ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

MULTI FACTOR GRAPHICAL PASSWORD AUTHENTICATION SYSTEMS USING CUED CLICK POINTS

G.Anitha

Research scholar, Department of Computer Science, Govt. Arts College, Ariyalur, Tamilnadu, India.

Dr.M.Prabakaran

Research Supervisor, Asst. Prof. of Computer Science, Govt. Arts College, Ariyalur, Tamilnadu, India.

ABSTRACT

In the present Lyra2, a password hashing scheme (PHS) based on cryptographic sponges. Lyra2 was designed to be strictly sequential for a given number of cores (i.e., not easily parallelizable beyond that number), providing strong security even against attackers using custom hardware or GPUs. At the same time, it is very simple to implement in software and allows legitimate users to fine tune its memory and processing costs according to the desired level of security against brute force password-guessing. Lyra2 is an improvement of the recently proposed Lyra algorithm, providing an even higher security level against different attack venues and overcoming some limitations of this and other existing schemes.

KEYWORDS: Password hashing, processing time, memory usage, cryptographic sponges

INTRODUCTION

USER authentication is a vital element in modern computer security. Although authentication can rely on biometric mechanisms ("what the user is") or physical devices ("what the user has"), the most widespread strategy is to use secret passwords ("what the user knows"), probably due to its cost effectiveness and efficiency. For better or for worse, their prevalence as one and commonly only factor for user authentication is unlikely to change in the near future.

Code word-base system as a rule take up algorithms famous as key hashing scheme (PHS) or answer origin function (KDF), which make a pseudorandom string of bits as of the code word itself. Typically, the PHS's output is either locally stored in the form of a "token" for future password verifications, or used as the secret key for encrypting and/or authenticating data. either the case, such solution use inside a one-way (e.g., hash) purpose, so that getting better the code word from the PHS's production is computationally infeasible. Nevertheless, given that user-defined passwords are commonly quite short and simple strings, this protection may still be bypassed by means of "brute-force", i.e., by testing several potential passwords, possibly with the help of dictionaries.

A Traditional authentication systems use text passwords which includes username and password. This password fails to provide the desired level of security. Text passwords, once chosen and learned, the user must able to recall it at the time of login, which makes them hard to remember. However if we keep changing our password frequently it is more vulnerable to be forgotten. To reduce brute force attacks the user should select long passwords which include characters as well as numbers. This makes them all the more difficult to remember.. Also they are prone to dictionary attacks and keyboard sniffers. Thus they are not much reliable and hence for greater security it can use graphical passwords.

The main goal of the recently created Password Hashing Competition (PHC). aim to speak to this want for stronger alternative, our study led to the tender of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Lyra, a means of maneuver of cryptographic sponge for secret word hash. In this article, we propose an improved version of Lyra, called simply Lyra2. Lyra2 conserve the safety, competence and suppleness of Lyra, counting: (1) the aptitude to arrange the preferred quantity of reminiscence, processing time and parallelism to be used by the algorithm; and the capacity of providing a high memory usage with a processing time similar to that obtained with scrypt. In adding, it carry important development when contrast to its ancestor: (1) it allow a senior safety level next to attack venues connecting time-reminiscence tradeoffs; (2) it allows legitimate users to benefit more effectively from the parallelism capabilities of their own platforms; (3) it includes tweaks for increasing the costs involved in the construction of dedicated hardware to attack the algorithm; (4) it balance fight next to side-canal pressure and attack relying on cheaper (and, hence, slower) storage space plans. These properties are part of the reasons why, among 24 submissions to the PHC, Lyra2 has been awarded a "special recognition" and has its usage endorsed by the PHC panel.

RELATED WORKS

In [1] SaikatChakrabarti and MukeshSinghal et al presents Authentication provides a means of reliably identifying an entity. The most common verification technique is to check whether the claimant possesses information or characteristics that a genuine entity should possess. For example, we can authenticate a phone call by recognizing a person's voice and identify people we know by recognizing their appearance. But the authentication process can get complicated when visual or auditory clues aren't available to help with identification for example, when a print spooler tries to authenticate a printer in excess of the system, or a processor tries to validate a person user classification in. Transmitting a password in plaintext from the user to the server is the simplest (and most insecure) method of password-based authentication. To validate a user password, the server compares it with a password (either in plaintext or an image of the password under a one-way function) stored in a file. However, this method lets an adversary passively eavesdrop on the communication channel to learn the password. To secure against passive eavesdropping, researchers have developed challenge-response protocols.

In [2] Cormac Herley,1P.C. van Oorschot, Andrew S. Patrick et al presents While a lot has changed in Internet security in the last 10 years, a lot has stayed the same – such as the use of alphanumeric passwords. Passwords remain the dominant means of authentication on the Internet, even in the face of significant problems related to password forgetting and theft. In fact, despite large numbers of proposed alternatives, we must remember more passwords than ever before. Why is this? Will alphanumeric passwords still be ubiquitous in 2019, or will adoption of alternative proposals be commonplace? What must happen in order to move beyond passwords? This note pursues these questions, following a panel discussion at Financial Cryptography and Data Security Passwords have served us well for many years, but they suffer from a number of problems that suggest their reign should be coming to an end. Users often choose weak passwords, making guessing and brute-force dictionary and exhaustive attacks feasible. Users also frequently forget passwords, necessitating expensive customer support calls or automated backup authentication schemes often involving challenge questions, which may be even weaker forms of authentication.

In [3] Large-Scale Study of Web Password Habits et al presents the results of a large scale study of password use and password re-use habits. The study involved half a million users over a three month period. A client component on users' machines recorded a variety of password strength, usage and frequency metrics. This allow us to quantify or estimation such quantity as the standard figure of passwords and standard shape of financial records every user has, how many passwords she type per day, how often passwords are shared among sites, and how often they are forgotten. We get very full statistics on code word power, the type and length of passwords selected, and how they vary by site. The data is the first large scale study of its kind, and yields numerous other insights into the role the passwords play in users' online experience.

In [4] degree of difference and invertibility property of BLAKE et al present BLAKE is a hash purpose chosen

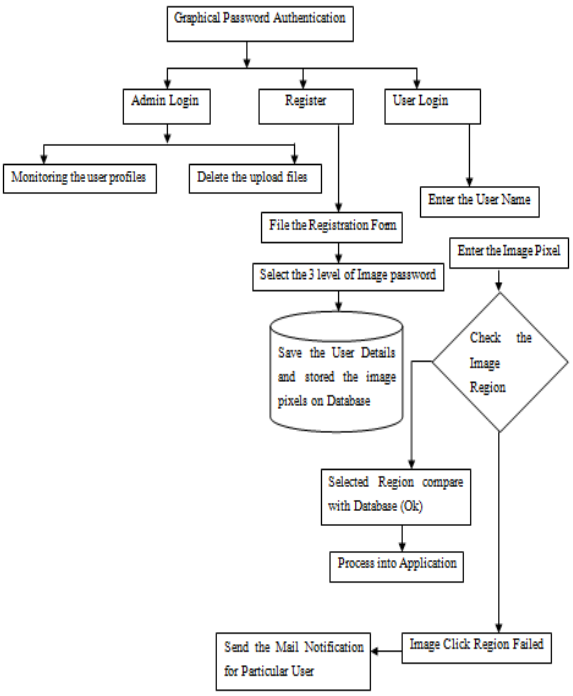
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

by NIST as one of the 14 next around candidate for the SHA-3 rivalry. In this paper, we follow a bottom-up approach to exhibit properties of BLAKE and of its building blocks: based on differential properties of the internal function G, we show so as to a surrounding of BLAKE is a variation on the memo room, and there an competent inversion algorithm. For 1.5 rounds we present an algorithm that finds preimages faster than in previous attacks. Exposed property lead us to explain large lessons of impracticable differential for two rounds of BLAKE's inside incarnation, and particular impossible differentials for five and six rounds, respectively for BLAKE- 32 and BLAKE-64. Then, using a linear and rotation-free model, we describe near-collisions for four rounds of the compression function. lastly, we talk about the difficulty of establish higher limits on the likelihood of discrepancy individuality for BLAKE.

In [5] Comprehensive evaluation of high-speed and medium-speed implementations et al presents A comprehensive comparison of all Round 3 SHA-3 candidates and the current standard SHA-2 from the point of view of hardware performance in modern FPGAs. Every algorithm is implementing using manifold architectures base on the concept of iteration, failure, unrolling, pipelining, and route duplication. Trade-offs flanked by speed and area are investigated, and the best architecture from the point of view of the throughput to area ratio is identified. lastly, all algorithms are rank base on their in general presentation in FPGAs. The trait skin of each algorithm vital from the top of view of its completion in hardware are identified. routine in hardware is one of the main criterion old in the SHA-3 struggle. Typically, this performance is evaluated using two major technologies: Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Contrast by FPGAs offer more than a few significant compensation, such as short development time, precise position place & route results, survival of tools for optimum choice of agenda options and automatic compilation of a large number of consequences, and relatively small number of vendors and device families that dominate the market

ARCHITECTURE



PROPOSED SYSTEM

In the future job we boast included thud name to help in recall the key. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In everyday being we see a variety of example of recall an thing by the noise connected to that thing enter User ID and choose one noise incidence which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To produce full vector consumer have to go for run of imagery and click on both likeness at click point of his pick.

MODULES

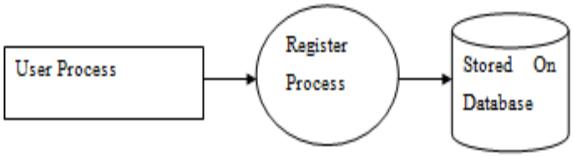
- Create User profile Vector (master):
- Profile Vector:
- Picture Selection Phase
- Verification Process
- Upload/Download Module:
- Mail Notification

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

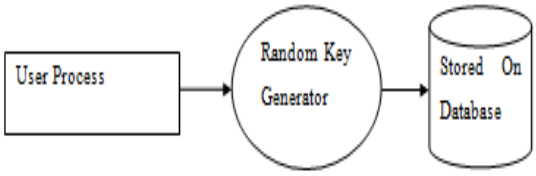
Create User profile Vector (master):

While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector. The Registration mode includes registering the user along with its details. These details comprises of a unique user-id (UID), Precision Value, e-mail address and phone number. The registration process proceeds further by allowing the user to select images, their respective click points. Selection of image can either be done using the handheld devices in-built camera or using the ones that are already present the device. The user can select any click point on the image. Similar to images, selection of sound signature can either be done by choosing one of the already present sounds or by recording one's own voice that helps in recalling the object. Once done the user clicks on the sign up button, thus generating a user profile vector which is stored in the database.



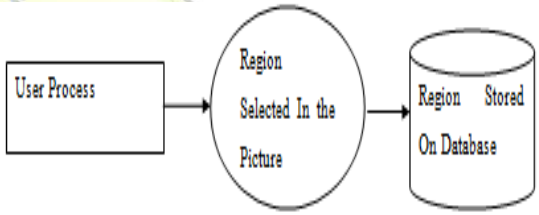
Profile Vector

enter User ID and choose one noise incidence or occasion which he fancy to be play at login time, a forbearance rate is also select with will settle on that the user is valid or an sham. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image and sound signature helps considerably for login.

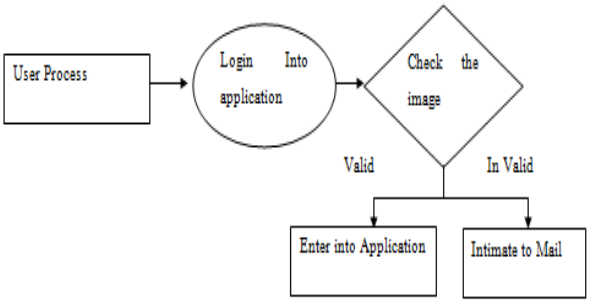


PICTURE SELECTION PHASE

In picture selection phase user select any image as passwords and consist of a sequence of click-points on a given image. Users may select any pixels in the image as click-points for their password. throughout code word formation, the majority of the picture is dim apart from for a small sight port area that is arbitrarily located on the picture. Users must select a click-point within the view port. If they are not capable or loath to opt for a peak in the modern scrutiny port, they may squash the Shuffle button to arbitrarily move the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A consumer who is strong-minded to arrive at a sure click-tip may still scuffle awaiting the sight port moves to the specific site, but this is a time overwhelming and more boring procedure.



VERIFICATION MODULE



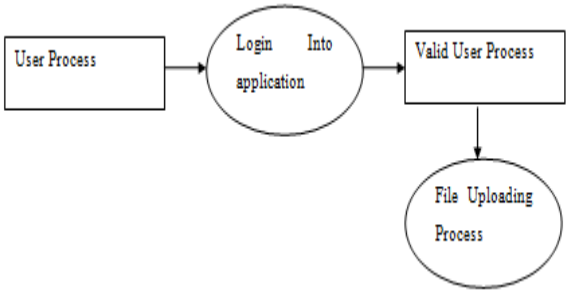
During verification phase, the details that the user enters during registration phase and login phase are verified. This module allows the user to send a secure text from one set of data to the other. Where the user authentication is access with the same id and password. It set of action is to deliver the data from source to destination in a secure manner. Where the text is to be securely delivered to the destination.

UPLOAD/DOWNLOAD MODULE:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

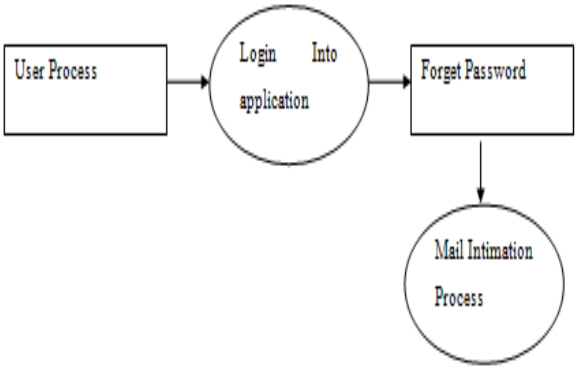
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Admin, defence, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defence, airforce and navy) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use.



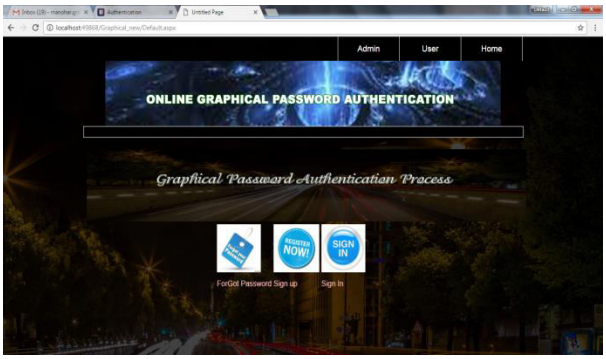
MAIL NOTIFICATION

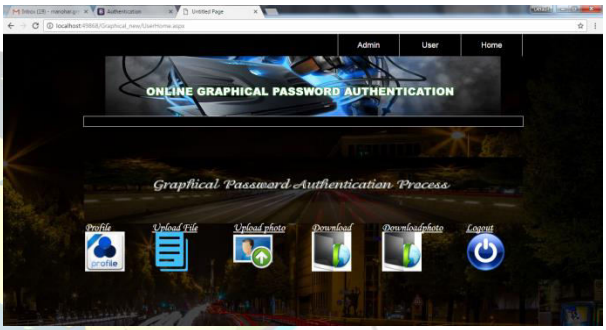
In the parcels input it add to the structure by create a request indiscriminately notify a letter structure that be supposed to in its place be infertile, or detecting modification to outline attributes that have been made for the only purpose of defeating the filtering system. Automatically user will get a mail notification.



OUTPUT RESULT

USER PROCESS





CONCLUSION

Text based authentication schemes face usability and security issues even though they are the most commonly used technique worldwide. Graphical passwords are easier to remember than text based passwords, but even the existing graphical password authentication systems have major drawbacks. In future scheme a new graphical code word scheme that overcome difficulty like hotspot supposition, bear surfing, lexicon attack. The system combines graphical passwords along with a handheld device and sound signature to form a multifactor authentication system. The age group of chance connect points during the online mode prevents the shoulder surfing attack as well as dictionary attacks. Storing the images at the server provides better security as compared to offline mode.

REFERENCE

[1] S. Chakrabarti and M. Singbal, "Password-based authentication: Preventing dictionary attacks," Computer, vol. 40, no. 6, pp. 68–74, 2007.

[2] NIST, SP 800-18 – Recommendation for Key Derivation Using Pseudorandom Functions, National Institute of Standards and Technology, October 2009.

[3] C. Percival, "Stronger key derivation via sequential memory-hard functions," in The Technical BSD Conference, 2009.

[4] B. Kaliski, PKCS#5: Password-Based Cryptography Specification v2.0 (RFC 2898), 2000. [Online]. Available: http://tools.ietf.org/html/rfc2898

[5] C. Herley, P. van Oorschot, and A. Patrick, "Passwords: If we're so smart, why are we still using them?" in Financial Cryptography and Data Security, vol. 5628, 2009, pp. 230–237.

[6] D. Florencio and C. Herley, "A large scale study of web password habits," in Proc. of the 16th Int. Conf. on World Wide Web, 2007, pp. 657–666.

[7] NIST, SP 800-63-2 – Electronic Authentication Guideline, National Institute of Standards and Technology, August 2013.

[8] M. D¨urmuth, T. G¨uneysu, and M. Kasper, "Evaluation of standardized password-based key derivation against parallel processing platforms," in Computer Security – ESORICS 2012, 2012, vol. 7459, pp. 716–733.

[9] M. Marechal, "Advances in password cracking," Journal in Computer Virology, vol. 4, no. 1, pp. 73–81, 2008.

[10] N. Provos and D. Mazi`eres, "A future-adaptable password scheme," in Proc. of the FREENIX track (USENIX'99), 1999.

[11] PHC, "Password hashing competition," https://password-hashing.net/.

[12] L. Almeida, E. Andrade, P. Barreto, and M. Simplicio, "Lyra: Passwordbased key derivation with tunable memory and processing costs," Journal of Cryptographic Engineering, vol. 4, no. 2, pp. 75–89, 2014, see also eprint.iacr.org/2014/030.

[13] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Sponge functions," ECRYPT Hash FunctionWorkshop, 2007, http://csrc.nist.gov/pki/ HashWorkshop/Public Comments/2007 May.html.

[14] ——, "Cryptographic sponge functions - version 0.1," http://keccak.noekeon.org/, 2011.

[15] M. Sprengers, "GPU-based password cracking: On the security of password hashing schemes regarding advances in graphics processing units," Master's thesis, Radboud University Nijmegen, 2011.