Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

CybIQ: Special secure Authentication method

Raghavendra Devidas[1], Hrushikesh Srinivasachar[2]

[1]ITT/QIM, Mercedes Benz Research & Development India Pvt ltd, Bengaluru-560066, India, Telephone No: +91 9538676171, Email: Raghavendra.devidas@daimler.com

[2]ITP/IE, Mercedes Benz Research & Development India Pvt ltd, Bengaluru-560066, India, Telephone No: +91 9886722802, Email: Hrushikesh.srinivasachar@daimler.com

Abstract: With increased vulnerabilities and vast technology landscapes, it is extremely critical to build systems which are highly resistant to cyber-attacks, to break into systems to exploit. It is almost impossible to build 100% secure authentication & authorization mechanisms merely through standard password / PIN (With all combinations of special characters, numbers & upper/lower case alphabets and by using any of the Graphical password mechanisms). The immense computing capacity and several hacking methods used, make almost every authentication method susceptible to cyber-attacks in one or the other way. Only proven / known system which is not vulnerable in spite of highly sophisticated computing power is, human brain.

In this paper, we present a new method of authentication using a combination of computer's computing ability in combination with human intelligence. In fact this human intelligence is personalized making the overall security method more secure.

Text based passwords are easy to be cracked [6]. There is an increased need for an alternate and more complex authentication and authorization methods. Some of the Methods [7] [8] in the

© 2021 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

category of Graphical passwords could be susceptible, when Shoulder surfing/cameras/spy devices are used.

Keywords: Pattern based access, Graphical password, safe password, non-intuitive password, non-static password, visually encrypted password.

1. Introduction

CybIQ, a unique special method for ensuring secure authentication in various systems which are vulnerable to cyber-attacks. CybIQ stands for the new secure method, created using a combination of computing capabilities and human intelligence. i.e

1. Conventional PIN/Password
2. The mapping of the numbers with objects
3. Random order of rendering by the algorithm
4. The computation / logic to arrive at the original password, by calculating the equation/simple math in brain.

Existing authentication methods have certain known vulnerabilities and care needs to be taken to ensure that the credentials are safe and not compromised. And the existing methods have both logical & physical credentials. For instance remembering a PIN or a password belongs to the logical category. And the thumb impression and ID card with a chip for instance is an example of physical identification method.

Now let's quickly go through the common vulnerabilities in everyday life, costing millions & billions of worth effort, money & reputation loss to individuals & organizations alike.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

- An ATM User might be secretively watched and his/her PIN might be captured through a Spy camera.
- User Accessing the personal/office bank account through a compromised/virus infected network/infrastructure might unknowingly lose id/password to intruders.
- A PC without up to date antivirus updates, might be easily hacked and the key credentials get exposed.
- Entering your debit/credit card pin on POS machine in public place or in a shopping mall is an easy target for stalkers.
- Malwares installed in smart devices can secretly read and apply the OTPs and perform unauthorized transactions.
- The credentials once exposed could be used for an illegitimate purpose.
- Covertly installed Keystroke loggers can capture key strokes and mimic the key entries as if the original authorized user is using the credentials.

Bio metric access mechanisms help solve some of the threats posed by hacker. However they are not completely safe. The problem areas with each one of the mechanisms are highlighted below.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Categories of Access control:

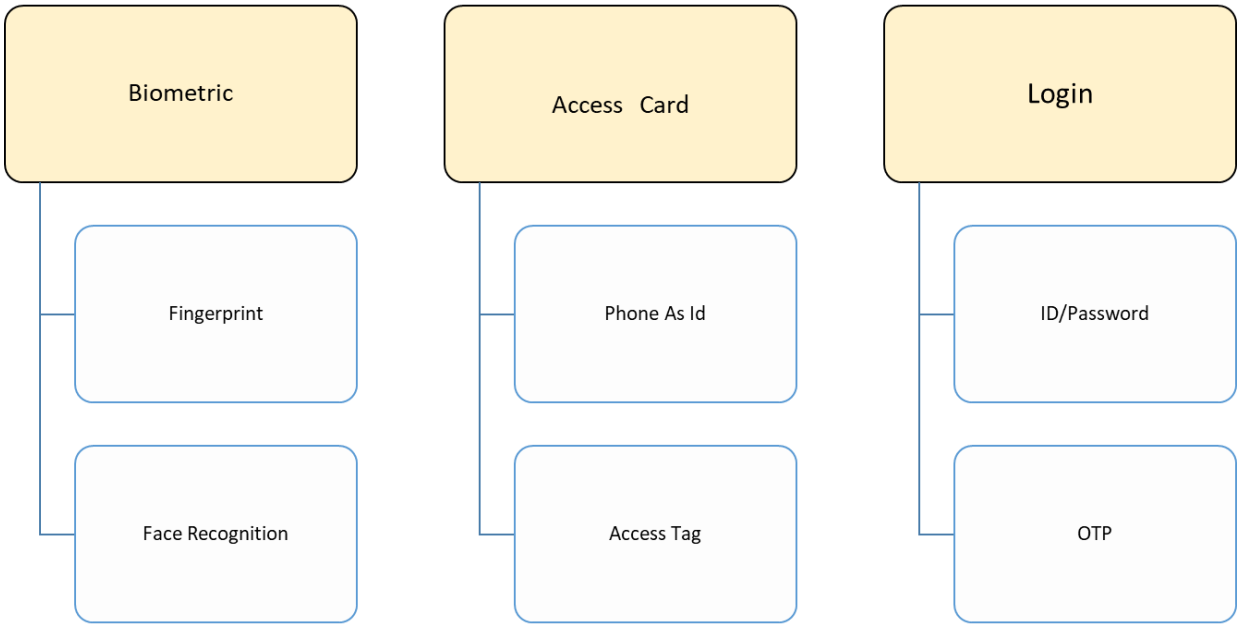

Fig 1. Categories of Access control systems.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Issues with existing access control methods

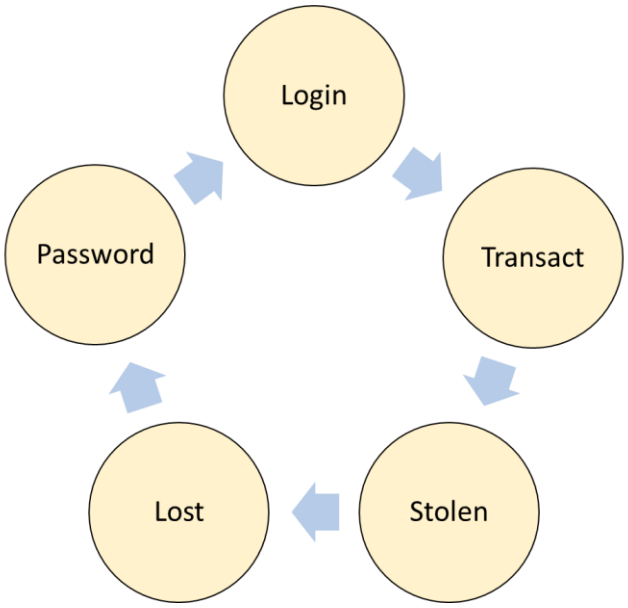

Fig 2. Issues with conventional PIN/Password access control method

Face Recognition:

- How does the system react if an image or a video with appropriate resolution is placed in front of Face recognition device?
- What is the result of placing a 3D printed face, Wax Face or even a photograph with appropriate resolution in front of the Face recognition device?

OTP:

- What if there is no internet access Or Mobile network access at a given place?
- What if the malware is secretly reading and transferring the OTP to the intruder?

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Access Card:

There is no control on who can carry the access card. Hence easily targeted by intruders.

Key Stroke pattern:

With Key loggers this can be broken.

The cyberattacks are everywhere, for instance in the operations of Ports in the shipping industry. There are several types of cyberattacks. Such as propagation of ransomware, manipulation of port communication system and Unauthorized UAV activity.

Though the solution rendered in this paper doesn't cover all aspects of Cyber-attacks. It does provide a reliable solution to the access control related vulnerabilities. It is important to protect critical resources from hackers. The relevance of such aspects is detailed in Ref [1]. One example is making the access control very strong by using CybIQ, which uses conventional key/PIN/password and special memorized password pattern.

Protection measures against hacking passwords:

There are several methods [10] which assist in providing protection against hacking of Passwords. As we have seen that the single factor authentication will be a risk and has some probability of identity theft. We have these days several authentication mechanisms to strengthen the authentication process, such as multi factor authentication. As there are new methods, there are corresponding sophistications for hacking these methods too. Some of the methods are very intuitive [9]. However have their own strengths & weaknesses with reference to usage in real world. Hence the search for the most secure authentication method continues. We have presented one such method in this paper.

The detailed study on vulnerabilities of several passwords and directions for building secure passwords in future [11] was very useful for us in identifying new authentication methods.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Historically there have been many alternate methods including graphical passwords [13].

Existing concepts in the area of graphical password [16], [17], [18], [19] & [21] on designs & solutions for shoulder surfing on graphical authentication methods inspired us for further research.

Some of the scenarios in which the Secret PIN/Password could get exposed:

Fig 3. An ATM user watched while entering PIN

Fig 4. Person trying to notice the Mobile phone user unlocking the screen

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Fig 5. User entering PIN into POS machine is stalked

Fig 6. Illustration of unauthorized user getting access to personal accounts with normal password.

Fig 7. Malware controlling the infected device and asking for ransom

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

2. Method

Each day we hear about multiple breaching incidents with respect to data security. There are limitations mentioned above in the existing access mechanisms. Financial institutions and individuals are losing money and assets causing huge damage/loss of reputation. Biometric Access control mechanisms do not prove to be 100% secure. In the current era of AI and Machine learning any new access control mechanism faces unimaginable challenges. Hence there is need for a complete new access mechanism which is beyond the current conventional methods employed. (i.e. static PIN/Password).

In the class of Graphical passwords which are resistant to shoulder surfing [15], it is still complicated from a usability perspective. Due to iterative login process. We have tried to keep the login process simple as it will be widely used. i.e to enter PIN/password as already familiar. But adding a specific additional feature to co-relate and enter credentials. The main consideration has been to keep the login process as simple as possible. While enhancing the strength of the password.

The method of authentication by gamification uses the Biometric (Keystroke pattern) and the Knowledge based factor [2]. Similarly the method proposed in this paper uses a combination of randomization of patterns / images and a memorized number with a mathematical operation. The pattern combination used for login cannot be used by an eavesdropper unless the same pattern is rendered while the eavesdropper tries to authenticate. The strength of the password increases with more digits / alphabets and with the kind of mathematical operation used.

Well known disadvantages of textual passwords and also about stable & alterable biometric signals are listed in detail in [3]. Image based authentication [4] is a very good alternative for dealing with issues in security challenges of the static PIN/Password based credentials. In this paper, our focus is on ensuring safety of the credentials than on the simplicity or usability. From

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

the usability perspective we had some interesting insights when we did the user reviews. For instance couple of users said that they would like to use the CybIQ method for one of their 5 bank accounts, where they have more cash or for their primary account. But for the rest of the banks transactions or for other IT systems they said, they are ok with the existing authentication mechanisms. They said better to bear little bit of inconvenience or overhead than to be sorry. Because cost of lost data/assets causes unbearable discomfort. An insightful detail of pattern based authentication scheme [5] is one of the great examples in the group of graphical passwords. The only disadvantage with such a method is, in case if the hacker manages to watch or record a user login session. It is possible for the hacker to reproduce the credentials based upon the logic captured/recorded. In fact the concept presented in [5] gives an inspiration for the next generation of secure passwords. Our method presented in this paper is immune to direct exposure for hackers. i.e even if a hacker manages to record / capture the login event, he/she cannot reproduce the credentials while login. This is because the process of authentication is a combination of randomized Pin/password and mapping of numbers with graphical content. The combination of computer's order of mapped objects and the association of these with personalized preferences is out of the reach for any hacker. Overall our method gives the basic platform for making the authentication process more robust and unique. In fact it gives the freedom to the user who is using this method to make the login the simplest for himself / herself and the most complex for the 3rd party. There have been some studies and solution proposed around the graphical password [12], which are either too complex or breakable. The detailed survey presented in [14] enables the usability perspectives of various authentication methods. Our research has taken inputs from such studies.

Solution:

The user will be given a conventional PIN/Password as already in practice. In addition to this, the user is given an option to choose a set of objects/pictures/colors or any other entity the user can relate to. Each of the object/entity is mapped with a specific number with a mathematical operation. For simple Use case it can be either addition (+) Or Subtraction (-).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

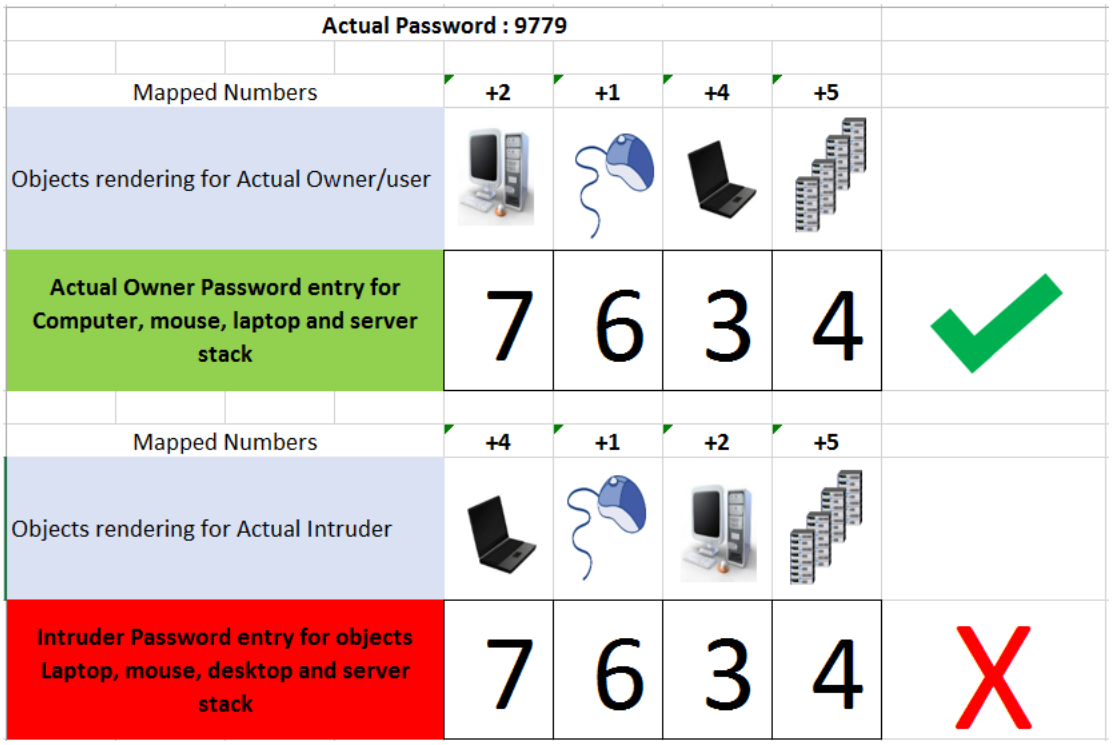

Fig 8. An illustrative example.

For Example:

A user who is given with the bank's debit card will be given with the following combination of mapping objects. The conventional PIN and any one of the mapping set given below

PIN:

5678

Mapping Set:

1) Pictures and their associated Nos:

   Sky: +1

   Tree: +2

   Plant: +3

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Vehicle: -2

2) Pictures and their associated Nos:

   Tiger: +2

   Lion: +3

   Deer: -2

   Wildebeest: -4

3) Pictures and their associated Nos:

   Hummingbird: +2

   Eagle: +4

   Woodpecker: +3

   Penguin: +4

As you have seen above, the set of objects and their associated numbers could be anything of the user's choice. These will not be enforced like a PIN. The user might wish to set the pictures of his/her family member with a number. This will help in easily recalling the associated number with mapped object.

When the user associates the mapping of objects with a group of identifiers such as a category of birds instead of just one bird. It becomes extremely difficult for the hacker to break the code behind i.e. even if the entered PIN/Password is deciphered, the hacker has no idea as to what they stand for.

This password mechanism can be considered as a feasible method, since the user can chose anything of his/her choice as long as he/she can remember and recall the associated number.

The overall workflow is explained in the below diagram:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

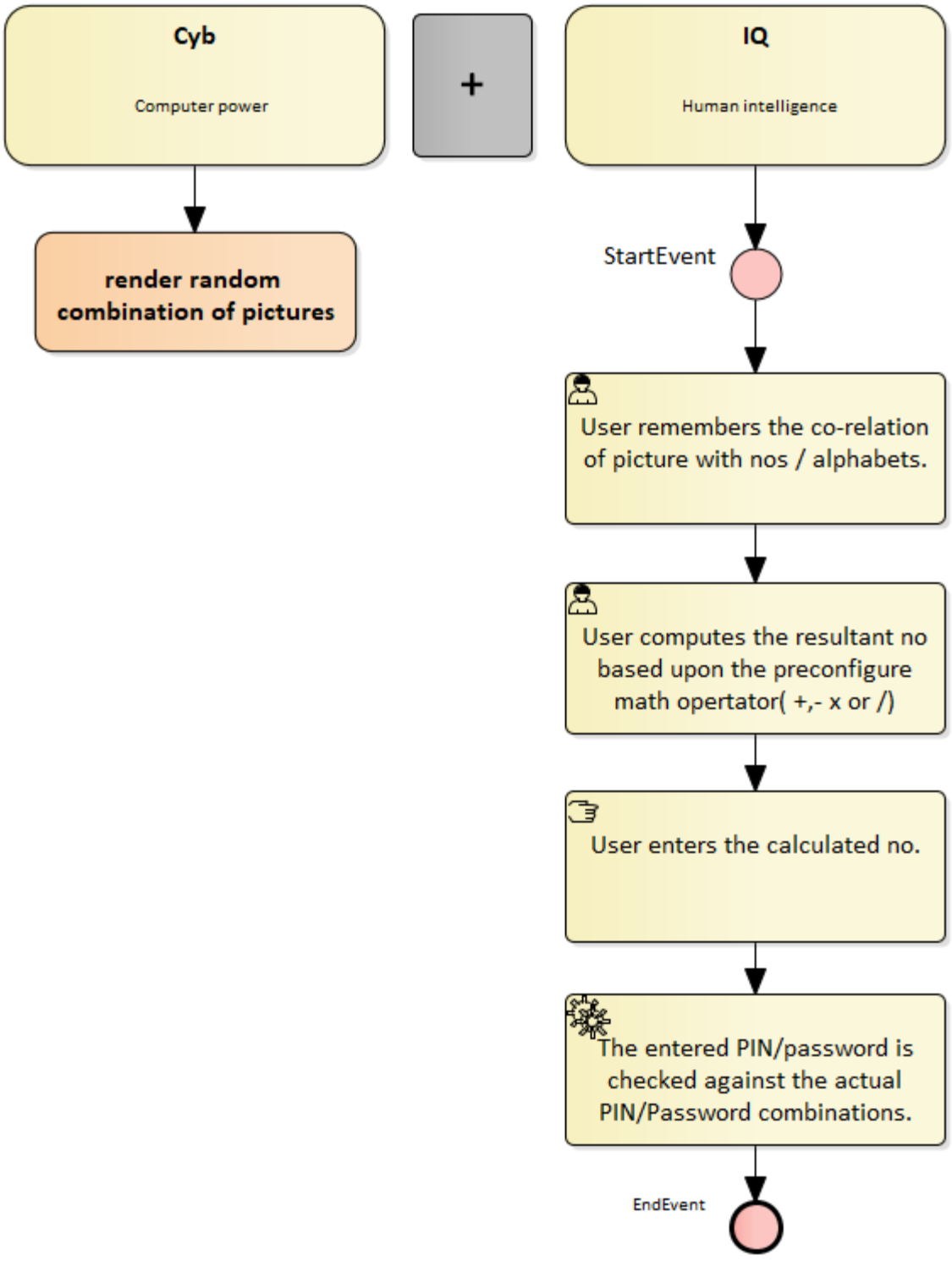

Fig 9. Workflow of PIN/Password entry by the User.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Uniqueness:

After a very detailed analysis, we found that our method can withstand attacks even after the complete user session is copied or recorded. This is mainly because, the proposed method is first of its kind. i.e The password entered by the user once will not be repeated at least for next n attempts. Thereby making it secure. This depends upon the no of positions or digits allowed for the PIN/Password and the extent of mapping along with the mathematical operation chosen.

The beauty of this method is that, it has intrinsic uniqueness while it renders non-repeating password combinations. It also allows each user to leverage this methodology and define another layer of unique combination of password generation. The latter can have an infinite combinations. Empowered by the human imagination and correlation to the real world.

Some of the password combinations that can be chosen are as follows:

a. One user can choose the final PIN to have any digits between 0 & 8. And when the addition is chosen as the math operator and when an object appears corresponding to the no 8. User will enter a number adding which the total exceeds 10. But the last digit is considered for the PIN equivalence.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

b. A user selects the final PIN to not produce a number greater than 10. i.e. the user selects mapping objects mapped to numbers 1 till 4. In fact this is one of the simplest manifestations of CybIQ.

c. A user selects the final PIN and has the mapping of objects However uses the multiplication operator to arrive at the final PIN. i.e

    a. Mapped objects are

        i. Car – 2

        ii. Van – 4

        iii. Bus – 6

        iv. Truck – 8

    b. Actual PIN is **4468**

    c. Mathematical operation is multiplication with only the last digit considered.

    d. The rendered PIN placeholders have the following pattern

        i. Bus Truck Car Van

        For this, the user enters

        ii. 4 3 3 2

Potential use cases:

UCs for Financial Institutions:

UCs for Mobile App Security:

UCs for IT Systems:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Most of the IT systems/tools have a well-defined access control mechanism. And in case of compromise with the Authentication method. Unauthorized users can perform illegitimate tasks and result in loss or incorrect operations.

PIN / Password strength:

The total unique combinations of the password are equivalent to the total permutations **nPr.**

Let's apply this for the 5 digit ATM PIN.

n = 6 (*Considering that the user selects/preconfigures 6 images and associates a number with them*)

r = 5

nPr = 6! / (6 – 5)!

=720 unique combinations of PINs.

i.e. the user can use one of these 720 unique password combinations (Without remembering each of these combinations separately!). While these are huge number of combinations to remember, the user doesn't have to remember all of these by herself. Instead the user needs to remember only the co-relation. Of course on top of the co-relation she has to apply simple math operation to arrive at the actual PIN. We have come across several methods under the graphical password category and have tried to keep the login process as simple as possible, while enhancing the strength of the PIN or Password.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Applying for alphabetic password and not just for numbers in a PIN:

While we have mentioned about the digital PIN, mapping objects and a simple math operation. This method is not only applicable for password or PIN with numeric alone. But it is extensible for alphabets as well. The correlation in this case can be one of the following:

1. To enter the character before based upon the picture shown for the field. In fact this was how the initial cypher text method were used.
2. More numeric are used in an alphanumeric password, so that maximum advantage can be taken.
3. Using consonant if one picture is shown, otherwise using a Vowel.
    a. For example if the password is ‘secureMe12#’ and if one picture is shown then the consonants in the above string will be entered as they are. However when the other configured picture is shown the consonants will be replaced by any vowels. i.e the password in this case will be ‘ieaueeae12#’ and also the password ‘aeauaeae12#’ is also valid. As this satisfies the defined or preconfigured rule.

3. Results

This method doesn’t just give a specific rule. Instead it acts as a specification to derive more user specific rules for strengthening PIN/Password. i.e each individual can use the CybIQ

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

specification and add her own personalized rules, as mentioned with several examples in the Methods section.

User Survey:

We conducted the user surveys for this method and had astonishing feedbacks. Though many said there are challenges in remembering and recollecting the mapped pictures / objects, others said they would like to use this kind of special access method for their primary bank accounts. They felt it's worth spending more effort to safeguard their assets than losing out to eavesdroppers. i.e they told, they wouldn't mind to have an elaborated set of mapped objects/pictures/categories for the alphabets & numbers in their PIN/Password.

Unique advantages:

The PIN /Password cannot be reproduced by the hacker, as the actual rendering of the PIN/Password is a result of random / jumbled order of pictures in the credential text/digit placeholders.

The strength of the Password depends upon the associated / mapped pictures for numbers & characters and the mathematical operation chosen. In fact another key aspect of password strength is the personalized set of pictures the user has selected.

A Survey conducted with a sample set users from various experience and backgrounds, users were asked the following questions

1. Do you think this method is Unique?
2. How Secure the method you think is?
3. How easy is the method for use?

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

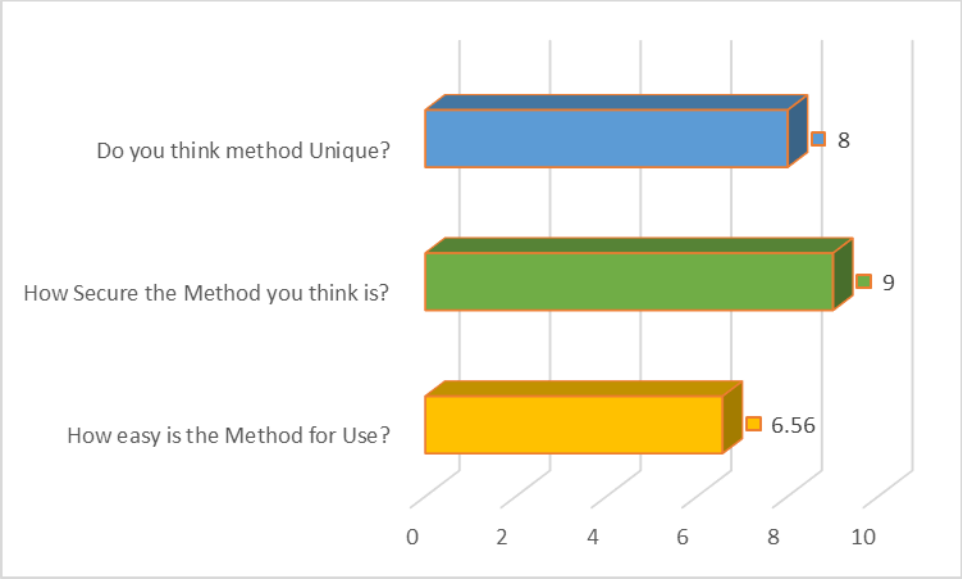

Fig 10. User Survey results.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Another question asked to the user is

4. Would you like to use such a method if given an option?

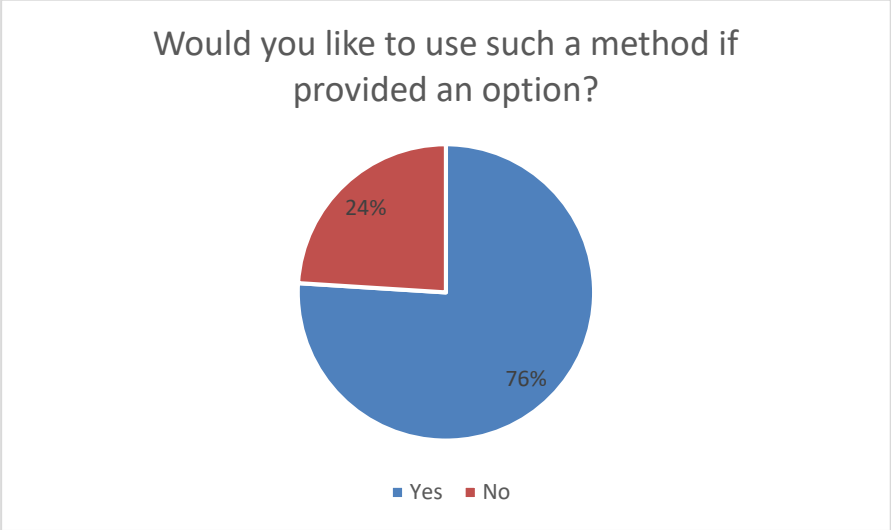

Fig 11. User acceptability.

Acknowledgements:

Jinny Bhinde: For providing pictures & drawings to visualize the concept.

Jalma Yasmin: For giving useful inputs and providing some of the drawings for this idea. And being part of some discussions for the validation of the concept.

Bharath Janardhana & Lakshmi Shenoy: For providing supplementary data for presentation of this concept at different platforms.

4. References

1. Adams, N., Chisnall, R., Pickering, C. et al. Guidance for ports: security and safety against physical, cyber and hybrid threats. J Transp Secur (2021). https://doi.cir-mcs.e.corpintra.net/10.1007/s12198-021-00234-6,
2. Ebbers F., Brune P. (2016) The Authentication Game - Secure User Authentication by Gamification?. In: Nurcan S., Soffer P., Bajec M., Eder J. (eds) Advanced Information

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

Systems Engineering. CAiSE 2016. Lecture Notes in Computer Science, vol 9694. Springer, Cham. https://doi.cir-mcs.e.corpintra.net/10.1007/978-3-319-39696-5_7

3. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," in Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, Dec. 2003, doi: 10.1109/JPROC.2003.819611.
4. Blonder, G.E.: Graphical password (1996). http://www.google.com/patents/US5559961, "Image based authentication"
5. Kumar T.R., Raghavan S.V. (2008) PassPattern System (PPS): A Pattern-Based User Authentication Scheme. In: Das A., Pung H.K., Lee F.B.S., Wong L.W.C. (eds) NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. NETWORKING 2008. Lecture Notes in Computer Science, vol 4982. Springer, Berlin, Heidelberg. https://doi.cir-mcs.e.corpintra.net/10.1007/978-3-540-79549-0_14
6. V. D. M. Kayem, "Graphical Passwords -- A Discussion," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 596-600, https://doi.org/10.1109/WAINA.2016.31
7. U. D. Yadav and P. S. Mohod, "Adding persuasive features in graphical password to increase the capacity of KBAM," 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013, pp. 513-517, https://doi.org/10.1109/ICE-CCN.2013.6528553
8. P. Chithra and K. Sathya, "Pristine PixCaptcha as Graphical Password for Secure eBanking Using Gaussian Elimination and Cleaves Algorithm," 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), 2018, pp. 1-6, https://doi.org/10.1109/ICCCSP.2018.8452829
9. M. ArunPrakash and T. R. Gokul, "Network security-overcome password hacking through graphical password authentication," 2011 National Conference on Innovations in Emerging Technology, 2011, pp. 43-48, doi: 10.1109/NCOIET.2011.5738831.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

10. C. S. Kumari and M. D. Rani, "Hacking resistance protocol for securing passwords using personal device," 2013 7th International Conference on Intelligent Systems and Control (ISCO), 2013, pp. 458-463, doi: 10.1109/ISCO.2013.6481198.
11. S. Ji, S. Yang, X. Hu, W. Han, Z. Li and R. Beyah, "Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords," in IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 5, pp. 550-564, 1 Sept.-Oct. 2017, doi: 10.1109/TDSC.2015.2481884.
12. S. Farmand and O. B. Zakaria, "Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)," 2010 2nd IEEE International Conference on Information Management and Engineering, 2010, pp. 644-650, doi: 10.1109/ICIME.2010.5478017.
13. Klein, D V. Foiling the cracker: A survey of, and improvements to, password security. United States: N. p., 1992. Web.
14. M. Eljetlawi and N. Ithnin, "Graphical Password: Prototype Usability Survey," 2008 International Conference on Advanced Computer Theory and Engineering, 2008, pp. 351-355, doi: 10.1109/ICACTE.2008.34.
15. Zhi Li, Qibin Sun, Yong Lian and D. D. Giusto, "An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack," 2005 IEEE International Conference on Multimedia and Expo, 2005, pp. 245-248, doi: 10.1109/ICME.2005.1521406.
16. Wei-Chi Ku and Maw-Jinn Tsaur, "A Remote User Authentication Scheme Using Strong Graphical Passwords," The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l, 2005, pp. 351-357, doi: 10.1109/LCN.2005.16.
17. P. Lin, L. Weng and P. Huang, "Graphical Passwords Using Images with Random Tracks of Geometric Shapes," 2008 Congress on Image and Signal Processing, 2008, pp. 27-31, doi: 10.1109/CISP.2008.603.
18. A. P. Sabzevar and A. Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords," 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, pp. 625-632, doi: 10.1109/SITIS.2008.92.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2021 doi:10.20944/preprints202111.0045.v1

19. Z. Zheng, X. Liu, L. Yin and Z. Liu, "A Stroke-Based Textual Password Authentication Scheme," 2009 First International Workshop on Education Technology and Computer Science, 2009, pp. 90-95, doi: 10.1109/ETCS.2009.544.
20. F. A. Alsulaiman and A. El Saddik, "Three-Dimensional Password for More Secure Authentication," in IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 9, pp. 1929-1938, Sept. 2008, doi: 10.1109/TIM.2008.919905.
21. Wiedenbeck Susan, Jim Waters, Leonardo Sobrado and Jean-Camille Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", Proceedings of Advanced Visual Interfaces, 2006, https://doi.org/10.1145/1133265.1133303