IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

An Effective Login Authentication using Two Password Field and Multiple Hash Algorithm

Sumit Gautam

Student, Army Public School, Jhansi, Uttar Pradesh, India

Abstract: Authentication maintains privacy of a user. Almost all authentication techniques have some vulnerabilities, these vulnerabilities are exploited by hacker in order to gain access to someone privacy without his or her permission which is illegal as per IT rules. This paper focuses on present method which uses alphanumeric password ,It increases the strength of a alphanumeric password and make it difficult to crack a password using common password cracking techniques such a dictionary based attack, rule based attack, password guessing and many more attack used by black hat hacker.

Keywords: brutus force, rule based attack, black hat hacker, Authentication.

I. INTRODUCTION

In almost many situation social engineering hacking techniques works. Hacker exploit human brain and try to trick user to give his or her password. Even sometimes password guessing works due to weak password. Human need to use password which is reliable and easy to remember such as pet name, hobbies, date of birth or a person name[1].Hacker try many password cracking techniques and tool in order to gain unauthorized access to his or her account such as dictionary attack. Fingerprint authentication is used from past many year but the hacker has found a way to exploit it by using finger print reader[2]. Textual password suffer from dictionary attack ,shoulder surfing and many, this lead to existence of a new method know as graphical method but it has its own disadvantages as it takes much time to authenticate[3]. This paper eliminates the limitation of current alphanumeric authentication.
This research increases the strength of a password to much extent and make password difficult to crack . It works on two concept using multiple password field and taking hash algorithm as a input from a user.

A. MECHANISM OF CURRENT PASSWORD AUTHENTICATION AND HOW HACKER CRACK PASSWORD:

There are currently three types of authentication:
Token based authentication: It is authentication which we use in daily life such as ATM, credit card ,metro card.
Biometric based authentication: It uses physical or behaviour of a person .It includes finger print authentication ,face recognition
Knowledge based authentication: It is of two types text based and picture based .Text based password is used due to it versatile nature.[4]
When login page opens, user enter email and password .Form validation is done using java script at client side and using PHP(server side language) at server side. PHP is link to SQL database where password, username , email ID and other details are stored .When user enter email and password then at server side comparison takes place, whether email and password entered by the user matches with the email and password stored in SQL database. If matched it create a session and redirected to login page otherwise it gives error" Incorrect email or password" . Black hat hacker (a person who hack illegally for his or her benefit) try tools and techniques such as dictionary based attack rule based attack (Rule based attack works when hacker has some prior knowledge of password.)or may be brutus force until password is broken . Brutus force is a technique in which all combination of password is tried until password is broken.

B. CONCEPT Of USING TWO PASSWORD FIELD :

Authentication is a process of validating and preventing unauthorized access to user account. It is used to maintain privacy and to protect it from hacker who are gaining access to his or her account illegally [5]. Thought due to advancement in technology it can be cracked by various method So in order to prevent unauthorized access this method can easy tackle the problem.

There are some characteristic of using the password:
- ✓ It should be easy to remember
- ✓ It should be quickly executable
- ✓ It should easy be alterable.[6]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

If we use multiple input field then password combination increases which make harder to crack. By using one input field for password there are fixed combination it means hacker has to try fixed combination in order to crack password. May be he can create dictionary of all combination and broke it down in many small dictionary then trying every combination from different computer or virtual machine. May be he can get correct password in one computer or virtual machine.

But as we use two input field for password then it has many combination which are not fixed. Suppose user enter password "521SG" in input field one and "SG" in input field two then in order to crack a password it has to try lots of combination. It checks for one digit password for 1st input field ,and try every combination of second input field (It means in 2nd input field it has to check all digit combination starting from one digit)If password is not found then it changes first digit of 1st input to another ASCII code then try every combination of second input field. This means that it has lots of combination even if password is short in one input field.

If password for every combination of 1st input field having one digit password with every combination of many digit password for second input field is not found it then checks for 2nd digit password of 1st input field with all digit password of 2nd input field trying all ASCII code.

It means by using multiple input field we can increase the complexity of the password to much extent .Thus, even if the password is short for one input field , it is hard to crack.

C. TAKING HASH ALGORITHMS As INPUT DURING LOGIN :

In current method at server side script such as PHP, the web developer use particular hash algorithm to store password in SQL database .When user enter the password during registration time (Sign up) then it is converted into hashes which is stored in SQL database.

During login user enter the password and email in input box, the hash algorithm which is set by web designer at web pages tell the password to convert in that particular hash algorithm, it compares whether the hash password stored in SQL database matches with the hash password entered by user, if matches it create a session and redirected to logon page else it shows an error of incorrect email or password. According to this paper ,during registration time it ask for email ,username , two password and its respective hash algorithm.(It ask from a user to select hash algorithm in which he wants to store password in SQL database)After taking all input it validate form and store it in a SQL database.

D. COMPLETE METHOD MECHANISM:

The main logic is to select hash algorithm as input from user and stored the password in that particular algorithm in database .Hacker is unaware in which hash algorithm password is stored so this make hacker task difficult may be password in plain text is same as password stored in database but there hash form will not match due to wrong hash, selected by hacker. Due to this password cracking become difficult.

During registration it asks user to select two hash algorithm, two password ,valid username and email, if valid input, then it convert both password in hash form ,it then store hash password ,username, email, hash algorithm in SQL database.

During login time user have to tell username and two password and has to select particular hash algorithm if username , both password and hash algorithm matches it create a session and redirected to login page else if any hash algorithm or password is incorrect it gives a error of wrong email or password ,the advantage of this particular technique is that if user enter one password correct and another wrong then it will not tell which password is correct it still gives an error "wrong password" this increases the security and prevents hacker from cracking password.

If hacker somehow give right password for 1st input field and wrong password for second input field then it gives an error that wrong password, this make hacker difficult to crack password as during cracking both the password should be correct if may be any password is correct it still give an error and hacker has to try every combination for both password field which takes much time and he has to guess in which algorithm password is stored which makes its hacking task much difficult. As hacker has to select both hash algorithm and try all combination of password in both input field, hash algorithm may be incorrect which make hacker task much difficult as he again he has to try every combination until password is found if not then he has to try again and again. We can use password salting in order to avoid from Rainbow table offline attack if hacker somehow get the database (Password salting is a technique where random string of characters are added to the password before calculating hashes). Salting defeat pre-computed hash attack hence preventing from rainbow table attack.[7]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

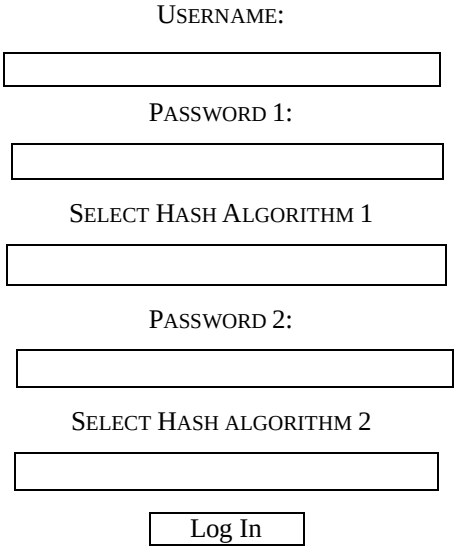
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

E. IMPLEMENTATION ALGORITHM CHART

DURING REGISTRATION TIME:
Step 1: Registration page opens
Step 2: User enter valid username, email, two password and there hash algorithm.
Step 3: User click on register button.
Step4: If valid form
Step 5: Message displayed "User registration successful"
Step 6: password is converted into hash form selected by user and all input along with hash password are stored in SQL database.
Step 7: Else Display message "user registration failed"

DURING LOGIN TIME:
Step 1: User enter username
Step 2: User enter password 1
Step 3: select hash algorithm 1
Step 4: User enter password 2
Step 5: select hash algorithm 2
Step 6:User click on login button
Step 7: If all input matches with the data stored in database
Step 8: Message displayed "Login successfully"
Step 9: Else Message displayed "Login failed"

F. EXPERIMENTAL RESULT



Let's understand with a simple example, Suppose there are total three algorithm SHA-256, md5 ,Spectral hash. It means there are total nine combination of all three Hash algorithm.

HASH ALGORITHM 1	HASH ALGORITHM 2
Md5 SHA-256 Spectral hash	Md5 Md5 Md5
Md5 SHA-256 Spectral hash	SHA-256 SHA-256 SHA-256
Md5 SHA-256 Spectral hash	Spectral hash Spectral hash Spectral hash

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

In order to crack password , hacker has to fix both hash algorithm and try all combination of both password field until match found i.e. hash algorithm 1 and hash algorithm 2 remain same and password keep on changing until all combination of both password field. If not found it will try another algorithm and try every combination for both password field until found. If not it will repeat process again and again until match found .Since it will take much time to crack .It means it is an effective method.

TABLE I

USERNAME	PASSWORD 1	HASH ALGORITHM FOR 1ST PASSWORD	PASSWORD 2	HASH ALGORITHM FOR 2ND PASSWORD
521sg	52#_k	Md5	qw	Md5
521sg	52#_k	Md5	qe	Md5
521sg	52#_k	Md5	qr	Md5
521sg	52#_k	Md5	q$	Md5
521sg	52#_k	Md5	q^	Md5
521sg	52#_k	Md5	q1	Md5
521sg	52#_k	Md5	q2	Md5
521sg	52#_k	Md5	q3	Md5
521sg	52#_k	Md5	q4	Md5

Hash algorithm has to be changed and again hacker tries all combinations for both the password

TABLE IIIII

USERNAME	PASSWORD 1	HASH ALGORITHM FOR 1ST PASSWORD	PASSWORD 2	HASH ALGORITHM FOR 2ND PASSWORD
521sg	52#_k	Md5	qw	Sha-256
521sg	52#_k	Md5	qe	Sha-256
521sg	52#_k	Md5	qr	Sha-256
521sg	52#_k	Md5	q$	Sha-256
521sg	52#_k	Md5	q^	Sha-256
521sg	52#_k	Md5	q1	Sha-256
521sg	52#_k	Md5	q2	Sha-256
521sg	52#_k	Md5	q3	Sha-256
521sg	52#_k	Md5	q4	Sha-256

Compare last column of both the table I and table II ,hash algorithm changes during next time of hacking when all combination are tried for both password field.
Same as above, there will be total 9 table with different algorithm. In each table it will try all combination of both password field until match found.

In order to crack password, hacker has to try all combination of both input field for particular algorithm if not found it will try another combination of algorithm (eg-MD5,SHA-3)and then try all combination for both password field until match found .If not found then hacker has to try again every combination for both password field and keep on changing algorithm until password found. But this take much time. Since there are many hash algorithm ,It means there are huge choice for selection of password algorithm by hacker, which make hacker task much difficult. Since user will login when both hash algorithm will same as selected by user during registration. Both Password enter by user first converted into hash form by using hash algorithm selected by user during log in then it compares both hash password with the password stored in SQL database .If match found user is redirected to login page. Otherwise it has to try many times with different algorithm and all combination for both password field.

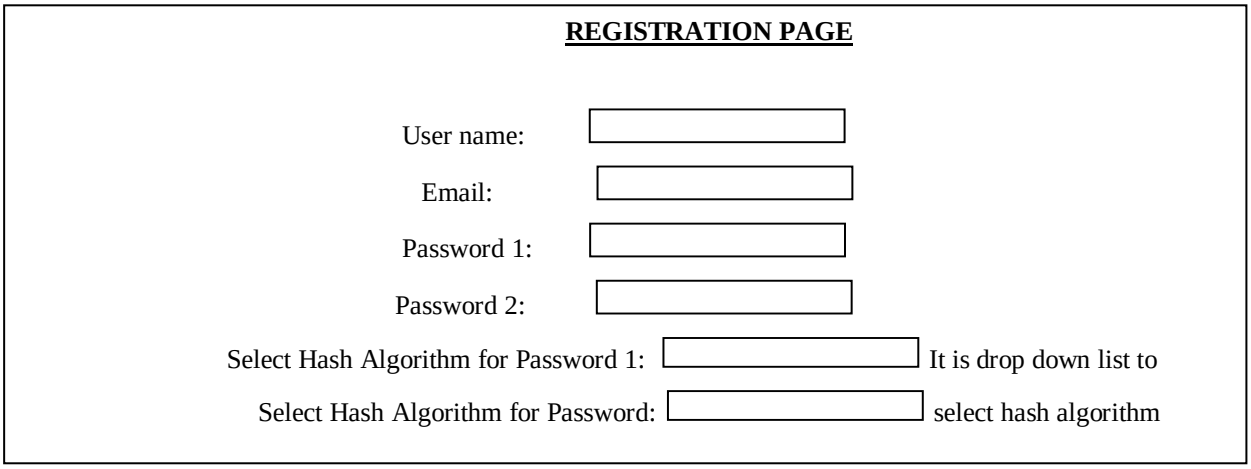
Let's take another example, Suppose 10 algorithm is there to select as a input and there are two algorithm selection field ,it means hacker has to try 10*10 =100 combination(selecting hash algorithm) and trying password cracking every time for each combination hence it is very difficult to crack a password. Here it takes 100 times and some extra time due to two input field. Hence password cracking take a huge time preventing hacker from hacking . Here ,there is no need to change password regularly. No need to use long password (Here it is recommended to use at least 8 total digit for two password field and there is no restriction in any one of the field for minimum digit, user can enter 2 digit or

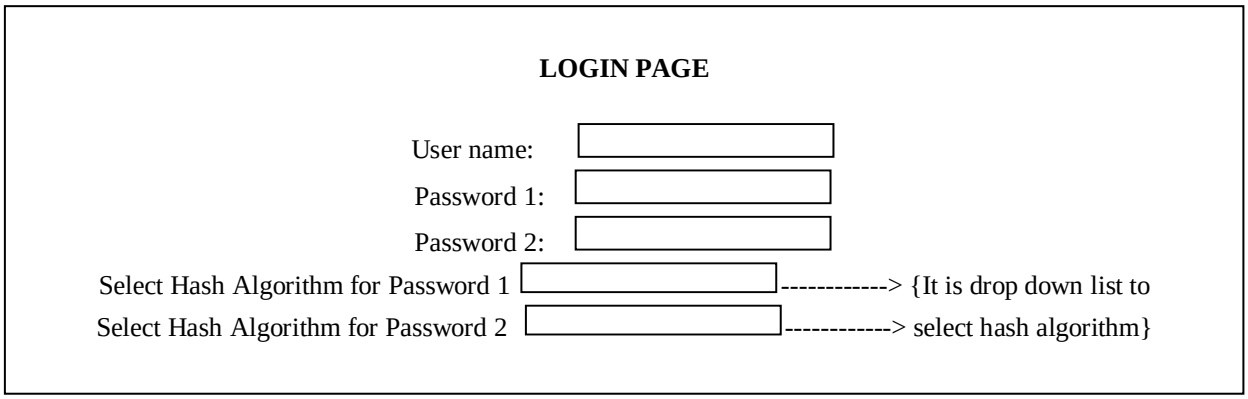
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

even more) . As the digit increases it complexity increases which makes harder to crack. Password length can be same or short as current method .For remembering password think it is a single password which is broken down into two string.”521sg@62”, now this password can be broken into two string (word) for two input password field as per this paper. Suppose user enter password one ”521” And password two ”sg@62” .Hence remembering password is not so difficult and there is no need to use long password. Thus we can say that here it increases the complexity of password to much extent by using two input field and multiple hash algorithms taken as input from user during login time.





According to present method long password increases complexity and makes harder to crack. Short password are easily cracked by password cracking techniques such as brutus force.Brutus force attack is used to recover forgotten passoword[8]but today it has been misused by black hat hacker. Security expert Bruce Schneier recommended user to use long password as it is hard to crack and he suggested to write it in a piece a paper and keep it safe as other valuable thing[9]. Since nobody wants to remember long password this research paper eliminated the need of long password and makes the current method more efficient.

G. ADVANTAGES

- ✓ It Increases the complexity of password to much extent.
- ✓ Hacker should try many combination as he is unaware of hash algorithm.
- ✓ If anyone password is correct it will still give an error until both the password is same if may be both password is same and any hash algorithm is incorrect it will give error “incorrect email or password” as hash password not matches with the hash password stored in SQL database.
- ✓ It takes much time to crack a password than a current method as hacker has to try every combination for both password field and try both hash algorithm from drop down list.
- ✓ It makes current alphanumeric login authentication much stronger, many research are made in order to remove weakness of current login authentication by different method such as graphical method or any other method but this paper not tell another method it makes current method even stronger and makes the current login authentication more secure.
- ✓ Password length can be shorter but at least total 8 digit for both password field.
- ✓ No need to change password regularly, one password can be remain for years.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

II. CONCLUSION

This paper focuses on current alphanumeric password authentication, It increases the complexity to greater extent, A black hat hacker should try huge combination as he is unaware of the hash algorithm, and much combination for both input field. This techniques is best than the current approaches, It is best as it makes the hacker task difficult to a greater extent. It maintains privacy of a user and provide security on the internet. This approaches can be use anywhere whether it is a website login page or windows password, It applies in all situation where text based password is needed. Network security will also increases to a greater extend if we apply this approach.

ACKNOWLEDGEMENT

I would like to thank **Mrs Ravina Sultana**, PGT of computer science department for inspiring ,motivating and helping me throughout my work. I would also like to thank my parents for their support and guidance in completing my research paper.

REFERENCES

[1] Delphin Raj K M, Nancy Victor "A Novel Graphical Password Authentication Mechanism, Raj et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(9), September - 2014, pp. 203-207© 2014
[2]. Markus Jakobsson, Sebastien Taveau , The Case for Replacing Passwords with Biometrics.
[3] S uraj R. Deulgaonkar ,V.T.Gaikwad, H.N.Datir, Secure Authentication Using Session Based Password with Virtual Keyboard, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 1, January 2016
[4] Er.Aman Kumar1, Er.Naveen Bilandi2 , A GRAPHICAL PASSWORD BASEDAUTHENTICATION BASED SYSTEM FOR MOBILE DEVICES , IJCSMC, Vol. 3, Issue. 4, April 2014, pg.744 – 754
[5] Nayana S1, Dr. Niranjanamurthy M2, Dr. Dharmendra Chahar3 ,Study on Three Dimensional (3D) Password Authentication system , International Journal of Advanced Research in Computer and Communication Engineering ICRITCSA M S Ramaiah Institute of Technology, Bangalore Vol. 5, Special Issue 2, October 2016
[6] Shraddha S. Banne1, Prof. Kishor N. Shedge2 , CARP: CAPTCHA as A Graphical Password Based Authentication Scheme , International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016
[7] https://en.wikipedia.org/wiki/Salt_(cryptography)
[8] https://en.m.wikipedia.org/wiki/Password cracking
[9] https://en.m.wikipedia.org/wiki/Password_strength

BIOGRAPHY

I have completed my 12th in May 2017 from Army Public School Jhansi, Uttar Pradesh, India. I Secured 96 marks out of 100 in computer science CBSE board .I have a keen in interest in White hat hacking and in making new things related to any topic in computer science engineering.