Cross Attack: An improvement for Dictionary Based Attack

Tanvi
Software Engineer
Samsung Electronics, SRI-Noida

Abstract: Password cracking is used everywhere either by government agencies or by hackers. Already existing techniques of password cracking are not capable of cracking more passwords in less time. This paper introduces a technique which can crack more passwords as compared to dictionary attack based on same dictionaries in almost the same time.

Keywords: Cross Attack, Password Cracking, Dictionary Attack, Better Dictionary Attack

INTRODUCTION

Password cracking is an upcoming research area these days. As more and more powerful computers are being developed, Govt. agencies and people are getting into field of break opening password protected data. The development of cloud computing has also helped in the Password Cracking. Amazon's EC2 can be used to crack password by applying a brute force attack. [1] Although the cost to crack a password increases as length and complexity increases but we can still crack the passwords. [2]

Dictionary attack is based on a list of words known as Dictionary. Dictionary attack is useful in breaking only simple passwords. Dictionary attack is not able to break complex passwords.

While Brute Force attack is 100% successful if the length and character set is known, the time taken by Brute Force is so long sometimes that it becomes impractical to make a Brute Force Attack.

So a solution which is intermediate between the two is developed and discussed in this paper.

I. DICTIONARY ATTACK

Dictionary attacks are based on the tendency of a user to select a password which is easy to remember or can be categorised by other means[3]. The Dictionary consists of the words that are related to the user e.g. the name of the user, the names of family members, file name which is protected, and words from a local dictionary etc. A dictionary can contain from a few word to several thousand words.

Dictionary may consist of following:

- All the words from local language dictionary
- Dictionary with words spelled backwards [5]
- List of first names, last names, city names etc
- Above with initial upper-case letters[5]
- Room numbers, telephone numbers, vehicle license plate number[5]
- Common phrases of local language[5]
- Important calendar dates, like date of births of family members of users.[5]
- Lines from songs[8]
- Book titles[8]
- Famous Movie Dialogues[8]

Dictionaries consist of words that vary in character sets and lengths. This makes it faster as compared to Brute force attack as it tries only most probable passwords. Dictionary size can vary from a few bytes to several Giga Bytes also. We can use different compression techniques to store these dictionaries. [3]

Dictionaries are of two types, the first type of dictionary consists only of most probable passwords whether from local dictionary, or user's environment. These dictionaries have a variable success rate ranging from 0%-100%.

The second type of dictionary is created for brute force attacks, which contains all the possible passwords of given length and from a given character set [3]. These dictionaries have a 100% success rate for passwords of corresponding length and character set. This form of dictionary is also available in a pre-compiled form, known as Rainbow Tables. This dictionary contains the word and the corresponding Cryptographic Hash Value. Rainbow Table is a special form of dictionary which handles the problem of Space-Time Trade-offs. A rainbow table contains several words in each line to reduce the size of the dictionary. Rainbow tables are used widely by crackers to crack passwords. These tables are available easily on the internet and are available for different cryptographic hash functions like MD5, SHA1, LM DES etc

Dictionary attacks thus have a success rate ranging from 0% to 100%. The dictionary with 100% success rate is very large in size, requires a lot of space, a lot of time to check and is able to crack complex passwords. While dictionaries with success rate less than 100% are faster to check, smaller in size and can crack only simple passwords.

The Dictionary attack was developed as a solution for fast password cracking. If we use the second type of dictionaries then the purpose is not solved as the time taken is very large. Thus we have a disadvantage that only simple passwords can be cracked if we use dictionary attack.

II. CROSS ATTACK: THE IMPROVEMENT

Cross Attack is an intermediate between the Dictionary Attack and Brute Force attack. This attack is a combination of Dictionary Attack and Brute Force Attack. Cross attack modifies the dictionary by appending some text to all the words in the dictionary. The text that is appended is calculated by the help of Brute Force Attack. The text appended is a list of all the passwords that can be formed from a character set containing all the special characters and digits, the lengths of word is 1, 2 or 3. The text appended is either suffixed or prefixed to the words in the dictionary.

Cross attack is also based on the tendency of user to select easy to remember passwords while trying to make the passwords complex. The passwords are made complex by combining an easy to remember password with a suffix or a prefix. This suffix or prefix increases the complexity of password while maintaining the ability of easy remembrance.e.g. An easy to remember password is "password", this password is very easy to break as "password" is a very common word. Due to rules imposed by certain websites and programs for selecting password, the users generally modify the password and append some text such as "123" and the new password becomes "password123". This password is difficult to break as it is not a meaningful word but a combination of meaningful word and a random text.

Cross attack modifies the dictionary and then appends these random texts to each word. e.g. if a dictionary contains words as

- password
- mobile
- computer
- monkey

The chosen character set for suffix/prefix part is "!@#$" , the length of suffix is chosen as 2, then the different texts possible from the above inputs are

!! !@ !# !$

@! @@ @# @$

#! #@ ## #$

$! $@ $# $$

Now each text is combined with every word in dictionary, so the new crossised dictionary becomes.

password!! password!@

…..

password$# password$$

mobile!! mobile!@

…

monkey$# monkey$$

The cross dictionary size is 16 times the size of normal Dictionary but Cross Dictionary covers most of the complex passwords thereby increasing the chances of success. Although the success rate is still between 0% and 100% but the chances of a success have increased.

The Cross attack takes time intermediate between the Dictionary attack and brute force attack. The time depends on the size of the dictionary, the length of text appended, and the character set chosen for text. If the character set chosen contains 10 characters and the length of selected text is 2, then the number of possible suffixes/prefixes is 100. So the size of the cross dictionary will increase 100 times. If Dictionary attack would have taken N seconds to complete then the Cross Attack will take

$$T=N*C^L$$

Where T is the Time taken to complete, C is the size of the Character Set, L is the Length.

Hence in our example the time required for Cross attack will become 100N seconds.

III. EXPERIMENT

We conducted an experiment on several password lists containing cracked password available on the internet [6]. The results compare the number of passwords cracked using dictionary attack and the number of passwords cracked using a Cross Dictionary.

Dictionary available on John the Ripper website [4] is used to perform dictionary attack. This dictionary is then Crossed using following character set

0123456789`~!@#$%^&*()_+-=:";'{}[]|\<>?,./'

with suffixes of length 1 and 2. The number of suffixes for each password are (43 + 43*43) = 1892. So the Crossed Dictionary size is 1892 times the size of original Dictionary. Table 1 shows the results of attacks based on the normal and Hybridized Dictionary on 4 different Word Sets [6].

Word Sets

A. MySpace Word Set (MS): This word set contains passwords of MySpace account that were made public in October 2006. The passwords were captured using phishing attacks. This Word Set contains words made from English Upper Case letters, English Lower Case letters, Special Characters and numbers. MySpace impose restrictions on the type of passwords selected by the users by making them choose password containing alphabetic and non alphabetic characters.

B. Elite Hacker Word Set (EH): This set contains words of multiple lengths with character set containing English Upper Case Letters, English Lower Case Letters, and Numbers. The word set is obtained from [6] and the source of data set is [7].

C. Conficker Worm Word Set (CF): This set contains a list of words that was used by Conficker worm to spread in different machines. The list contains words of multiple lengths, with words made from character set of Lower Case English letter, Upper Case English Letter, and Numbers.

D. Facebook Word Set (FB): FB set consists of passwords of Facebook account phished during September 2010. This set contains words of variable length that are formed from a character set of Lower Case letters, Upper Case Letters, Numbers and special Characters.

Password list name	*No of Passwords to crack*	*Passwords cracked by Cross attack*	*Passwords cracked by Dictionary attack*	*%age improvement*
MS	1753	191	16	1093.75
EH	895	267	219	21.9178
CW	182	110	62	77.4193
FB	2437	181	66	174.242

Table 1 displays the number of passwords cracked by normal dictionary attack and the crossed dictionary.

From Table 1 we can see that a Crossed dictionary always breaks more passwords as compared to normal dictionary. In our tests we have received an improvement ranging from 21% to 1093% which indicate that the chances of cracking a password increases in an cross attack even if the success rate lies between 0% and 100%.

From the above 4 results we see that in case of elitehacker list the improvement is only 22% which means that passwords in this list are very simple and easy to remember. While in case of Myspace list we have seen a very major improvement of 1093% which means that although the users use simple and easy to remember passwords, but they try to make the passwords difficult to crack by incorporating some special characters.

Figure 1 gives a graphical representation of the number of passwords cracked by Normal Dictionary and Crossed Dictionary for different lists.

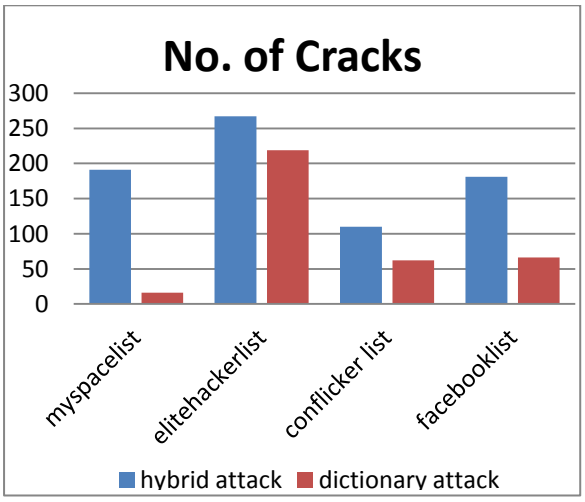

Figure 1: Comparison of Passwords cracked by Normal and Crossed Dictionary

Out of 4 list, MS and FB list contains passwords which contain alphanumeric with special characters as character set. Nowdays, Aphanumeric with special characters is considered as best character set for choosing passwords. This character set make strong password. Figure 1 shows that MS and FB list shows best results on cross attack over dictionary attack. It states that Cross attack is successful on best character set used for generating passwords.

IV. CONCLUSION

Dictionary attack for cracking password was very successful in the early days when users used to keep passwords that were easy to remember meaningful words, but as the information available to the user increases, users select passwords that are complex but still easy to remember, so we have proposed a modified form of dictionary attack which is almost as fast as a Dictionary Attack and can crack complex passwords. Based on the results we can conclude that if the suffixes and prefixes are carefully chosen then we can achieve an improvement of upto 1093% in the number of passwords cracked which itself explains the advantage of Cross attack

REFERENCES

[1] *Amazon's EC2 brings new might to password cracking*(Online, 2012)**:** http://www.theregister.co.uk/2009/11/02/amazon_cloud_password_cracking/

[2] *Cracking Passwords in the cloud: Insights on password policies*(Online, 2012): http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html

[3] T.Fisher, *"Everyday Password cracking"*IRM Research white Paper, Dec 2007

[4] *John the Ripper password cracker*(Online, 2012): http://www.openwall.com/john/

[5] R. Morris, K. Thompson; *"Password Security: a case study",* Comm. Of ACM, Vol 12; Nov 1979

[6] *Passwords SkullSecurity* (Online, 2012): http://www.skullsecurity.org/wiki/index.php/Passwords

[7] *Elite Hacker Website:* http://www.elite-hacker.com

[8] Kuo, Cynthia; Romanosky, Sasha; and Cranor, Lorrie Faith, "*Human Selection of Mnemonic Phrase-based Passwords*" (2006).Institute for Software Research. Paper 36.