iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IX **Month of publication:** September 2020

DOI: https://doi.org/10.22214/ijraset.2020.31614

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

A Study on Cyber Security for Password Generation

M. P. Vaishnnave[1], T. E. Sankaranarayanan[2], R. Manivannan[3] , K. Ramkumar[4]
[1]*Teaching Fellow, Dept of IT, University College of Engineering, Villupuram*
[2]*Dept of IT, University College of Engineering, Villupuram*
[3]*Dept of CSE, Annamalai University, Annamalai Nagar*
[4]*Dept of IT, University College of Engineering, Villupuram*

Abstract: ***Password-based authentication is the first of defense of most information systems. Password security enhances the security of the whole information system. Therefore, administrators will formulate the various password strategies to help users to improve security for authentication. To determine the password vulnerability and to enhance user privacy, strong password is must. This paper focuses generation of strong password. Also, we enhance the traditional password generation strategy based on Mnemonic Shape, X-Pass is proposed. X-Pass combines the characters generated by our mapping strategy to help users create a safe and strong password. We have designed a 4x4 matrix called X-Matrix that contains all the hex-digits in it. This hex-digits is converted to numerical digits through binary conversion and we lookup UNICODE character based on numerical digit. After, all numerical digits are processed and returned the characters are appended and then pre-processed to remove the non-printable characters and then finally returns the strong password with UNICODE encoding.***
Keywords: Password generation, Mnemonic shape, hex-digits, numerical digits, UNICODE character

I. INTRODUCTION

Authentication is the main role in security systems [5]. It can be often proved through a username and passwords, sometimes combined with other elements called factors. There are many types of authentication some of them are password authentication, token authentication, biometric authentication [6]. In these types we are discuss about the password authentication. Password is a string of characters used to verify the identity of a user during authentication. It uses username and password for authentication [7]. It is designed to known only to the user and allows user to gain access to a devices, applications or websites.

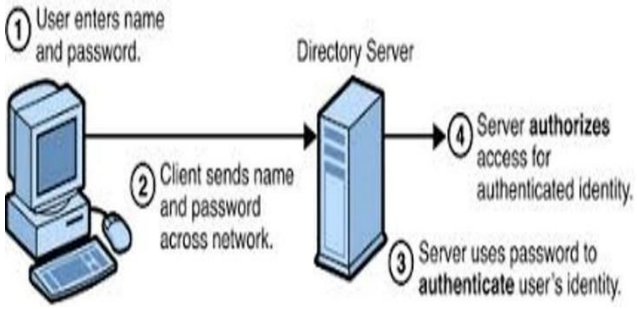


Fig 1: Password Authentication

II. REVIEW OF A PASSWORD STRATEGY FOR STRONG PASSWORD GENERATION

A. Issues in Password Authentication

Even though the password authentication is the one of the best authentication methods it also has some issues. In early, simple passwords are used for authentication which is not secure. Some common issues in the password authentication are as follows:

1) Easy passwords can be cracked easily
2) Random password can't be remembered
3) Issue in remembering multiple passwords

The above issues are some common type of issues in the password authentication. It should be overcome and should have a strong

password. The issues of password are described in fig2.

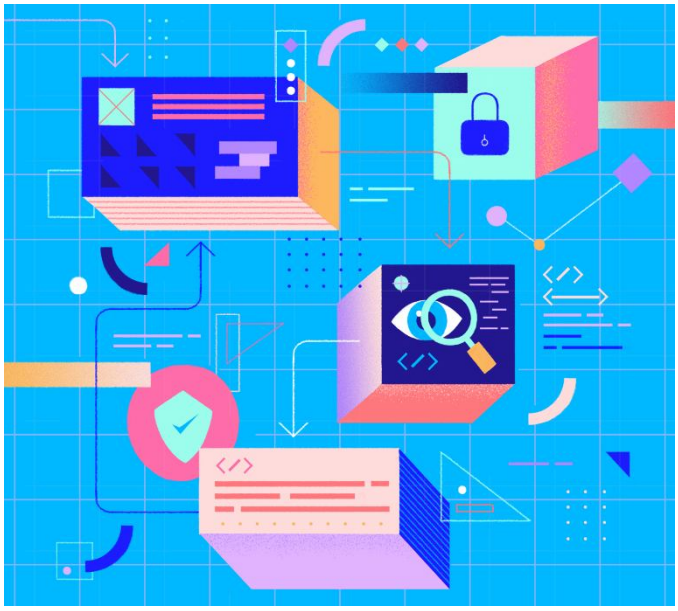


Fig 2: Issues in password authentication

B. Password Attacks

Password authentication is authorizing user and permit the users to access the resources[8]. In some cases, the password can be attacked easily by mediator called Hackers. Hackers hacks the password given by the user to secure their data or information by using some attacks. Some of the attacks which are used to crack or to hack the passwords are as follows:

1) Brute-force attack
2) Dictionary attack
3) Rainbow table attack
4) Phishing attack
5) Shoulder surfing attack
6) Keylogging attack
7) Malware attack
8) Guessing the password

The above attacks are done by hackers to crack passwords of users. The brute-force attack is shown in fig3.

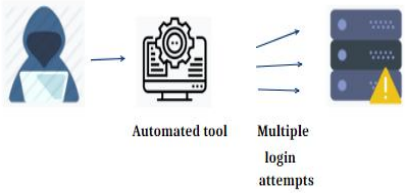


Fig 3: Brute force attack

C. Existing System for Password authentication

The existing system proposes only generating the password based on the characters. It generates password by randomly choosing the characters. User's password will be stored by both the issuer and the user in their local storage. User need to enter their randomly generated password for each site. The password authentication uses only a character and it is not a strong password. It just gets information from user and stores it in the database. When, user enters password to login it checks the password with already entered password in the database and allow the user to access the application. It uses ASCII to secure a password. The basic

password authentication is shown in fig4.

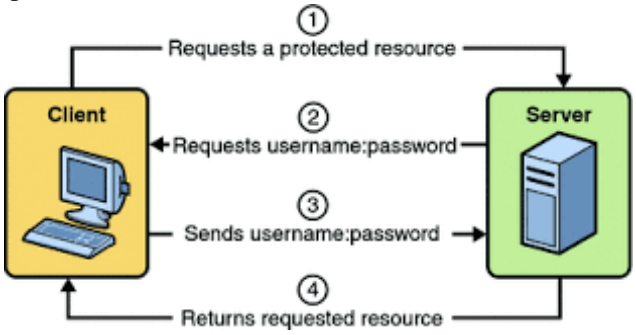


Fig 4: Basic password authentication

D. Issues in the Existing Work

There are some issues in the existing works which specifies that the password authentication in the existing work doesn't look strong. The existing work proposes that the strategy of password generation using the mnemonics shapes. In these, the mnemonics shapes are used to generate a password. Issues in these are shoulder surfing attack, which is the main issue in these works. It can be overcome by our proposed work. The mnemonic shape-based password generation simulation as shown in fig5. Patterns of all alphabets are shown in fig6.

Fig 5: Mnemonic shape simulation on keyboard

Mnemonic	Sequence	Mnemonic	Sequence	Mnemonic	Sequence
a	87yhj8ik	s	98ikj	K	YHNhuhm
b	4eserds	t	uio8ikl	L	YGVb
c	54er	u	7ui88io	M	CFTgbhujm
d	iuhj9ij	v	8iko0	N	YGVyhnji
e	ui87yhj	w	4r5t6	O	(*ui9
f	87ygftyu	x	8i9u	P	YHNyujh
g	poklpl,m	y	t6y7yg	Q	76tghu7j
h	9ijiok	z	78uhj	R	6yh67uyj
i	6yh	A	4es4rfer	S	987ujmnb
j	7ujh	B	5tg56yttyhg	T	%^&6yh
k	4rfr5rg	C	76TGH	U	5tghju7
l	7uji	D	UHBuikmnb	V	YHNji
m	i9o0p	E	yhnmyuhj	W	TGBhujmko
n	ujjuik	F	YGVyugh	X	&UJ8uh
o	09io0	G	87yhjik	Y	7u9ijn
p	okmoplk	H	UHBijnhj	Z	WERrdxXCV
q	76yu7uj	I	7898uhghj		
r	y7ujju78	J	8ikj		

Fig 6: Patterns for all Alphabets

III. LITERATURE GAP IN CYBER SECURITY FOR PASSWORD GENERATION

Most of the password generation strategy will be depends upon only the alpha-numeric characters. Even it uses alpha-numeric characters the information is not more secure. In the recent for generating a strong password Mnemonics based techniques are used by the author Jianhua song et al [1]. The Alphapwd which combines the order of writing a stroke of letters with generation of password to help the users for creating a safe and easily rememberable password. At last, results of these is that the password is generated is stronger than other password sets. In addition, analyzing the passwords generated by Alphapwd and Change of Keyboard, and Special Characters Insertion, it is found that the security in Alphapwd password is stronger than the other password generators.

Jun Luo et al has proposed that the password generation using RNN (Recurrence Neural Network) [2]. To determine the password vulnerability and to enhance user privacy, a recurrence neural network (i.e., long short-term memory (LSTM) and gated recurrent unit (GRU)) based password generation schemes is contributed for group attribute context-ware applications. In this work, different group attribute context-ware are considered for modeling training, and natural language processing (NLP) is adopted for password prediction, and the password similarity computing is established for analyzing the group relations. In these, it indicates that the group attribute-based password generation model has more accuracy than the ordinary model. By using RNN it takes over 18 hours of time duration to train the model with dataset and required to have a dedicated GPU (Graphics Processing Unit).

Jannatul Bake Billa et al had proposed an application for generating and managing password in the local storage itself [3]. This approach doesn't need to store the password anywhere like the existing ones. It will only save the three parameters that is set by the user to identify them in the local storage of the device where they installed the system. Hope this system is to provide the users with a safer feeling to use password manager systems as it becomes more secured.

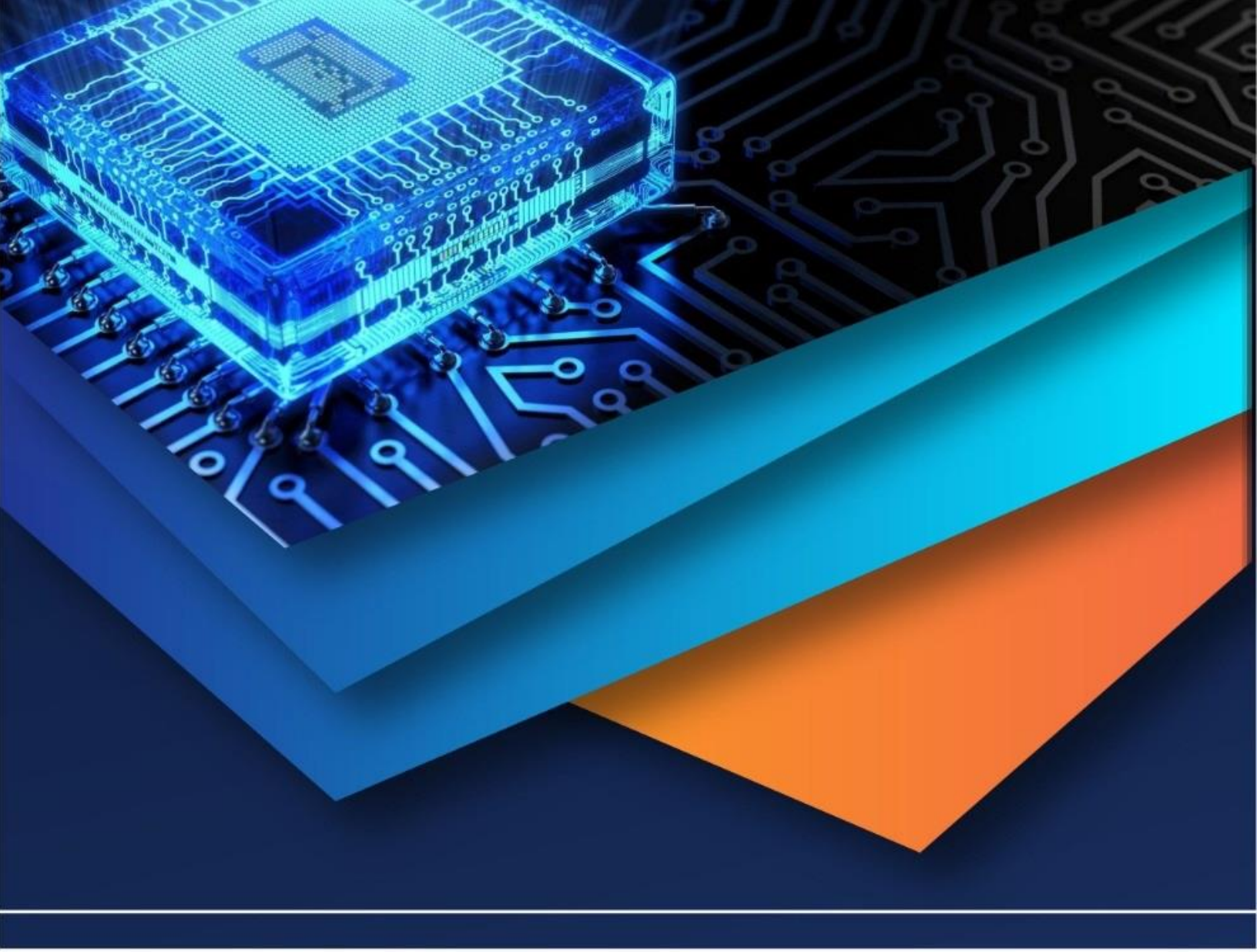
Farhana Zaman Glory et al have proposed a methodology for generating a password which is based on the user inputs [4]. In this paper, a unique algorithm is proposed which will generate a strong password. The password which is generating will be based on the users given information, i.e. (numbers and some words) so that they do not feel challenged to remember the password. The password generated will be in specific pattern so it is easy to crack the password by finding hashes for that pattern.

IV. CONCLUSION

To provide a secure way to access this password generator using scramble keypad and keyboard. No need for hardware keyboard. To generate uncrack-able, Unpredictable, strong password using special algorithm. No local memory or cache memory is to be used to save the generated password. Best means for privacy. Password recovery is done with Two-factor authentication. Withstand to all type of password attacks. In future, its more to be challenged to protect the information and its can be secure.

REFERENCES

[1] Jianhua Song et al [2019] - Alphapwd: A Password Generation Strategy Based on Mnemonic Shape
[2] Jun Luo et al [2019] - Recurrent Neural Network Based Password Generation for Group Attribute Context-Ware Applications
[3] Jannatul Bake Billa [2019]- PassMan: A New Approach of Password Generation and Management
[4] Farhana Zaman Glory [2019]- Strong Password Generation Based On User Inputs
[5] Authentication – https://en.wikipedia.org/wiki/Authentication
[6] Types of Authentication – https://www.solarwindsmsp.com/blog/network-authentication-methods
[7] Password Authentication – https://www.ssh.com/manuals/server-zos-product/55/ch06s01s01.html
[8] Password Attacks - https://solutionsreview.com/identity-management/the-top-7-password-attack-methods-and-how-to-prevent-them/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY