ISSN:0975-9646

A Model to Restrict Online Password Guessing Attacks

Aqib Malik , Dr. Sanjay Jamwal

Department of Computer Science,

Baba Ghulam Shah Badshah University, Rajouri, J&K, India

Abstract— **Passwords are a critical part of information and network security. Password serves as a basic mean of authentication to protect user accounts but a poorly chosen password, if compromised, could put the whole network at risk. Password are one of the most common reason for the security breakups. Online guessing attacks (brute force attack and dictionary attack) on password protected remote login services increasing rapidly. Providing legitimate user's login conveniently while preventing such type of attacks is difficult. Automated Turing test (ATT) are effective and are very easy to implement but cause reasonable amount of inconvenience to the legitimate user. Here in this paper we have proposed a model which limits the number of login attempts from unknown source IP address as low as three attempts and the user can make five failed login from the known and frequently used machine.**

Keywords— **Online guessing attacks, Brute force attack, Dictionary Attack, ATT.**

I. Introduction

Today majority of the system uses password as a means of authentication. Passwords are very suitable for the user and are easier to implement and as a result are very popular for user authentication. Although there are many authentication mechanism have been suggested in the past but none of them got good response in the consumer market [1]. Authentication based on password is very convenient, but also has some drawbacks due to the very nature of this system. Humans have a very great trends of choosing very simple, easy and short password which can be easily remembered like name of their loves one, pets name, date of birth etc. As a result chosen password belongs to a small domain. Passwords are Used with user name to get access to the secure system.

Passwords ranges from single character to the hundreds of characters in length. The purpose of the password is to authenticate a user. This information is only known to the user. Passwords are used to secure a system or account, in Which users have their secret and personal information, in other Words by using password user has secure their system or account from unauthorized user. A typical user has password for many purposes: logging in to web account, reading email, using social networks, using banking accounts, and many more the purposes go on. As the passwords keep on growing, the purpose to maintain secure account also keeps growing. The account is secure when it has secure password. User should never limit the password with personal information, as it is easy to guess and used by unauthorized user. User should create a strong password

Password guessing attacks are done by the human beings and by some malicious software (botnet). These attacks can be launched easily by any one due to the free availability of these software over the internet. Some of the software which are used for the purpose of guessing are "John the Ripper, Crack, and Rainbow Crack". The password guessing is possible for the attacker because the attacker is free to make as much guesses as he can .If the login machine do not locks the account from many unsuccessful attempts have made it is easy for the attacker to make online guessing. Alternatively the attacker can also done offline attacks, the attackers machine gives the hashed value of particular targeted password. Hash values of the password can be obtained by the continuous monitoring and capturing of the network traffic, yet this can be prevented by using the "Encrypted Key Exchange". Still the vulnerabilities of operating system and the failures due to access control can lead password database. Moreover password database can be stolen by the insiders with the physical access to the system device.

II. LITERATURE REVIEW

A lot of work has been done in the past in order to make user account protected against online password guessing attacks .Some of the past work is discussed below.

A. Account Locking

In this mechanism of account locking the account of the account holder is locked for some particular time (say 24 hours) after a fixed number of failed login attempts made by the user (account may be locked if the failed attempts are more than three or five with in a given time)[2]. This mechanism is useful in preventing online password guessing attacks, but with having some limitations. If this feature of account locking is adopted then the system will become susceptible to the denial of service attack in which an attacker knowingly launch many failed login attempts so that the genuine user remain deprived from the service with in a fixed period of time.

B. Delayed Response

In this mechanism the service provider provides a delay response to the user request, say for example not faster than one answer per second i.e. the server responds after consuming some time for the user request. This may prevent an attacker from checking enough number of passwords in a fixed period of given time, because the service provider responds slowly and in a particular given time the attacker gets slower response. Due to the delayed response mechanism the attacker guesses limited password.

Delayed response scheme is very suitable for the local machines from which the user of an account logins from physically attached keypads. Yet, it is not effective for the large networking environment. The attacker can login many attempts in parallel and can beat the timing measures using a fact that the login of the user are dealt by the servers that can address login in sessions in parallel example, "the attacker can send a login attempt every 10ms, thus obtaining a throughput of 100 login attempts per second" irrespectively how much the server delays the response [2]. This method of delayed also suffers from "global password attacks". A system which have a large list of user accounts over a network which is approachable to the attacker suffers from this attack

C. SPAKA

SPAKA stands for strong password-based authentication and key agreement is a protocol which provides user authentication and key agreement over unsafe channel of network without the support of previously shared cryptographic key. SPAKA protocols are susceptible to online password guessing attack, but do not disclose any information of the user, more over it is not susceptible to eves dropping and man in middle attack [3].

In addition to the online dictionary attack the 3-pass SPAKA protocol are susceptible to a more powerful many- to- many password guessing attacks. In case of 3 pass SPAKA protocol when the user is going to login, the protocol the service provider sends out only a message that carries a challenge for the server side and its proof of the acknowledge of the verifier. The attacker then collect these values and then send these values to protocol at the end of the second pass. The attacker then use the value to manage password guessing attacks offline. She can start multiple of such operating sessions and gather a lot of information before the server finds out the attack.

D. CAPTCHA

CAPTCHA (stands for completely automated public Turing test to tell computer and humans apart) is a challenge response test which is used to find out whether the user is human or not" [4]. In CAPTCHA some challenge is put before to a user when the user is going to access his account. These challenges, for example a badly formed and a scattered image of a word with some falsified text in the background, which is for humans to answer instead difficult for computers (an online attacker is essentially a programmed computer) to answer [5] [6]. This scheme is a good defence against password guessing techniques but for a genuine user who is putting correct user name and password to a machine from where he has logged in several times has also to pass this test in order to access the account. Fig. 1 is an example of text based CAPTCHA[7].

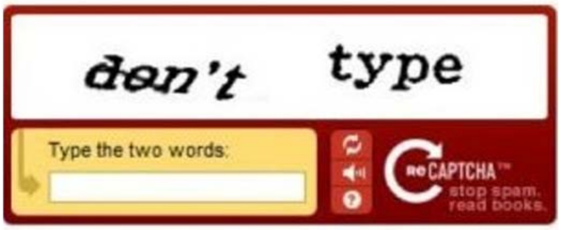

Fig. 1 Text based CAPTCHA

III. ANALYSIS OF BRUTE FORCE ATTACK AND DICTIONARY ATTACK.

A. Analysis of Brute force Attacks

Brute –force attack can be launched by the rigours searching of hash values of each and every chosen set of characters and the length of string. Now these calculated hash values are compared with hash values which are stored on the database of server until the match is found. Example of the brute force attack of the English alphabets from the length of eight lowercase alphabets are "aaaaaaaa", "bbbbbbbb" upto the end "zzzzzzzz".

Brute force attack constitutes of trying all possible code and combinations until the correct one is found [8]. It tries every combination of digits from 0-9, letters a-z and some special characters e.g. abc, cba, bca, etc.

The complete brute force attack which includes all the numbers 0-9, alphabets a-z and special characters in theory is guaranteed as the success rate of 100% yet attempting brute force attack of more than 8 characters, the time to needed to carry out the attempt becomes difficult because of the huge key space.

B. Analysis of Dictionary attack

Dictionaries are "raw text files" consisting of one word or a phrase in a line. In a dictionary attack the user guesses the words which are commonly used like name of user, pet's name, date of birth etc. [9]. Each line in the "candidate match" in which the hash value is calculated and then compared to the hashes to be recovered. The difference between the two attacks i.e. dictionary attack and brute force attack is that Dictionary is list of all possible names places or mobile numbers rather than the possible string combinations. A dictionary needs to be well optimized otherwise it risks to becomes a brute force attack and hence loses its efficiency. Therefore dictionary list includes the passwords which are popular and the words from the English language. Dictionary attacks are of commonly two types.

1) Combined Dictionary attack

Combined dictionary attack is ta type of dictionary attack which is composed from several dictionaries by combining the strings through the string concatenation operation in order to produce a "combined dictionary" e.g. we have a one dictionary of a university name bgsbu and the other dictionary is rajouri we concatenate these two dictionaries to form a combine dictionary i.e. bgsbu+ rajouri=bgsburajouri. This is a new technique which has been brought because it has been come into notice in order to make secure passwords user combines several passwords into one combined password. Table1 shows a Combined Dictionary.

TABLE I
Combined Dictionary

Input	Output
Bgsbu Rajouri 1234	bgsbubgsbu bgsbu1234 rajouribgsbu bgsburajouri 1234bgsbu 12341234 1234rajouri rajouri1234

2) *Hybrid Dictionary attack*

Hybrid dictionary attack are the combination of dictionary attack and brute force attack. In a hybrid base attack dictionary words taken as an input and adds the brute force string to each entry of dictionary. Hence for each string of dictionary it produces lot of other strings e.g. Dictionary entry "*orange*" produces "*123orange*", "*124orange*" up to "*999orange*" .This kind of dictionary attacks results in the "exponential increase computation" and time based on the amount of character to be added with the entries of dictionary.

IV. PROPOSED MODEL

Automatic Turing test is very effective for the defence of automatic online password guessing attacks. ATT creates inconvenience to the legitimate user who puts correct pair of user name and password must answer to ATT on the login attempts. In order to improve this problem we have proposed this model which is very friendly for the legitimate user and is very effective for the defence of online password guessing attacks. This model improves the user security, usability trade-off, and is more efficient beyond browser based authentication mechanism. In order to limit the number of password guessing attacks this model enforces ATTs after a five failed login attempts from a known machine and three failed login attempts from unknown machine. The known machines are those machines from which a successful logins have occurred in a fixed time. The machines are identified by their IP addresses saved on the login server as a white list (WL). White listed IP addresses will expire after a certain fixed time. By tracking through IP addresses it provides the given model to increase the number of complexities for the password guessers while it decreases ATTs for the genuine user attempts for each login. This model have a data structure containing all the log information. It also maintains the white list of IP address failed login attempts from a known machine (F_KM) as well it also maintains the list of failed login attempt from unknown machine (F_UM). Table II shows list of Abbreviation used.

Proposed model maintains three data structures.

1. WL: - A white list of source IP address, user name and password such that for each pair, a successful login from the source IP address has been initiated for the user name previously.
2. F_KM:- Entry in this table represents the number of failed login attempts from a known machine.
3. F_UM:- Each entry in this table contains the number of failed log in attempts from unknown machine.

TABLE II
Abbreviations used

Notation	Description
UN	User Name
PW	Password
WL	White list
F_KM	Failed login from Known machine
F_UM	Failed login from Unknown machine

A. *Working*

If the IP address is already in F_KM and F_UM deny access for a fixed time shown in fig.2.

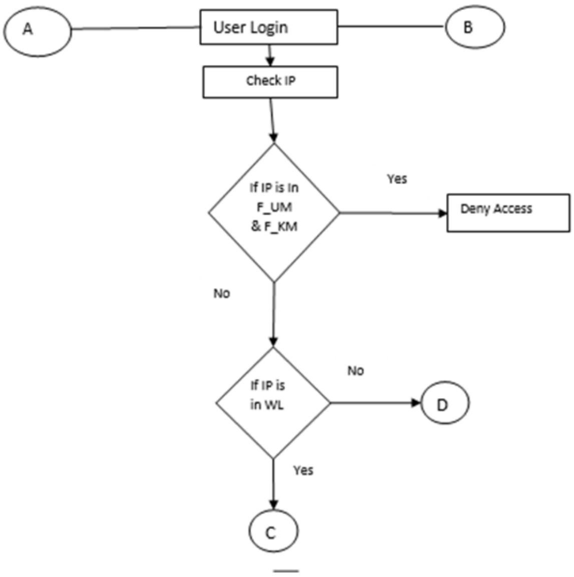

Fig. 2. IP is already in F_UM & F_KM

1) *When Login is done from a known machine.*

I. Read the user input i.e. user name and password, If the provided credentials is from IP address which is present in White list (WL) and login attempts is less than and equal to 5 .In this case the user is granted access to his/her account.
II. If the provided credentials is incorrect for attempt is less then and equal to 5, then the IP

address of that system is deleted from white list (WL) and it will be added to data structure containing failed login from the known system (F_KM).

III. The user will be blocked for a fixed period of time.

IV. If again after fixed time the user login attempt is made from the same IP address then the user has to go through the multiple Turing tests. If all the entries are correct then access is granted. Fig. 3 shows the working of login done from a known machine.

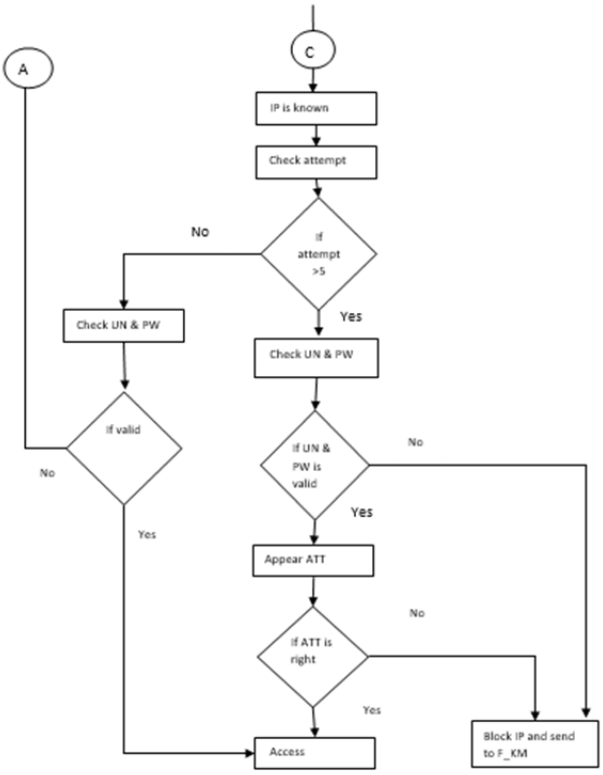

Fig.3. Login from known Machine

2) *When Login is done from an unknown machine*

I. If a valid user name and password is provided from an unknown machine (An unknown machine is that from where no successful login has been occurred in a given time) then there is no need to answer the ATT. Once the user successfully logins the account the IP address of that particular system is added to the white list (WL).

II. If the entered pair of user name and password is not valid at first attempt and the IP address is not present in while list (WL) at that time the user can make three more login attempts. If still user name and password is invalid then the IP address of that system is sent to F_UM and user has to go through the ATTs.

III. Then again the user is provided a chance to login to the account, if the user name and the password is correct then he has to go through the ATTs.

IV. If the user is failed to attempt the first ATT then the user has to face another ATT test. If he successfully go through the ATT he has to go through multiple ATT (logical answering, text based captcha, puzzle test etc.).

V. If the user successfully answers all the multiple ATTs then the user is granted access to the system.

VI. If the user makes failed login attempts grater then three then IP address of that system is sent to F_UM and the user will be blocked from the account for a particular time period. Fig. 4 shows the flow chart when login is done from an unknown machine.

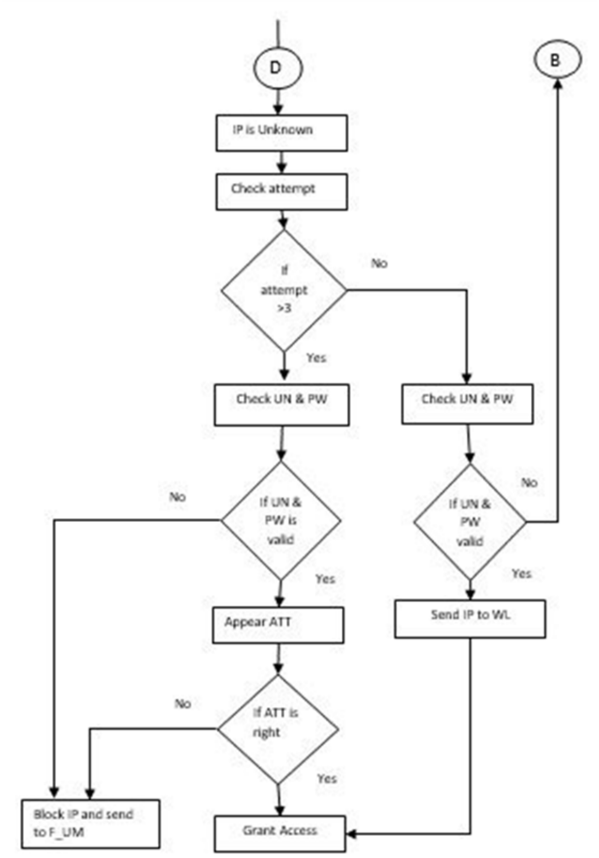

Fig. 4 Login from Unknown Machine

V. CONCLUSION

On line password attacks on password-based systems have been observed from decades. Using these guessing attacks hacker access the account of legitimate user's account. The ATT based technique is efficient in dealing against dictionary and brute force attack. The purposed work enhances the efficiency of the technique and makes the system more restrictive on guessing attacks. It helps in the commodious login process for the legitimate users as legitimate users need not to go through the ATTs from a known machine. Which increase the serviceability. Due to the use of multiple ATTs the security for the legitimate user increases.

REFERENCES

[1] Benny Pinkas, Tomas Sander, “Securing passwords against dictionary attacks,”

[2] vipul Goyal, virender Kumar, Mayanl Singh, Ajit Abraham and sugata Sanyal, “A new protocol to counter online dictionary attacks,” 2005.

[3] Peng Wang “Strengthen password based authentication protocol against online dictionary attack,”

[4] CAPTCHA definition www.en.wikipedia.org/wiki/captcha/

[5] Arya Kumar, A.K.Gupta “Password Guessing Resistant Protocol,”

[6] Ville Saalo, “Novel CAPTCHA schemes,”.

[7] Imagehttps://www.google.co.in/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF8#q=+captcha+based+on+text+images

[8] Fuji,K. and Y. Hirakawa,2008. “A study of password authentication method against observing attacks,” 6th international symposium on intelligent system and informatics.

[9] Kersler, Gary C., 2002. “Password strengths and weakness,”