Graphical Password Using Captcha

Y. Chandra Sekhar Reddy, M. Venkateswara Rao, M. Kameswara Rao,
C.V. Phaneendra Kumar, A. Anil Sai
Department of Electronics and Computers Engineering, K L University, India

Article Info

Article history:

Received Mar 14, 2016
Revised May 9, 2016
Accepted May 25, 2016

Keyword:

Captcha
Cyber Security
Dictionary Attacks
Graphical Password
Two Key Factor

ABSTRACT

In this 21st century one of the main issues to tackle was Cyber Security attack. We have numerous authentication processes like two key factor passwords, graphical passwords and many others. Text based passwords are prone to many attacks like dictionary attacks. In this paper, we have implemented a new authentication method namely; a family of graphical passwords built on Captcha technology. As graphical password addresses many security problems like online guessing attacks, relay attacks etc. Captcha is used to distinguish humans and bots. So, we use images with captcha's as one of the authentication step along with normal alpha-numeric password. It also overcomes the problems of pass points in graphical password systems.

Corresponding Author:

Y. Chandra Sekhar Reddy,
Department of Electronics and Computer Engineering,
K L University,
Email: Chandra.yarramreddy@gmail.com

1. INTRODUCTION

Today, fundamental task in security is to encrypt the password. To secure information we use a common method called password authentication [40]. Basically we use alphanumeric passwords which consist of strings of letters and digits, but these have many deficiencies in security issues. For easy to remember users tend to choose simple passwords which are short [41]. Many people use names, phone no. or any other easy phrase to remember, but they very verdict to hacking. In order to keep our data or information secure we need to make our password strong enough to the hackers for guessing [42], [43]. We use internet for many purposes for buying a small object to selling a big object without internet communication we can cannot survive fast in this modern world of development. Today every individual has his/her own communicating device like cell phone and they may use it for banking [24] purpose also which requires a high security. In our daily life we use many devices and internet like personal computers, social networking sites, E-mails and many more. For easy to remember we use one password to all our accounts which reduces security [44], [45]. Authentication determines whether user is valid or not.

In advance authentication process graphical passwords [1] plays a prominent place to secure the users account information. In graphical password methods it has different ways like pattern method [6], which was used in our mobile phones to unlock it. Text based one is the general password which consists of names, numbers or any other phrases. Alphanumeric password consists of text and numbers. Graphical password [7] consists of images for security, in which it can use for pass points, hot spots etc. In next level of advance method captcha was used, in which captcha is used to distinguish humans and bots apart. CAPTCHA [28] is acronym of Completely Automated Public Turning test to tell Computers and Humans Apart. Captcha consists of text and numbers in different font styles. In my project we have used this concept for security and develop this work.

2. BACKGROUND

We have different types of authentication steps like text passwords, alphanumeric passwords, graphical passwords [34], hotspots on images, pass points and many others. These types were easily pone to attacks. There are many types of attacks namely dictionary attacks, relay attacks, shoulder surfing [25], [26] attacks, brutal attacks etc.

1) In brutal force attack only small length passwords can be found, in this algorithm it searches all the possible elements [16] until the correct password found. It can resists to limited characters only [9].
2) In dictionary attack it involves guessing passwords from list of dictionary; it has higher possibility of guessing when it was in alphabetical order. It will have less possibility when it consists of different characters in password. It takes long time for searching according to the length of the password [10].
3) In shoulder surfing attack it refers to someone using direct observation of password by other means like video recording, key stroke [15] recording, someone watches over the user’s shoulder as user enters a password [13].
4) Phishing [11] is way in which hacker can acquire confidential information like usernames, passwords; credit information’s by creating an identical page like user access sites i.e. fake websites look like and feels like same to legitimate one and information is carried out through e-mail spoofing.
5) Pharming [12] is advanced version of phishing in which intended to redirect a website to another bogus site. It creates vulnerability in DNS server software. Compressed DNS servers are referred as poisoned.

Computers used by hackers installed with software in which it generates randomly from sequence of alphabets and finally we can get the required one at any point of time and they can use it, it’s just like token generation in banking systems etc. By clicking on the text is one type of authentication called Click-Text [4]. we user uses his/her account in public places hackers can get it by key loggers. Key loggers are software in which it can record the keys pressed by the user at the time of entering username and passwords. So this is another type of hacking technique. Super computers are those which fast in actions when compared to normal computers. They can get the information which were displayed on the screen [3] and can decode itself in order to fill the forms in registration of the user authentication and many other ways. These computers can easily grab the information which is very useful in hacking. In recent researches they found that super computers cannot get the information which was on the images.

3. RELATED WORK

3.1. Graphial Password

In graphical password [1] schema images were used as password for authentication, images were used in different techniques for authentication like pass points [17], [18], hot spot. Images were used in sequence to unlock; this records the pattern [29] of clicks on the images. Passlogix [8] are used to check user clicks. Recognition–based scheme requires identifying among decoy of images. Face recognition is one of the types of authentication refers to Passfaces. In this it stores the images of the faces in database in grid [35] section and sections were noted for verification and when it matches with the authentication time it accepts and rest it rejects.

In Draw-A-Secret (DAS) [31] user records his password by drawing on 2D grid. System encodes the sequence of grid cells along drawing path of user. Pass-Go [30] improves DAS [20] usability by intersecting grid intersection point rather than grid cells. BDAS [32], [33] adds background images to DAS to create users more complex passwords. Cued-recall scheme, an external cue is exists to memorize and enters password. PassPoints [21] is widely used click-based cued-recall scheme where clicks were recorded and have re-clicked same during authentication. Cued click point (CCP) [36] is similar to PassPoint but used one image per click, in which next image selects by function. Persuasive Cued Click Point (PCCP) [5] is extending CCP by selecting a point on image resulting in creating random click.

3.2. Captcha

Captcha is generally used to differentiate humans and bots apart. It consists of text [22] and numbers in it in different fonts. It is an acronym of Completely Automated Public Turning test to tell Computers and Humans Apart. Two types of visual Captcha are text Captcha [39] and Image-Recognition Captcha (IRC) [23]. Initial recognition is on character while rest is on non-character objects. Text Captcha is relying on difficulty of character segmentation, which is hard and expensive computationally. IRCs rely on difficulty of object identification or classification. Asirra [38] relies on binary object classification: a user is asked to identify all the cats from a panel of images of cats and dogs [19]. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application. In researches made on humans it was noticed that humans recognize images longer time when compared to phrases, number etc.

In many banking sites in order to register a user CAPTCHA's were used in order to avoid bots interference in it and make it perfectly by humans. CAPTCHA's were of different types in which small equation was given and answer has to type as conformation, equation was in image to avoid bots, which can easily solve it when they were in text format. This technique is widely used to avoid bots filling the forms. Many organizations to secure their information they use different security techniques. In our daily life we use many such techniques one of it was, during our transactions in banking through net banking after registering through our mobile phone we get alert by which we can acknowledge what has from our account at that time.

OTP is also one of the secured processes, which is another advanced step in security enhancing. In this user gets a one time password at the time of transaction and by entering the number which was generated and sent to the mobile at the required area we can continue our transaction safely. In CAPTCHA technique for visual problems person audio facility was provided. As mentioned above CAPTCHA images were resistant to Optical Character Recognition (OCR) attacks. In new method of CAPTCHA user does not require to enter text, instead user were asked to select pick or images from a decoy of images. This can be used as graphical password. We have many types of graphical password in demand. In w8 an image is used in which user has to select few point in sequence in order to access next when he/she want to login. When login he has remember the positions at which he made points in sequence and it acts as a password, it's is very hard to remember so it is not used mostly.

3.3. Captcha in Authentication

In this protocol Captcha and password are used in a user authentication protocol, which is called as Captcha-based Password Authentication (CbpA) [2] protocol to stop online dictionary attacks. CbPA-protocol requires solving a Captcha challenge validating user ID and password; user has to solve Captcha challenge before denied access. In Improved CbPA-protocol [2] only user trusted cookies were stored and applied Captcha challenge only on number of failed login attempts. In this scheme Captcha is an independent entity with text or graphical password icons [27], but is both Captcha and a graphical password scheme [14] which is combined into a single entity.

4. PROPOSED WORK

In this paper, we have added an extra authentication method to distinguish bots and humans as well as to avoid super computers to hack by using images (captcha) as one of the password. This is an extension made to general registration process in order to provide security. Image authentication discuss under graphical passwords, it has been taken into consider that captcha in an image format and made it as one of authentication.

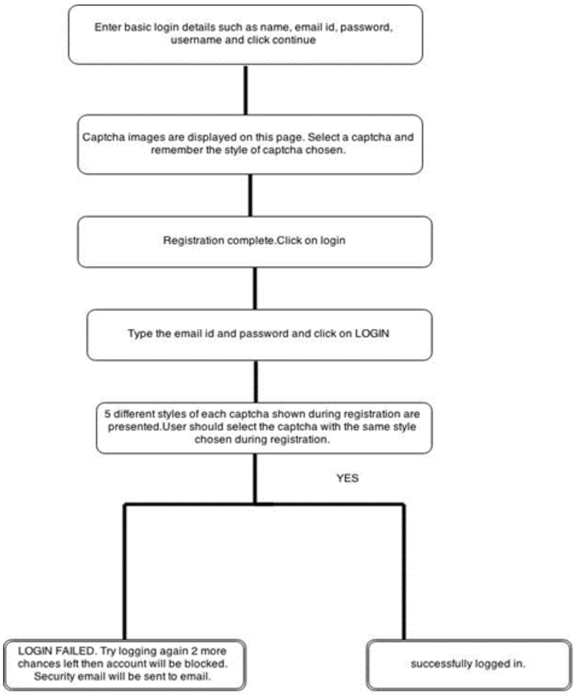

Enter basic login details such as name, email id, password, username and click continue
Captcha images are displayed on this page. Select a captcha and remember the style of captcha chosen.
Registration complete.Click on login
Type the email id and password and click on LOGIN
5 different styles of each captcha shown during registration are presented.User should select the captcha with the same style chosen during registration.
YES
LOGIN FAILED. Try logging again 2 more chances left then account will be blocked. Security email will be sent to email.
successfully logged in.

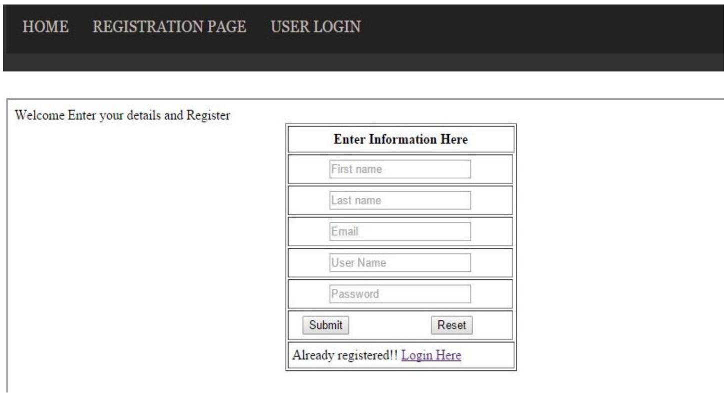
Figure 1. Flow chart of Proposal

In this project we have used Net beans for development purpose, jsp’s for validation of information entered in the page, frontend using HTML and backend using JSP. In login page it contains of one Alpha-numeric password and then he/she has to select one of the images (captcha) as second password which he/she selects at the registration time. In registration page along with normal Alpha-numeric password, user has to select an image (captcha) as second password and he/she has to remember the words and also its style so that he can login very securely without fear of hacking. When user wants to login he/she enters is Alpha-numeric password and also he/she has to select his image which was selected at the time of registration from decoy of images [37] and also of different font styles of same word, exact image has to select from it and he/she can login successfully, if not he/she receives an error. For more security reasons number of trails will be limited and after it account will be locked.

5. RESULTS AND ANALYSIS

5.1. Registration Page

In this page general details like his name, email required for further assistance, user name which is used during login time and password of alpha-numeric and then submit details to the server then it redirect to captcha selection page in which captcha has to select from decoy of images, but in this we mentioned only few for easy appearance.



Welcome Enter your details and Register

Enter Information Here

First name

Last name

Email

User Name

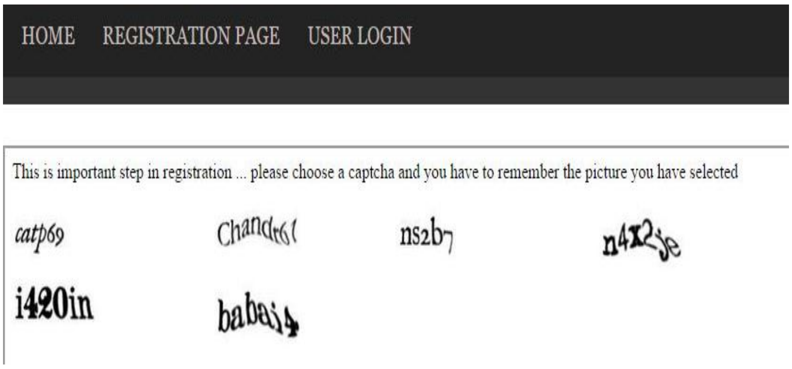
Password

Already registered!! Login Here

Figure 2. Registration Page

5.2. Captcha Selection at Registration Time

In this page user need to select his captcha for future access to account and he/she has to remember it exactly along with its style too. After selection user successfully completes his registration and he/she can login by their credentials. To the convenient for view we have developed only basic captcha’s and less in number, in general it has many images and different in styles too. Data bases have link to the images path for accessing them at right times. These can get stored with a specific id for verification when user has selected it. In more secure conditions we can use images with colours and same font as others and can make more captcha’s.

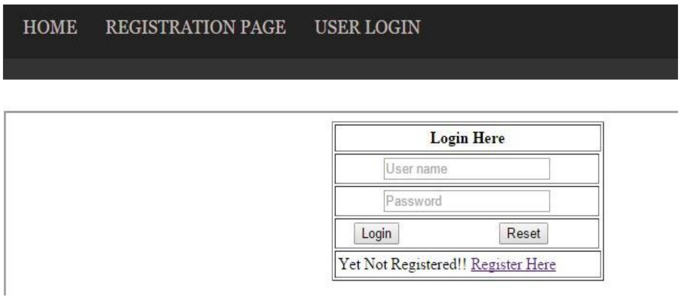


This is important step in registration ... please choose a captcha and you have to remember the picture you have selected

Figure 3. Captcha Selection at Registration

5.3. Login Page

User can login into his/her account by entering the user credentials and press login button and it redirects to the page in with captcha's of different font styles and words were exists.

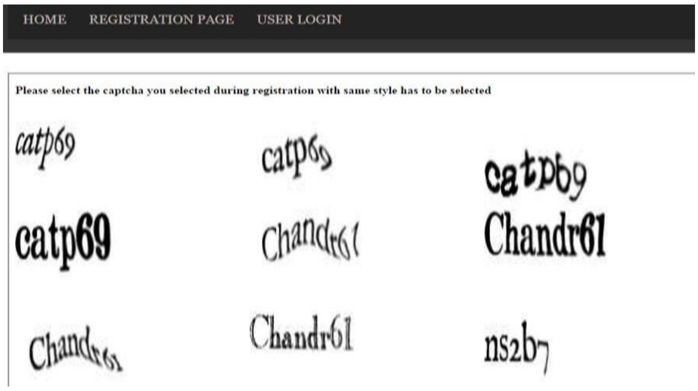


Yet Not Registered!! Register Here

Figure 4. Login Page

5.4. Captcha Selection and Verification at Login Time

In this page he/she has to select the captcha which user has opted at the time of registration and has to select it then it can login successfully, if he fails to select exactly it will redirect to failure page and displays error message.

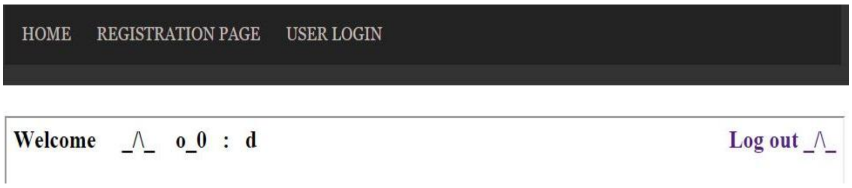


Please select the captcha you selected during registration with same style has to be selected

Figure 5. Captcha Selection at Login

5.5. After Successful Login

If user selected captcha matches to his account 'welcome' page appears if not error occurs and he/she can logout by the link which has displayed at the right top of the page.

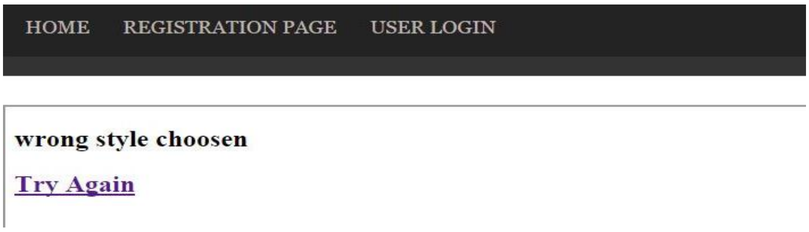


Welcome _/_ o_0 : d

Figure 6. Successful Login

5.6. Wrong Captcha Selected

As user selected captcha doesn't matches to his account or selects wrong captcha this page gets display. If an unauthorized try to use it after 3-4 trails account will gets locked and user can send request to the admin and gets permission and admin will unlocks account after verification.



wrong style choosen

Try Again

Figure 7. Wrong Captcha Selected

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [2], [5]. The discussion can be made in several sub-chapters.

6. CONCLUSION

CAPTCHA can prevent the bots attacks on accounts and provide security and users can remember images long lasting and this helps users. So this helps in many ways for security, interface of frontend should be more friendly and attractive and more storage capacity of databases for images. By this project Captcha as Graphical is implanted in our project.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys. 2012: 44(4).

[2] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Comput*. January/February 2012: 9(1): 128–141.

[3] S. Kim, X. Cao, H. Zhang, and D. Tan, *"Enabling concurrent dual views on common LCD screens,"* in Proc. ACM Annu. Conf. Human Factors Comput. System. 2012: 2175–2184.

[4] J. Bonneau, "*The science of guessing: Analyzing an anonymized corpus of 70 million passwords*," in Proc. IEEE Symp. Security Privacy. Jun 2012: 20–25.

[5] Chiasson, S., Stobert, E., Forget, A., Biddle, R., van Oorschot, P.C.: "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism". *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2012.

[6] "Android", http://beust.com/weblog/archives/ 000497.html, site accessed in Dec, 2012

[7] "Signing in with a picture password", in Building Windows 8 in the MSDN Blogs, http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-witha-picture-password.aspx, last accessed in Oct 2012.

[8] "Passlogix", http://www.passlogix.com, last accessed in Oct 2012.

[9] "Brute force attack", http://en.wikipedia.org/wiki/Brute_force_attack, last accessed in Oct 2012.

[10] "Dictionary attack", http://en.wikipedia.org/wiki/Dictionary_attack, last accessed in Oct 2012.

[11] "Phishing", http://en.wikipedia.org/wiki/Phishing, last accessed in Oct 2012.

[12] "Pharming", http://en.wikipedia.org/wiki/Pharming, last accessed in Oct 2012.

[13] "Spyware", http://en.wikipedia.org/wiki/spyware, last accessed in Oct 2012.

[14] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., *"A Novel Cued-recall Graphical Password Scheme",* In sixth International Conference on Image and Graphics (ICIG). 2011: 949-956.

[15] X. Liu, H. GAO, L. Wang and X. Chang, "An Enhanced Drawing Reproduction Graphical Password Strategy". Journal of Computer Science and Technology. 2011: 26(6): 988-999.

[16] Eluard, M.; Maetz, Y.; Alessio, D.; "*Action-based graphical password: Click-a-Secret*", 2011 IEEE International Conference on Consumer Electronics. 2011: 265-266.

[17] H.C.Gao, L.C.Ma, J.H.Qiu and X.Y.Liu, "*Exploration of a Hand-based Graphical Password Scheme*", Proceedings of the 4th international conference on Security of information and networks. 2011.

[18] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

[19] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "*A new CAPTCHA interface design for mobile devices*," in Proc. 12th Austral. User Inter. Conference. 2011: 3–8.

[20] H.C. Gao., Z.J. Ren., X.L. Chang., X.Y. Liu., etc., "*A New Graphical Password Scheme Resistant to Shoulder-Surfing*", International Conference on Cyberworlds (CW). December 2010: 194-199.

[21] P. C. van Oorschot, A. Salehi-Abari and J. Thorpe. "Purely Automated Attacks on PassPoints-Style Graphical Passwords". *IEEE Transactions on Information Forensics and Security*. 2010: 5(3): 393-405.

[22] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text", Journal of Computers. 2010: 5(5).

[23] B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs," in Proc. ACM CCS. 2010: 187–200.

[24] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, “Breaking e-banking CAPTCHAs,” in Proc. ACSAC, 2010: 1–10.

[25] AH Lashkari, et al., “Shoulder Surfing attack in graphical password authentication”, International Journal of Computer Science and Information Security (IJCSIS). 2009: 6(2).

[26] H.C. GAO, X.Y. Liu, R.Y. Dai, etc., “*Analysis and Evaluation of the ColorLogin Graphical Password Scheme*”. The 5th International Conference on Image and Graphics, September 2009: 20-23.

[27] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, “*Towards usable solutions to graphical password hotspot problem*”, In 33rd Annual IEEE International Computer Software and Applications Conference. 2009.

[28] H.C.Gao, X.Y.Liu, S.D.Wang, R.Y.Dai. “*A new graphical password scheme against spyware by using CAPTCHA*”. In: Proceedings of the symposium on usable privacy and security. July 2009: 15-17.

[29] S. Chiasson, A. Forget, E. Stobert, P. C. van Orschot, and R. Biddle. “Multiple password interference in text and clickbased graphical passwords”. In ACM Computer and Communications Security. 2009.

[30] H. Tao and C. Adams. “Pass-Go: A proposal to improve the usability of graphical passwords”. International Journal of Network Security. 2008: 7(2): 273-292.

[31] P. C. van Oorschot and J. Thorpe. “On predictive models and user-drawn graphical passwords”. ACM Transactions on Information and System Security. 2008: 10(4): 1-33.

[32] L. Y. Por, X. T. Lim, M. T. Su, and F. Kianoush. “The design and implementation of background Pass-Go scheme towards security threats”. WSEAS Transactions on Information Science and Applications. June 2008: 5(6): 943-952.

[33] L. Y. Por and X. T. Lim, “Multi-Grid background Pass-Go”. WSEAS Transactions on Information Science and Applications. 7(5)

[34] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, “*YAGP: Yet another graphical password strategy*”. In Annual Computer Security Applications Conference. 2008: 121-129.

[35] R. Weiss and A. De Luca, “PassShapes - utilizing stroke based authentication to increase password memorability”. In NordiCHI. October 2008: 383-392. ACM.

[36] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. “Influencing users towards better passwords: Persuasive Cued Click-Points”. In Human Computer Interaction (HCI), the British Computer Society. September 2008.

[37] E. Hayashi, N. Christin, R. Dhamija, and A. Perrig., “*Use Your Illusion: Secure authentication usable anywhere*”, In 4th ACM Symposium on Usable Privacy and Security (SOUPS), Pittsburgh. July 2008.

[38] P. Golle, “*Machine learning attacks against the Asirra CAPTCHA*,” in Proc. ACM CCS. 2008: 535–542.

[39] J. Yan and A. S. El Ahmad, “*A low-cost attack on a Microsoft CAPTCHA*,” in Proc. ACM CCS. 2008: 543–554.

[40] K. Renaud. “Evaluating authentication mechanisms”. In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6 2005: 103-128. O’Reilly Media.

[41] A. Adams and M. A. Sasse. “Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures”. Communications of the ACM. 1999: 42: 41-46.

[42] D. Feldmeier and P. Karn. “UNIX Password Security-Ten Years Later”. In Crypto'89, August 1989.

[43] R. Morris and K. Thompson. “Password Security: A Case History”. Communications of the ACM. 1979: 22(11): 594-597.

[44] D. Florencio and C. Herley. “*A large-scale study of WWW password habits*”. In 16th ACM International World Wide Web Conference (WWW). May 2007.

[45] Adams, M. A. Sasse, and P. Lunt. “*Making passwords secure and usable*”. In HCI 97: Proceedings of HCI on People and Computers, London, UK, 1997: 1-19.