International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 08, August 2017
ISSN: 2455-3778
http://www.ijmtst.com

Enhanced Authentication Method using Keyboard Pattern Based Password Generation

R.Vadivukkarasi[1] | K.Kuppusamy[2]

[1]M.Phil Scholar in Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.
[2]Professor & Head, Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article
R.Vadivukkarasi and K.Kuppusamy, "Enhanced Authentication Method using Keyboard Pattern Based Password Generation", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 08, August 2017, pp.-37-40.

ABSTRACT

In recent years, network security depends largely on passwords to authenticate the user's data from hackers. The most common computer authentication methods are alphanumerical usernames as passwords. Many real life successful hacking, techniques attempt to enable unauthorized access to sensitive database. To seize password, hackers perform brute-force, dictionary or rainbow table attacks to reveal plaintext passwords. Dictionary attacks are very fast for cracking hashes but their success rate is not sufficient. However there are significant drawbacks in this method, to overcome this problem of security, authentication methods are developed by researchers that use image as password. A novel method that exploits several password patterns which are commonly preferred by users when trying to choose a complex and strong passwords is proposed in this paper. The method uses MD5 algorithm and SHA1 to secure the transaction and generate a random password using PBP technique. In order to analyze and show success rates of this proposed method, cracking tests on real-life leaked password hashes are performed using both traditional dictionary and pattern -based dictionary method. In this proposed method, to identified several patterns are used ten different schemes for securable transactions and communications are used the experimental result shows efficiency of the proposed method.

Keywords: *Authentication, Dictionary attacks, Pattern based attacks, Appending, Prefixing, Mixed-pattern Password.*

I. INTRODUCTION

Network security consists of the policies and practices to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security starts with authenticating commonly with a username and a password.

Authentication is one of the most important requirements for information security. An attacker hacks a system to reveal the passwords stored within database and get access to accounts of all users. In past many enterprise companies and organizations were victims of such attacks. Attackers frequently use SQL injection vulnerabilities that exist within applications in order to access database tables.

Passwords for identity authentication or access control are still widely used by means of ensuring system security despite the increased use of alternative techniques such as graphical passwords, smart-card or biometrics. However, these passwords are vulnerable to dictionary

attack. In an attempt to force users into selecting strong passwords, system administration policies often regulate several complex rules for creating passwords.

Users may be required to use numeric or special characters, have to enter passwords of a minimum length, and avoid words found in a dictionary. Users often struggle to create passwords that meet these requirements. In this research work, strong password generation for authentication purpose is taken into account.

II. PBP-GENERATOR

A new method for increasing success rates of resisting dictionary attacks. In this method analyzed leaked real-life user passwords and identified several patterns which are commonly chosen by many users to create a complex and strong password from a dictionary word a software tool, is developed namely pbp-generator ("pattern based password generator"), that implements the identified patterns and creates a new pattern-based large dictionary file from a given dictionary file.

2.1 Keyboard Pattern Based Password Generation

A software tool namely ***pbp-generator*** is created for benchmarking. pbp-generator gets a dictionary file as input, creates several variations of each dictionary word from the given input file identified patterns and adds them to the output file which represents the generated pattern-based dictionary file.

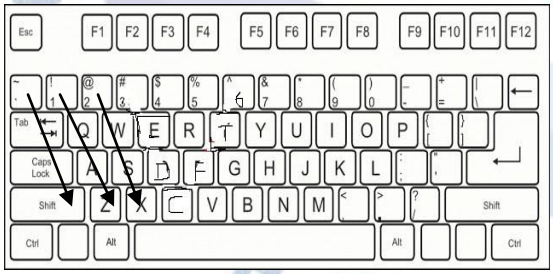


Fig:2.1 Keyboard Pattern Based Password Generation

Take a password "!qaz@WSX#edc" for example. This 12-character sample password is at first glance a seemingly random string; it is actually generated utilizing the keyboard layout. It is clear that the user chooses an easy-to-remember approach forming a keyboard pattern starting with the "!" key down to the "z" key without the Shift key pressed, followed by a parallel same pattern starting with the "@" key with the Shift key pressed, and then another similar parallel pattern starting with the "#" key down to the "c" key without the Shift key pressed.

2.2 Dictionary attack

Dictionaries are raw text files consisting of one word or phrase per line. Each line is a candidate match where each hash is computed and compared to the hashes to be recovered. The difference between a Dictionary and a brute-force attack is that a Dictionary contains a list of probable matches rather than all possible string combinations. A Dictionary needs to be well optimized otherwise if it includes any string combinations it risks becoming a brute-force attack and loses its efficiency. Therefore Dictionaries often include known popular passwords, words from the English and other languages, ID numbers, phone numbers, sentences from books etc. Rule based dictionary attacks are also very powerful. This attack uses the Rule Asset to mutate the Dictionary Asset and try to recover passwords using the improved Dictionary.

III. MD5 ALGORITHM

Md5 algorithm works around a 128-bit state, partitioned under four 32-bit words, indicated A, B, C, What's more d. These are initialized on certain settled constants. The principle calculation that point employments each 512-bit message square thus should change the position. Those preparing of a message square comprises from claiming four comparative stages, termed rounds each round will be made of 16 comparative operations In view of An non-linear capacity F, secluded expansion Also left revolution. Those md 5 algorithm will be marginally slower over md 4, Be that may be All the more preservationist to plan. Md 5 might have been outlined in view it might have been felt that md 4 might have been maybe continuously received for use All the more rapidly over advocated Eventually Tom's perusing the existing. On account md 4 might have been planned on a chance to be exceptionally fast, it will be during the edge As far as risking great sepulcher systematic strike. Md 5 backs off An bit, surrendering a little over speed for An substantially more amazing probability of ultimacy security. It fuse a few suggestions produced Toward Different reviewers, Also holds extra optimizations.

3.1 . Steps involves in MD5 algorithm

Step1: Enter password using keyboard. Read the keyboard password pattern.

Step2: Convert the keyboard pattern in to message digest using MD5 algorithm.
Step3: Split the bits as blocks.
Step4: Generate one time password.

a) Compute a 128 bit HMAC=MD5(K_{sh},N_h)

b) Generate a 64 bit authentication code using DES in CBC mode of encryption.

c) Generate a 32 bit value

32 bit value=x1,x2,x3,x4,.....x64

d) OTP = Hexa Decimal (32 bit value)

Step5**:** Performance encryption

BEGIN

INPUT : PT (plain text),K (key)

Choose a key with length equal to plain text.

Convert both plaintext and key in to its ASCII values and their equivalent binary value.

In pre processing,

$PT_i = PT_i (XOR)_{REV}$

P_{TP} = Binary value of Plaintext

K_b= reversed binary value of key

Calculate n

n = MAX (ASCII in K)/6 \\ n is calculated by dividing the highest ASCII value by 16.

n = number of bits. Shifted right.

END

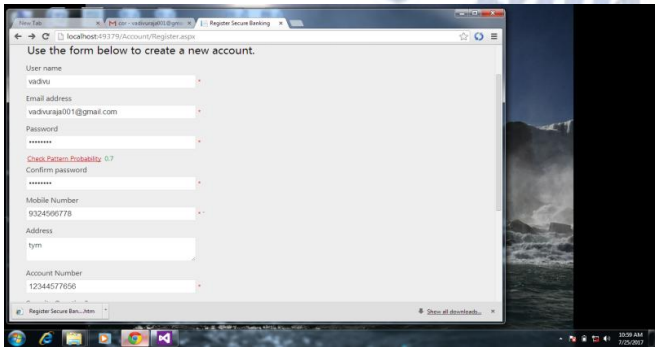
3.2 Algorithm description

Normally the data are stored and viewed as a user readable format. but in proposed method the data are stored & viewed as a encrypted format, to increase more security. To ensure the security large number of bits are used.

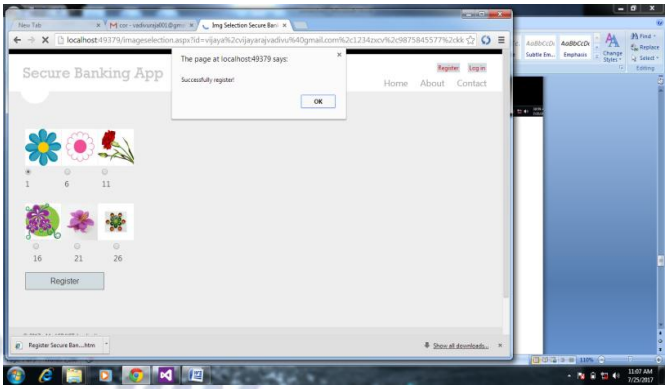
IV. Experimental Results For Banking Transaction

This proposed system is implemented in the Banking Transaction. In banking transaction the above mentioned algorithm is used for encryption process. The major functions of banking transaction are Withdrawal, Deposit and Balance Enquiry.

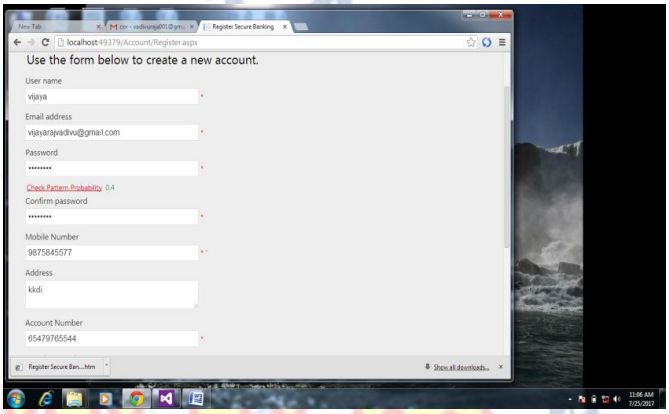
User account creation



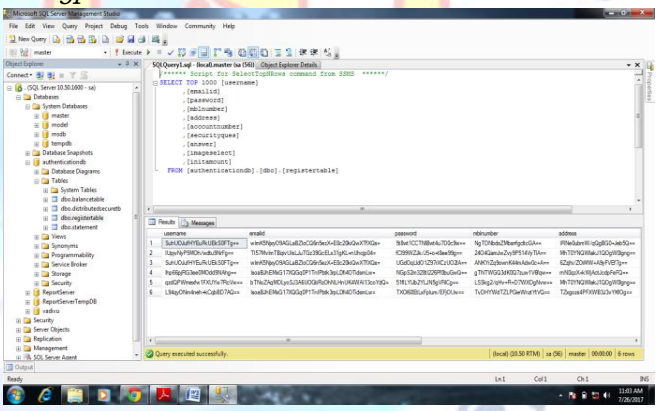
Capcha selection



Another account creation



Encrypted table



V. Conclusion

Weak passwords are critical threats for authentication systems. Seizing password hashes, especially unsalted hashes, attackers can use different attack techniques (i.e. brute-force, dictionary, rainbow-tables) to crack hashes and reveal plaintext passwords. Security experts try to establish security awareness for strong passwords. In addition, authentication systems enforce password policies to fulfill complexity rules. Being forced to use strong passwords, people tend to use similar patterns when choosing their “strong” passwords. But such patterns endanger security of passwords. Dynamic-encryption scheme could avoid directly stealing and modifying of the IDs of the users who are having accounts. The dynamic

ID generation mechanism provides a reliable one-time-password to the users.

ACKNOWLEDGMENT

I would like to thank Dr.K.Kuppusamy for his guidance and support for preparing this paper.

REFERENCES

[1] L. O'Gorman, "Comparing passwords, tokens and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[2] (2011). PlayStation Network Hack: Why it Took Sony Seven Days to Tell the World. [Online].Available:http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstationnetwork-hack-sony

[3] (2009). Rock You Hack Compromises 32 Million Passwords.[Online].Available: http://www.scmagazine.com/rockyou-hack-compromises-32millionpasswords/article/159676.

[4] (2013). Software Company Tom Sawyer Hacked, 61,000 Vendors Accounts Leaked. [Online].Available:http://www.databreaches.net/software-company-tom-sawyer-hacked-61000-vendors-accounts-leaked.

[5] M. Weir, S. Aggarwal, B. de Medeiros, B. Glodek, "Password cracking using probabilistic context-free grammars", Proc. 30th IEEE Symp. Secure Privacy (SP), pp. 391-405, May 2009.

[6] (2013). Hackers Leak Data Allegedly Stolen from Chinese Chamber of Commerce Website. [Online]. Available: http://news.softpedia.com/news/Hackers-Leak-Data-Allegedly-Stolen-from-Chinese-Chamber-of-Commerce-Website-396936.shtml.

[7] Shuo Chen and Maode Ma, "A Dynamic-Encryption Authentication Scheme For M2M Security in Cyber-Physical Systems".