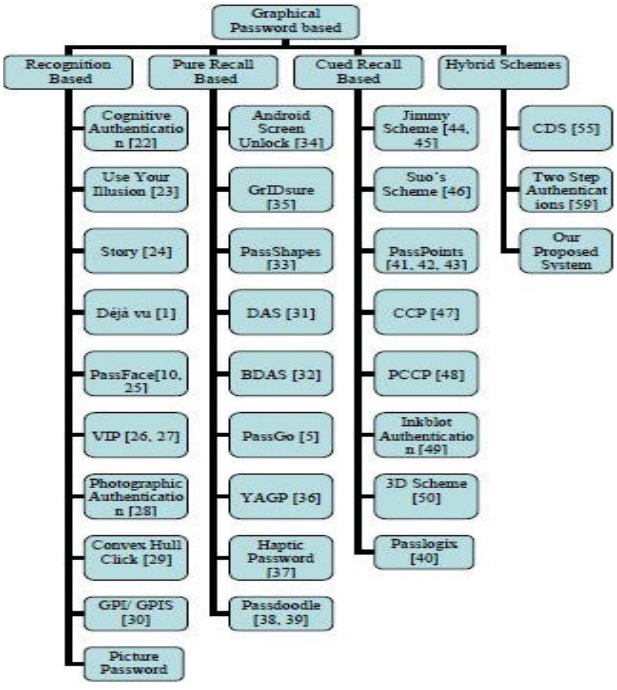

Fig. 4 Different types of system

IV. Security and Usability

Graphical Password Schemes/ Systems	Type of Scheme	Resistant to Possible Attacks					
		Brute Force Attack	Dictionary Attack	Guessing Attack	Spy-ware or Naïve Key logging	Shoulder Surfing Attack	Phishing Attack or Social Engineering
Blonder's Scheme	Recognition Based	Y	N	Y	N	Y	N
DAS	Pure Recall Based	N	Y	Y	N	Y	N
BDAS	Pure Recall Based	N	-	-	-	-	-
Qualitative DAS	Pure recall Based	N	-	-	-	-	-
Syukri Algorithm	Pure recall Based	N	Y	Y	N	Y	N
PassPoints	Cued Recall Based	Y	N	Y	N	Y	N
PassFace	Recognition Based	Y	Y	Y	N	Y	N
PassGo	Pure Recall Based	Y	-	-	-	-	-
Passlogix	Cued Recall Based	Y	N	Y	N	Y	N
PassMap	Pure Recall Based	Y	N	-	N	Y	N
Passdoodle	Pure Recall Based	N	-	-	-	-	-
Viskey SFR	Pure Recall Based	Y	N	Y	N	Y	N
Perrig and Song	Recognition Based	Y	N	Y	N	Y	N
Sobrado and Birget	Recognition Based	Y	N	Y	N	N	N
Man et al Scheme	Recognition Based	Y	N	N	Y	Y	N
Picture Password Scheme	Recognition Based	Y	N	Y	N	Y	N
CDS	Hybrid	-	-	-	-	Y	-
WIW	Recognition Based	-	-	-	-	Y	-
Association based scheme	Recognition Based	-	-	-	-	Y	-
Déjà Vu	Recognition Based	Y	-	Y	-	-	-
Haptic Password Scheme	Pure Recall Based	-	-	-	-	Y	-
YAGP	Pure Recall Based	Y	-	Y	-	Y	-
Photographic Authentication	Recognition Based	-	Y	-	-	-	-
Two Step Authentication	Hybrid	-	-	-	Y	N	Y
Our Proposed System	Hybrid	Y	Y	Y	Y	Y	Y
Note: Y= Yes resistant to attack N=No not resistant to attack							

Fig. 5 Comparisons of our system

The comparative study [5] of various systems is shown in Fig. 5. The possibilities of passwords generated in this system are very complex and depend on the random generated right QR code with other codes and finally a onetime password is to be sent on the users' mobile.

V. Conclusion

In order to protect the information from all the attacks, our aim is to provide a complex strength which overcome the attacks. We have presented a new hybrid technology in the graphical password scheme integrated with encode passphrase QR codes with OTP to enhance the stability of the system. This system is helpful when logging after a long while. By using this system, we have a challenging core for future. In upcoming days' other patterns may be used for recalling purpose like barcodes etc. Traditional text-based password can be encrypted into a string while transferring, but if pictures are encrypted into a string as well, it then reveals no advantage against text based passwords. So the question remains to be how to encode the graphical password in reality. The field is new and open for future works.

References

[1] William Stallings and Lawrie Brown. "Computer Security: Principle and Practices." Pearson Education, 2008.
[2] Authentication: http://www.objs.com/survey/authent.htm
[3] L.Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002,http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.
[4] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006.
[5] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-4 Issue-5, June 2015. Graphical User Authentication Techniques for Security: a Comparative Study Harinandan Tunga, Diya Saha.
[6] Mr. Pratik, A Vanjara,and Dr. Kishor Atkotiya, Analysis &Design 'Graphical Password Authentication Using Cryptography Algorithms' Volume: 1, Issue: 9,September 2012 ISSN - 2250-1991.

[7] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[8] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[9] W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium, 2003.
[10] Passfaces Corporation. The science behind Passfaces,White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm
[11] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse", In Third Australasian Conference on Information Security and Privacy (ACISP): Springer Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[12] Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" in Proceedings of the 9th USENIX Security Symposium, August 2000.
[13] Salim Istyaq and Lovishagrawal "A New Technique for User AuthenticationUsing Numeric One Time Password Scheme" in International Journal of Computer Sciences and Engineering (IJCSE), Volume-4, Issue-5, E-ISSN: 2347-2693 on 31 May-2016, pp. 163-165.
[14] Salim Istyaq, "A New approach of Graphical Password with Integration of Audio Signature Combination of Recall and recognition" in International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 6, Issue 4, Aug 2016, 45-50.
[15] Mohammad Sarosh Umar and Mohammad QasimRafiq, "*A Novel Graphical Interface for User Authentication on Mobile Phones and Handheld Devices"*, International Journal On Advances in Intelligent Systems, volume 4, numbers 3 and 4, pp 380 to 387, 2011 (IARIA Journals) Publication Date April 30, 2012.

Mr. Salim Istyaq (M 2016) became Member of World Academy of Science, Engineering and Technology in May 2016. The place of birth is Aligarh, U.P. India. The Author has B.Sc. Engineering in Computer, M,Tech. in Communication & Information Systems. Currently pursuing Ph.d. in Computer Engineering from Aligarh Muslim University, Aligarh, U.P. India. Presently, working as an Assistant Professor in Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, A.M.U., Aligarh-202002, U.P.-India since 2004 to till date. Earlier, worked as Guest Faculty in ECE Department, Jamia Millia Islamia, New Delhi-110025. Also worked in Computer Engineering, Al-Mergheb University, Alkhoms, Libya. So, far published 7 Papers in International Journals (one paper in World Academy of Science, Engineering and Technology) and 02 in IEEE Conferences. Review Committee Member in Editorial Board of various International Journals (World Academy of Science, Engineering and Technology, OMICS, ARSEAM, IJETAE)