# AUTHENTICATION METHODS: A CONCEPTUAL REVIEW

Simran Malhotra[1], Dr. Ravinder Tanwer[2]
[1]M. Tech Research Scholar, [2]Professor,
Department of Computer Science & Engineering, Ratan Institute of Technology and Management, Palwal, Haryana

***Abstract: In order to access any of the information or data, we require to authenticate the user so that only the authorized users can access the data. With the development of science and technology there are number of authentication methods and this paper reviews the various types of available authentication schemes and methods***
***Keyword: Graphical Passwords, Grid Passwords, Security, User Authentication***

## I. INTRODUCTION

Authentication is the way toward perceiving a client's character. It is the component of partner an approaching solicitation with a lot of recognizing accreditations. The accreditations gave are contrasted with those on a document in a database of the approved client's data on a nearby working framework or inside an authentication server. The authentication process consistently runs toward the beginning of the application, before the consent and choking checks happen, and before some other code is permitted to continue. Various frameworks may require various sorts of certifications to learn a client's personality. The qualification frequently appears as a password, which is a mystery and known uniquely to the individual and the framework. Three classes in which somebody might be validated are: something the client knows, something the client is, and something the client has. [1]

Authentication procedure can be portrayed in two unmistakable stages - distinguishing proof and real authentication. ID stage gives a client personality to the security framework. This personality is given as a client ID. The security framework will look through all the theoretical items that it knows and locate the particular one of which the real client is right now applying. When this is done, the client has been recognized. The way that the client claims doesn't really imply this is valid. A real client can be planned to other conceptual client object in the framework, and in this way be allowed rights and consents to the client and client must offer proof to demonstrate his personality to the framework. The way toward deciding asserted client personality by checking client gave proof is called authentication and the proof which is given by the client during procedure of authentication is known as a qualification. [1]

## II. PASSWORD TYPES

Current authentication procedures can be parceled into three rule zones:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based procedures, for instance, scratch cards, bank cards and shrewd cards are comprehensively used. Various token-based authentication frameworks in like manner use information-based methodology to improve security. For example, ATM cards are all around used along with a PIN number. [2]

Biometric based authentication frameworks, for instance, fingerprints, iris clear, or facial affirmation, are not yet by and large got. The genuine drawback of this technique is that such frameworks can be expensive, and the unmistakable evidence procedure can be moderate and normally unstable. Regardless, such a framework gives the biggest measure of security.[3]

Information based frameworks are the most for the most part used authentication methodologies and consolidate both substance based and picture-based passwords. The picture-based frameworks can be furthermore parceled into two classes: affirmation - based and audit based graphical systems. Using affirmation-based frameworks, a customer is given a course of action of pictures and the customer passes the authentication by seeing and perceiving the photos the individual in question picked in the midst of the enlistment arrange. Using survey based frameworks, a customer is mentioned to reproduce something that the individual in question made or picked before in the midst of the enrollment stage.[3].

## III. TEXTUAL PASSWORDS

Text passwords are settled, most generally utilized today, in spite of numerous choices proposed to supplant text passwords to date. Text password research has three many years of history and an ongoing exploration shows new worldview in usable text passwords scrutinizing the previous history. [4] We give a far reaching outline of distributed examination in text password plans in two time, covering convenience, security and deployability viewpoints, just as framework assessment dependent on ease of use, deployability and security benefits that a perfect plan may give. The paper first indexes existing web authentication conspire approaches, featuring novel highlights of chosen plots and distinguishing key convenience, deployability or security benefits. We at that point assess the convenience, security and deployability necessities fulfilled by the plans in the two times, distinguish security dangers that such frameworks must address, examine ease of use issues and survey known assaults. At last we examine the change between the two times and the future exploration bearing and necessity of the text password schemes. Since practically all PC frameworks store passwords in some scrambled structure,

  

think about the password as a key to a cryptographic framework. Cryptographic frameworks give greater security as the key size develops, recommending that passwords are increasingly secure as they develop longer. There is a trace of validity in this perception. In any case, a more extended password isn't as solid when contrasted with a shorter password as one would might suspect. This is because of the impediments forced by some PC frameworks and the manner by which individuals pick their passwords. [4].

## IV. GRAPHICAL PASSWORDS

A graphical password is an authentication framework that works by having the client select from pictures, in a particular request, introduced in a graphical UI (GUI). Consequently, the graphical-password approach is at times called graphical client authentication (GUA). A graphical password is simpler than a text-based password for the vast majority to recall. Assume a 8-character password is important to pick up passage into a specific PC arrange. Rather than w8KiJ72c, for instance, a client may choose pictures of the earth (from among a screen brimming with genuine and imaginary planets), the nation of France (from a guide of the world), the city of Nice (from a guide of France), a white plaster house with angled entryways and red tiles on the rooftop, a green plastic cooler with a white top, a bundle of Gouda cheddar, a container of grape juice, and a pink paper cup with minimal green stars around its upper edge and three red groups around the center.

Graphical passwords may offer preferred security over text-based passwords in light of the fact that numerous individuals, trying to retain text-based passwords, utilize plain words (as opposed to the suggested mix of characters). A word reference search can frequently hit on a password and permit a programmer to pick up section into a framework in a flash. Yet, on the off chance that a progression of selectable pictures is utilized on progressive screen pages, and if there are numerous pictures on each page, a programmer must attempt each conceivable mix indiscriminately. On the off chance that there are 100 pictures on every one of the 8 pages in a 8-picture password, there are 1008, or 10 quadrillion (10,000,000,000,000,000), potential mixes that could frame the graphical password! (By and large) a huge number of years to break into the framework by hitting it with arbitrary picture groupings. [5]

While passwords are a frail type of insurance, their effortlessness makes them simple to utilize and direct. In the event that clients are persuaded of their value, proper training gave, and a little consideration taken, passwords can give sufficient assurance.

### 4.1 Advantages of Graphical Passwords

Next to no examination has been done to consider the difficulty of breaking graphical passwords. Since graphical passwords are not commonly used for all intents and purposes, there is no give a record of certifiable examples of breaking graphical passwords. Here we rapidly test a part of the possible procedures for breaking graphical passwords and try to finish a connection with text-based passwords.

Savage power search

The essential protect against savage power search is to have a sufficiently broad password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the quantity of Printable characters excepting SPACE. Some graphical password methods have been seemed to give a password space like or greater than that of text-based passwords. Affirmation based graphical passwords tend to have tinier password spaces than the audit based strategies. [5]

It is all the more difficult to finish a beast power ambush against graphical passwords than text-based passwords. The attack programs need to therefore make definite mouse development to imitate human information, or, as such for audit based graphical passwords. By and large, we confide in a graphical password is less frail against animal power ambushes than a text-based password. [6]

Vocabulary attacks

Since affirmation based graphical passwords incorporate mouse commitment as opposed to support input, it will be unfeasible to finish word reference ambushes against such a graphical passwords. For some audit based graphical passwords it is possible to use a word reference ambush yet an automated vocabulary attack will be significantly more erratic than a text based dictionary attack. More exploration is required around there. All things considered, we acknowledge graphical passwords are less feeble against word reference ambushes than text-based passwords. [6]

Speculating

Unfortunately, apparently graphical passwords are much of the time obvious, a significant issue typically associated with text-based passwords. For example, considers on the Passface procedure have shown that people consistently pick weak and obvious graphical passwords. Nali and Thorpe's examination revealed similar consistency among the graphical passwords made with the DAS procedure . More exploration attempts are relied upon to understand the possibility of graphical passwords made by authentic customers.

Shoulder surfing

Like text-based passwords, the greater part of the graphical passwords are defenseless against shoulder surfing. Now, just a couple of acknowledgment based techniques are intended to oppose shoulder-surfing . None of the review-based techniques are considered should-surfing safe.[7]

## V. GRAPHICAL PASSWORD TYPES

Graphical Password Authentication has three significant classifications dependent on the movement they use for authentication of the password:

- Acknowledgment based Authentication: A client is given a lot of pictures and he needs to recognize the picture he chose during enrollment. For instance, Passfaces is a graphical password plot dependent on

  

perceiving human countenances. During password creation, clients are given a huge arrangement of pictures to choose from. To sign in, clients need to recognize the pre-chosen picture from the few pictures introduced to him.

- Review based Authentication: A client is approached to replicate something that he made or chose at the enlistment stage. For instance, in the Passpoint plot, a client can click any point in a picture to make the password and a resistance around every pixel is determined. During authentication, the client needs to choose the focuses inside the resistance in the right arrangement to login.
- Prompted Recall: Cued Click Points (CCP) is an option in contrast to the PassPoints procedure. In CCP, clients click one point on each picture instead of on five focuses on one picture (not at all like PassPoints). It offers signaled review and quickly alarms the clients on the off chance that they commit an error while entering their most recent snap point.
- The current graphical password techniques can be ordered into two classes: acknowledgment based and review based techniques. [7]

## VI. CONCLUSION

Thus , the various methods are discussed in paper and the graphical methods are more impressive as they are easy to understands and more appeal for user to remember the sequence require for the authentication process.

## REFERENCES

[1] Gary Pan, Seow Poh Sun, Calvin Chan and Lim Chu Yeong,"Analytics and Cybersecurity: The shape of things to come",CPA ,2015
[2] Erol Gelenbe and Omer H. Abdelrahman,"Search in the Universe of Big Networks and Data",IEEE ,2014
[3] Benedicto B. Balilo Jr., Bobby D. Gerardo, Ruji P. Medina,"A comparative analysis and review of OTP Grid Authentication Scheme: Development of new scheme",International Journal of Scientific and Research Publications, Volume 7, Issue 11, November 2017
[4] Anjali Somwanshi,Devika Karmalkar,Sachi Agrawal,Poonam Nanaware,Mrs. Geetanjali Sharma, "Dynamic Grid Based Authentication With Improved Security ",International Journal of Advances in Scientific Research and Engineering (ijasre) ,Vol. 03, Issue 3, April -2017
[5] S. Pandey, R. Motwani, P. Nayyar and C. Bakhtiani, "Multiple access point grid based password scheme for enhanced online security," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 144-148.
[6] S. Agrawal, A. Z. Ansari and M. S. Umar, "Multimedia graphical grid based text password authentication: For advanced users," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), Hyderabad, 2016, pp. 1-5.
[7] M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), Aligarh, 2017, pp. 171-174.
[8] R. Balaji and V. Roopak, "DPASS — Dynamic password authentication and security system using grid analysis," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 250-253.
[9] E. Yoon and K. Yoo, "Improving the Generalized Password-Based Authenticated Key Agreement Protocol," 2008 The 3rd International Conference on Grid and Pervasive Computing - Workshops, Kunming, 2008, pp. 341-346.
[10] J. -. Robinson et al., "Web-enabled grid authentication in a non-Kerberos environment," The 6th IEEE/ACM International Workshop on Grid Computing, 2005., Seattle, WA, USA, 2005, pp. 5 pp.-.

  