International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Password Cracking Technique : A Survey

Himanshu Kumar, Neelam Mathur
UG Scholar, Dept. of CSE, Lingaya's GVKS Institute of Management & Technology, Faridabad, India
himanshu996kumar@gmail.com, neelammathur1996@gmail.com

Abstract: ***As the word implies, Personal Account Security System WORD (PASSWORD) is a secret word or expression used by authorized persons to prove their right to access, information, etc. Nowadays, attacking the passwords is one of the most straightforward attack vectors, which authorize access to information system. Password cracking is the process of guessing or recovering a password from stored locations or from a data transmission system. This paper is mainly to give a brief review of the password cracking methods and import techniques of password cracking and this paper also highlights a new technique for password cracking. Different methods of cracking are explained, including dictionary attack, brute force, and rainbow tables. Password cracking across different mediums is examined.***

Keywords: Algorithms, Brute force attack, Dictionary attack, Passwords cracking tools, Rainbow attack, Security, Techniques Vulnerabilities.

I. INTRODUCTION

Nowadays, security becomes very big issues, many developed countries such as the united state of America(USA), Russia, united kingdom(UK), China, etc very used to ensure the security of their country from hackers of other countries. This is the most dangerous thing for any country that there data is secure or not, as the world know that the data lost is the big problem for any country and for anyone. Bleaching of security is also sometimes is very useful for some department for securing their data by gathering important information about terror attacks or any suspicious activity that can be dangerous for a country or any organization. There are many techniques which are used to crack the passwords or decryption algorithms are used to crack passwords but there are also many complicated algorithms are used to secure the passwords.

Personal Account Security System WORD (PASS WORD) is a word or string of characters used for user authentication to prove identity. Cracking password is really a pretty difficult task to complete and much more difficult to secure it. There are many examples that are used in movies and games for cracking password and making strong password as strong it can be. All these movies gives an idea or a aim to do something unique to secure world as possible as can.

There are lots of techniques are used to cracking the password and lots of algorithms also used to secure passwords. Under below are some cryptography techniques are used now a days.

II. PASSWORD CRACKING

Password cracking is one of the techniques which is used to crack the password is some manner. At the defense level, restoring the data from the waste computers or destroyed computer is essential for them. So the password cracking at that time is very important for us.

Password cracking in leman language is cracking the password for some use with a particular technique. The Password can be cracked by some methods that given below:

1. Guessing:

Guessing the password is one of the common and simple technique used. There are lots of other techniques which are used to crack the password but the mainly used technique is guessing a password because it is easy to do but the probability of getting the correct password is very low.

Mainly the password is related to the date of birth, family name, love one's name, etc. so the password is easily guessable at that time.

2. Dictionary Attack:

The dictionary attack is another type of password cracking technique which is most of the time and it is more reliable than the guessing the password. The dictionary attack is nothing but the combination of words which is stored in a particular file or a folder and match with a password column. It will check one by one word to that dictionary. If the password is misspelled, is in another language, or very simply uses a word that is not in the dictionary or profile, it cannot succeed. Most of the time, even using two words in one password can thwart a dictionary attack. The percentage of getting a correct password is 40% or maybe less or more. It can differ.

Example of tools are: John the Ripper, Cain and Abel

3. Brute Force:

Brute force password attacks are the last resort to cracking a password as they are the least efficient. In the most simple terms, brute force means to systematically try all the combinations for a password. This method is quite efficient for short passwords but would start to become infeasible to try, even on modern hardware, with a password of 7 characters or larger. Assuming only alphabetical characters, all in capitals or all in lower-case, it would take 267 (8,031,810,176) guesses. This also assumes that the cracker knows the length of the password. Other factors include number,

case-sensitivity, and other symbols on the keyboard. The complexity of the password depends upon the creativity of the user and the complexity of the program that is using the password.

The upside to the brute force attack is that it will ALWAYS find the password, no matter its complexity. The downside is whether or not will still be alive when it finally guesses it.

4. Rainbow Attack:

Rainbow tables are a type of pre-computed password attack. The last two attacks, Dictionary and Brute-Force, enter a password into the locked program, it compares the hash to the correct password hash. Rainbow tables compute hashes for each word in a dictionary, store all of the hashes into a hash table and then retrieve the hash of the password to be cracked, and do a comparison between each password hash and the real password hash. It can retrieve the hash of the password to be guessed and the hashing algorithm is the same between the rainbow table and the password. As comparision, low-security hashes are computed using MD5, sometimes SHA-1. Rainbow tables have only become an efficient technique recently, as the hard drive space needed to store the hashes was slightly cumbersome until memory became cheaper.

III. CRYPTOGRAPHY TECHNIQUES

Cryptography is one of the essential technologies used in building a secure VPN. Different applications of the same basic algorithms can provide both encryption that keeps data secret and authentication that ensures the two security peers in a VPN are who they claim to be.

1. DES:

Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which understand that both sender and receiver use a shared key to encrypt and/or decrypt the data.

The problem in this is that if a persona pattern of encryption of a single alphabet or variable then this technique can be compromise.

2. Triple DES:

An enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level.

The triple DES key length contains 168 bits but the key security falls up to 112 bits.

3. AES:

Advanced Encryption Standard, is the new encryption standard recommended by NIST to replace DES. This is technique is mainly used by the US government and many other countries. This mostly used technique because it uses mostly 192 and 256 bits i.e., really a very high encryption.

4. Twofish:

Twofish is also a symmetric block cipher having festal structure. it provide more security and its level is also nice and its contains total 16 round of encryption, in addition it made 128 bits cipher text after completing 16 around on encryption.

5. Blowfish:

Blowfish is that type of algorithm which is designed to replace the DES technique. This symmetric cipher splits messages into some block around 64 bits and encrypts them separately. Blowfish is famous for its highly faster speed and overall effectiveness as many claim that it has never been defeated. Seller or retailers take full advantages of its free availability in the public domains. Blowfish can also be found in this e-commerce platform for securing the payments to password management tools. It is most useable encryption technique.

Under below Diagram shown a working of Blowfish.

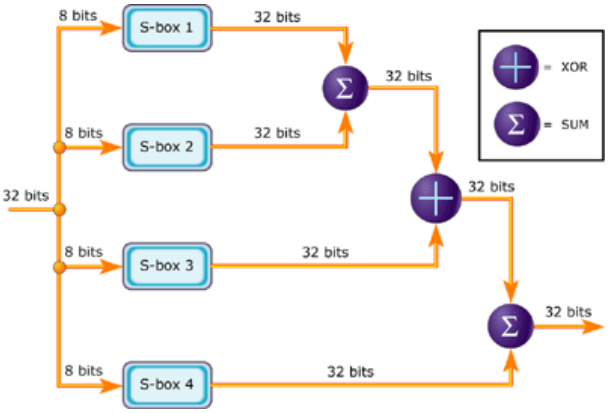

Fig. 1. Encryption Data by Blowfish Algorithm

IV. RELATED WORK

Brute force, Rainbow attack and Dictionary attack all these are very useful attack for password cracking.[2] There are many methods and techniques can conduct password cracking, in the on-line or offline environment. The tools that can guess the passwords for differential goals and certain prevention tactics are presented. Password cracking strategies are also researched and analyzed and many surveys are also presented on this topic.

V. ISSUES

Resources will continue to be updated, and there will be latency before the new configurations are updated. Attack chains will have multiple possible paths with

different representations of each link type. Attackers may find still new ways to breach and intrude into someone's privacy. Also, risk can be compromised but can't be removed completely.

VI. FUTURE WORK

The idea behind password cracking techniques is that to improve the types of attack that today's world are using. It can be improved by upgrading the techniques that are using or it can be improved by generating new techniques to solve or crack the password.

One of the best advantages of giving a new technique is that it is more reliable and the world doesn't know about it. The technique which is the main idea of this paper is to collect all the symbols, numerical and characters in a particular folder with including upper character and lower characters. Then try to match which character with an Encrypted password and computer takes only the meaning full word and then stored in a particular folder one by one then the chances of guessing the password will be increased.

After matching and storing the words, guessing the password will take the less time and improve the efficiency of getting near to password. Each character will tell a new word but the meaning full word can be found easily, if it doesn't make the meaningful word then the word will be discard.

It is little bit related to the Rainbow attack. Rainbow attack also use all this characters, numerical and special types of character but this technique is little bit different from this rainbow attack.

VII. REFERENCES

[1] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S ,"A Review on Password Cracking Strategies", International Journal of Security and Its Applications

[2] www.ijrcct.org/index.php/ojs/article/view/664/pdf.

[3]http://www.ijser.in/archives/v2i11/SjIwMTM0MDM=.pdf

[4] Rajdeep Bhanot1 and Rahul Hans2 "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015).

[5] https://www.embedded.com/design/configurable-systems/4024599/Encrypting-data-with-the-Blowfish-algorithm.