ISSN: 2321-7782 (Online)

Volume 3, Issue 11, November 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods

Savita Kamalakarrao Kulkarni
Dept. Of Computer Science & Application
Vindyachal Shikshan Sanstha's VSS College
Jalna, 431203, India.

Abstract: In daily life we always use passwords for various computer applications like computer login, Banking, ATM machines-mail etc. But these passwords are not secure either online or offline .internet provides greater opportunities for attacker/hackers for cracking the passwords. In this paper different methods of password attacks are mentioned in first (I) part. In second (II) part various counter measures are mentioned. In third (III) part different authentication methods for greater security to related attacks are mentioned. In fourth (IV) part comparative analysis of different password attacks & their relative countermeasures for protection from attacks &different authentication methods are described.

Keywords: Password, Password attacks, countermeasures, Authentication methods, Conclusion.

Objectives: The main objectives of this research are

- ***To introduce what is password, password attacks & different techniques or methods of password attacks.***
- ***To introduce the countermeasures for preventing the password from password attacks.***
- ***To discuss with different authentication methods for preventing password attacks.***
- ***Analyze the authentication methods & countermeasures for different attacks.***

Research Methodology: Basically secondary data is used because maximum data is collected on internet from different sites, web blogs, research papers & so on.

I. Introduction

Figure 1

In our daily life we are using passwords in many ways like passwords, pass phrases, pass codes, PIN etc. everywhere such as for banking ,ATM machines ,email logins ,computer login, & so many purposes. We always hear the password security warnings like don't share your password with others even with your friends, never use vendor default password, never use easy to guess password etc But are we sure that these passwords are safe, surely authenticated and can't be hacked by any other unauthorized persons. The answer is no because in day to day life the growth of the Internet has created unlimited opportunity for the intruders/hackers to steal secrets, as the computer security or network security become stronger , the hackers becomes sharper to find out the techniques for stealing the passwords.

Password: A password is a word or string of characters used to access to a resource for user authentication to prove his/her identity or access approval. Ex. Pass code is a numeric type of password kept secret from those who are not allowed to access.

The password was used by ancient from early days. In modern time the user name & passwords are used by peoples for login access to protected computer system, operating system, online bank account, mobile phones, cable TV decoders, ATMs (Automated Teller Machines)etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mails accessing applications, databases, networks, web sites, and even reading the morning newspaper online. It is not necessary that password should be only words .As stated above password may be

Pass code/Passkey: pass code in which purely numeric keys or values are used such as PIN (Personal Identification Number) used in ATM machines.

Password: password in which word is used.

Pass phrase: Pass phrase in which multiple words called as phrases are used,

Passwords are shorter enough to be memorable& typed. Many organizations and government organizations provides rules for password generation called as password policies.

Password Attacks:

password attacks are the classic way to find out the password & login to access to a resource or computer system for gaining power and control of a computer system or resource or network. The growth of the Internet has created unlimited opportunity for the intruders or password hackers. Their goals might be different but they all have the goal of gaining power of computer system to steal secrets, tinker with Web sites, abscond with credit card information, or just generally make mischief. For preventing our computer from password attack we should know what are the techniques used by hackers that can access the password for stealing important information like client databases, credit card information & many more.

Following are some common methods used to break into a password protected systems.

1. ***Brute Force Attack***:

The most reliable and time consuming attacking method is the brute force attack for attackers or hackers. The attacker can tries with every possible combinations of characters, numbers ,special characters such as starting from abcd11…..ABCD999……zzzz123…….ZZZZ10& so on. A hacker can use a computer program or script for guessing the most possible combinations of characters for guessing password. To guess password a hacker can starts from easiest. Brute force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. This means short passwords can usually be discovered quite quickly, but longer passwords may take decades.

Reverse Brute Force Attack: In a reverse brute-force attack, a single (usually common) password is tested against multiple usernames or encrypted files. The process may be repeated for a select few passwords. In such a strategy, the attacker is generally not targeting a specific user. Reverse brute-force attacks can be mitigated by establishing a password policy that disallows common passwords.

2. ***Dictionary Attack:***

The attackers assume that the user can use a complete word as a password so the attacker can try a complete dictionary word in a special software program or script to login by cracking the password. instead of guessing each & every combination of characters as like in brute force attack. Here hacker/ attacker will use only the most possible words from dictionary hence the name dictionary. The dictionary attack can be succeed because of the human being tendency to use the words which are shorter enough i.e.7 characters in length & easy to remember (Ex." password") from dictionary hence the attacker can easily guess such words from many software programs or script .Even the user cleverly uses the combinations of words such as " superadminstrator","daynight" etc. then also will not prevent his/her password from being cracked not more than few second extra later from dictionary attacks. Dictionary attacks work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary. Dictionary attack tools require a dictionary input list.

3. *Key Logger Attack/malware Attack :*

A hacker or attacker uses a program to track all of the user's keystroke so that at the end of day everything that the user has typed including his login IDs and password have been recorded. A key logger attack is different from brute force or dictionary attack. A key logger or screen scraper program which are the malware virus or full blown virus programs that can be installed by malware which records everything user typed on his/her screen. These programs can be installed directly by the hacker or they make the trick to install this program by user through email by clicking or downloading the link hence these programs must be first make on the user's device. Some malaria will look for the existence of a web browser client password file and copy this which, unless properly encrypted, will contain easily accessible saved passwords from the user's browsing history. Even though stronger passwords don't provide much greater security against the key logger attacks hence now a days many business or organizations wants to must have Multifactor Authentication(MFA).With multi factor authentication or 2 factor authentication & advance authentication a user is required to provide not only password but also another security factor like a unique code generated from their secure mobile app on their smart phone or token device, so even if a hacker is able to attain a system factor he won't be able to access the second security password because of a network protected by MFA since this network is nearly impenetrable to an outside attack.

4. *Rainbow table attack:*

A rainbow table is a list of pre-computed hashes i.e. of an encrypted password used by most of the systems used today. Hashes mean the numerical value of an encrypted password, and that is the hashes of all possible password combinations for any given hashing algorithm mind. The time it takes to crack a password using a rainbow table is reduced to the time it takes to look it up in the list. However, the table itself will be huge and require some serious computing horse power to run, and it is useless if the hash it is trying to find has been 'salted' by adding random characters to the password before applying the hashing algorithm. It is said that salted rainbow tables are exist, but these would be so large as to be difficult to use in practice.

5. *Phasing Attack:*

It is an easy way to hack the users. If the users are going to give password in easy way then there is no necessary to try for cracking the password. This is true because of this phishing attack. In this attack the attacker send a fake email clams to be from legitimate organization. This is usually combined with a threat or request for information such as the account will be closed, balance is due, information is missing from your account etc. The email will ask the supplier the confidential information such as bank account details, account no,ATM PIN, VPN no, password etc. These details are then used by the owners of the website for making fraud .hence user provide his/her own confidential information to the hacker very easily.

6. *Social engineering:*

The practice of tricking the user into giving or giving access to sensitive information, thereby bypassing the most or all protection. Social engineering takes the whole 'ask the user' concept outside of the inbox that phishing tends to stick with and into the real world .EX. Suppose after hacking attempts failed a hacker tried as social engineer by walking into the building or offices and claiming that he/she had to do some urgent work in the server room.

7. *Offline cracking:*

Passwords are safe in blocking automated guessing applications because after entering wrong password it will automatically block the system .but in actual password cracking can takes place offline outside the system using a set of hashes in a password file that has been 'obtained' from a compromised system. In this method hacker can take a captured password hash (challenge –response packets) & converting it to its plaintext original. To crack a password, an attacker needs tools such as extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information.

8. *Shoulder surfing/spearing:*

The most confident of hackers will take the guise of a parcel courier, aircon service technician or anything else that gets them access to an office building. Once they are in ,they will notice the staff members how they are entering the passwords, the attacker trick out the user to install that file into his name of spying in which attacker spies the user's system then the key logger makes the log file of his login movements & then sends it to the attacker's file. The attacker observes the user how he/she enter the password ,in how much time ,what keys of the keyboard the user has pressed & hence attacker get the password & then he can access the target system. The attacker can use the binocular to see the video recording of the user that how he/she enter the password all these recording can be seen from distant place with the help of mobile camera or any other such devices, use the hidden close circuit TV camera to observe the camera, analyzes the recorded video of user's password entering from a remote location. The attacker can listen the password entered by the user in it user's password that how many keys the user has pressed and operations are recorded once or twice then the attacker uses all the possibilities related to the password length to break it.

9. *SQL Injection Attacks:*

The poorly designed websites are the victim of this type of attacks. In this attack the attacker can inject the SQL commands & gain access to obtain the data from database. It is a code injection technique used to attack websites & login with administrator privilege.

10. *Password Guessing:*

Depending upon our brain's emotional attachments we sometime gives password to the things that we likes, hence the chances are that there may be random passwords based upon our interest ,hobbies,pets, family & so on. Infact password are based upon the things that we like to chat on social networks and even we include in our profile, so the attacker can look very carefully at these information for guessing the password instead of using dictionary attacks or brute force attacks. Hence the password cracker's best friend is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user generated 'random' password is unlikely to be anything of the sort. Automated password guessing programs and crackers use several different approaches. Hybrid password guessing attacks assume that network administrators push users to make their passwords at least slightly different from a word that appears in a dictionary. Hybrid guessing rules vary from tool to tool, but most mix uppercase and lowercase characters, add numbers at the end of the password, spell the password backward or slightly misspell it, and include characters such as @!# in the mix.

11. *Password Resetting:*

Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password resetters. In most cases, the attacker boots from a floppy disk or CD-ROM to get around the typical Windows protections. Most password resetters contain a bootable version of Linux that can mount NTFS volumes and can help to locate and reset the Administrator's password.

II. COUNTERMEASURES

Figure 2

Taking some general countermeasures can prevent hacking of important passwords

Password policies:

A strong password-creation policy that includes the following criteria:

- » make it at least 7 characters long, combination between small and capital letters, at least one number and special character like !@#$%^*()_+
- » Do not simply use a dictionary word or a logical sequence of characters like aaa555ccc, 1234567890 etc.

A combination of the following strong, yet easy to remember passwords techniques may be used are:

- » choose a dictionary word like success, then reverse it sseccus
- » add numbers in front or at the end of it 146sseccus or sseccus953
- » consider adding at least one special character like !@#$%^&*()_+ anywhere
- » the use of at least one capital letter would increase the crack able possibilities even more
- » replace certain characters with numbers that you associate with them, security would be s3cur1ty where e stands for 3 and i stands for 1
- » separate each letter with a number, security would be s1c3u2r4i6t5y
- » Use upper- and lowercase letters, special characters, and numbers. Never use only numbers. Such passwords can be cracked quickly.
- » Misspell words or create acronyms from a quote or a sentence.
- » Use punctuation characters to separate words or acronyms.
- » Change passwords every 6 to 12 months or immediately if they're suspected of being compromised.
- » Use different passwords for each system.
- » Use variable-length passwords.
- » Don't rely completely on similar-looking characters, such as 3 instead of E, 5 instead of S, or ! instead of 1.
- » Don't reuse the same password within at least four to five password changes.
- » Use password-protected screen savers.
- » Don't share passwords.
- » Avoid storing user passwords in an unsecured central location,
- » Keep the password in a locked file cabinet or office safe
- » Full (whole) disk encryption which can prevent an intruder from ever accessing the OS and passwords stored on the system.
  - ▪ A secure password management tool such as LastPass ,Password Safe an open source software originally developed by Counterpane
- » Enable security auditing to help monitor and track password attacks.

- Test your applications to make sure they aren't storing passwords indefinitely in memory or writing them to disk. A good tool for this is WinHex
- Keep your systems patched.
- Know your user IDs.
- Account Lockout: Enable account lockout to prevent password-cracking attempts. Account lockout is the ability to lock user accounts for a certain time after a certain number of failed login attempts has occurred.

III. Prevent Hacking with Password-Cracking Attacks Countermeasures

Following are the countermeasures that protects from the entire password cracking attacks.

Countermeasure for Brute-force Attacks: Brute-force Attacks may be prevented by creating a very long password and using many numbers and odd characters. The longer the password the longer it takes for the hacker to crack the password. Creating a phrase for a password is the best option for staying secure.

Countermeasure for Dictionary Attacks: Theseare very simple to prevent. Don't use a password that is in the dictionary. Some people may think that if they use a word from the dictionary but replace most of the letters with a number, then they are safe. They are not. There are 1337 speak dictionary's out there too. Basically what 1337 speak is, is changing a word like "animal" to 4n1m41. For a secure password, using a phrase such as "doyoulikecheese?88".

Countermeasure for key logger attacks: The key logger attack can be avoided by using the virtual keyboard in which the position of characters will change randomly. OTP (one-time password) can be used to avoid key logger attacks. For Ex. when Gmail account is configured with two-step authentication, OTP sent to the mobile is required to login. OTP can be obtained in special devices such as SafeNet eToken NG-OTP, RSA SecurID tokens. Antilogger such asZemana, sandboxie, key scrambler can be used to avoid key logger attacks.

Countermeasure for Rainbow Attack: Avoid rainbow table cracking by simply making password extremely long. Creating tables for passwords that are long takes a very long time and a lot of resources.

Countermeasure for Phishing attacks: These are very simple to avoid. When users are asked to put his/her personal information into a website, look up into the URL bar. Ex. If user is supposed to be on Gmail.com and in the URL bar it says something completely different like **gmail.randomsite.com**, or **gamilmail.com**, then this is a fake. When someone is on the real Gmail website, the URL should begin with**www.google.com** anything else is a fake.

Countermeasure for Social Engineering Attack: To protect from social engineering you must learn to question the possible attacker. If you get a phone call from someone, and you think that there may be a chance that the person isn't who he says he is, then ask him some questions that he should be able to answer to establish his legitimacy. Some professional social engineers study the company before attacking, so they might know all the answers. That's why, if you still have some doubts, you should ask the head of whatever department the attacker is from to find out if he is legit. Better safe than sorry.

Countermeasure for Shoulder Surfing Attack: When typing password make sure there is no one behind attempting to peak. If there is, be alert to drop him/her. Also, make sure that not to keep any sticky notes lying around that have password or password hints on them.

Countermeasure for SQL Injection attacks: Patches for Operating Systems, softwares, and antivirus are to be regularly updated. A proper validation of input data can mitigate SQL Injection attack. Access Control permission on the database must be strictly defined.

Countermeasure for Guessing Attack: To prevent this attack from happening, never use a password like birth date, mother’s maiden name, pets name, spouse’s name, or anything that someone may be able to guess.

Other password-protection countermeasures include

Automated password reset: This functionality lets users manage most of their password problems without getting others involved. Otherwise, this support issue becomes expensive, especially for larger organizations.

Password-protect the system BIOS: This is especially important on servers and laptops that are susceptible to physical security threats and vulnerabilities.

Stronger authentication methods: Examples of these are challenge/response, smart cards, tokens, biometrics, or digital certificates etc., as discussed below.

IV. Authentication Methods-The Possible Solutions

When enforcing authentication methods on both network and security policy levels, the majority of users proved to be unreliable in storing and creating strong passwords. The service desk is often too busy to handle "forgotten passwords" requests, and unless the company doesn't undertake a passwords awareness initiative, the problem will continue to grow.

4.1 Pass phrases:

Pass phrases are usually something that we always remember either a quote, favorite sentence or a combination of both numbers and special characters. The majority of encryption software require to use a pass phrase for private key instead of a password.

Advantages: Pass phrases were thought with the idea to be easier to remember, but virtually impossible to crack. Although virtually impossible to crack due to their length.

Disadvantages: Both the passwords and passphrases can be logged through the use of a key logger, or sniffed if transmitted over plain text communication channel.

4.2. Conventional Password Method:

The traditional or conventional password authentication is old & most widely used method. In this scheme the user enters login his username and password. The system first authenticates the user from the user database and on the basis of authentication of the user and then grants the access to the system is granted.

Advantages: It is simple, easy to remember, easy to use, no additional hardware or software or specialized personnel required.

Disadvantage: It is vulnerable various attacks like shoulder surfing attack, key loggers, and spoofed login and phishing attacks.

4.3 Public Key Infrastructure (PKI) / Public Key Cryptography:

The password can be encrypted to avoid eavesdropping attacks and other attacks. Public key cryptography is also known asymmetric cryptography. Public Key Infrastructure(PKI) functions gives entities, namely employees or servers the ability to communicate, authenticate, sign and verify identities by creating digital certificates, It generates two mathematically related keys, public key and private key.. The public key is available to anyone wanting to exchange data with the entity and the private key is the only way for the entity to decrypt, or identify itself properly. The message may be encrypted using public key or private key and decrypted using its corresponding private key or public key.

Advantages: It provides confidentiality of the message. It is used for creating digital signatures. It is very useful when communicating over insecure networks like the Internet and both on the internal servers.

4.4. Keystroke Dynamics:

Keystroke dynamics is a biometric solution in which the users rhythmic typing on the keyboard and the timing between the key pressed is used as an authentication technique. Along with the conventional password following information is recorded.

a) The time taken between a key press and a key release

b) The time taken between two consecutive keys pressed.

Advantage: It requires no extra hardware only programming skill is enough. It prevents from shoulder surfing, key loggers, phishing, etc. Even with the password the attacker cannot access the system.

Disadvantages: High rejections occur due to different typing speed of users. It is difficult to identify even the legitimate user.

4.5. Click Pattern:

Click Pattern provides strong password rather than text-based password. The click area contains different color or combination of different symbols. The user click rhythm is also maintained along with click patterns.

Advantages: It does not require any extra hardware and prevents from shoulder surfing attack, key loggers, phishing, etc. It is difficult to compromise even the password is known.

Disadvantages: It may have more rejections due to different mental levels of users.

4.6. Graphical Passwords:

Graphical password is an alternative for text-based passwords. Graphical objects are displayed and the user needs to select it. Selected objects are then drawn by user using mouse, touchpad or touch screen. System runs preprocessing on the objects and converts it into hierarchical form. Finally, hierarchical matching is done foruser authentication.

Advantages: It prevents from shoulder surfing attack.

Disadvantages: The system authenticates the user only if proper sketch is drawn by the user on the touch sensitive screens. The processing time depends on how good the user draws the sketches. Normally it takes longer time for process compared to other schemes. Also it depends upon the ability of the user to draw sketches and its processing time is much longer than other schemes.

4.7. One-Time Password:

One-time password (OTP) is a password valid for a short period of time and can be used only once. An OTP may also be generated from a password list. Banking and financial companies always use this method.

Advantages: OTP is used for avoiding identity theft. It protects the online transactions from replay attacks, key loggers, shoulder surfing attacks, etc. An OTP captured by an attacker may be of no use to him.

Disadvantage: It requires some additional technology such as SMS to mobile, or call to mobile for OTP, etc. An OTP may be of random challenge-response type.

4.8. Biometrics:

Biometric is an image-based authentication system in which finger prints system , face reading system , iris/ retinal scanner system, speech recognition system, signature verifications system, hand geometry system, handwriting system, are used to verify against the original specimen . The image is preprocessed first and then the classification of images is done. Biometrics is the next generation of authentication methods.

Advantages: It is real and unique signature and cannot be stolen, cannot be forgotten; neither can they be given to another person. Biometrics will change the way we authenticate ourselves, hopefully with 99% accuracy.

Disadvantages: It is costly and difficult to implement. It is not a completely matured method and it can be easily compromised and is time consuming also sometimes the number of false results.

4.9. Authentication Panel:

In these password schemes, instead of pressing exact button for password, the user is prompted to select the location of the password word from the given panel.

Advantages: Vulnerabilities can be rectified by updating weak components regularly. It prevents from brute force, dictionary and video recording attacks. It does not require extra hardware and it is fast

4.10. Zero-Knowledge Proofs:

In this method, the user can prove his identity to the verifier without revealing the secret that is known only to him.

Disadvantage: If the secret is revealed to the verifier, he may share it with someone else.

4.11. Virtual Password: This Novel password scheme offers secure user's password in on-line environments.

Advantages: It can provide protection against different online attacks as phishing and password file compromise attacks.

4.12. Moving Balls Based Security Scheme:

In this method scheme the user click the mouse, then a user have number of balls moving in different columns and it all seen on screen, now the user just has to remember the number of columns and the respective balls.

Advantages: it protects from dictionary attacks, shouldering

Disadvantages: user must have to remember the number of columns and the respective balls.

4.13. Digital Signatures:

Digital Signature is a mathematical method that proves the integrity of the document. It is used by companies for distributing their software. The distributor or sender computes the hash for the document and shares it on Web page with the public. The user downloading the software computes the hash and matches against the hash that is available on the Web. If they are same, accept it otherwise reject it. The sender may encrypt the message using public key and the message is decrypted using private key by the recipient. The sender knows that the message can be decrypted only by the particular recipient as he is the only persons having knowledge about the private key. Broadly speaking, a digital signature is a document which is hashed first and then it is encrypted with the private key of the sender and is appended to the original document. The recipients on the other end, decrypts the document using public key so he knows for sure it is send by the particular sender. Then it is hashed by the recipient and he verifies it with the actual hash. Now the verifier or the recipient is able to identify the sender as well as get assurance that the message has not been modified.

Advantages: It provides integrity, authentication and non-repudiation aspects of security. It assures the recipient that the document has not been altered in transit.

V. Comparative Analysis

The table I given below explains about various attacks, countermeasures, authentication mechanism, advantages and disadvantages, hardware required etc.

Table 1: Comparative Analysis of Password Attacks, Their Counter Measures,& Authentication Methods

Attack	Countermeasure	Authentication Method	Resistance to attacks	Advantages	Disadvantages	Additional Hardware Required	Mental Attitude Effect	Protection Level	Processing Time
Brute-force Attacks	very long password and using many numbers and odd characters. Creating a phrase for a password	Passphrases	1.Brute force 2.Dictionay	1. Easier to remember 2.virtually impossible to crack due to their length.	1. Logged through the use of a key logger, 2.sniffed if transmitted over plain text communication channel.	No	Yes	Medium	Fast
Dictionary Attacks	Don't use a password that is in the dictionary. Using a phrase such as "doyoulikecheese?88".	Conventional Password Method	1.Brute force 2.Dictionary	Simple, easy to remember, easy to use.	It is vulnerable various attacks like shoulder surfing, key loggers, spoofed login, phishing attacks.	No	Yes	Low	Fast
Key logger attacks	Using the virtual keyboard. OTP (one-time password), must have Multifactor Authentication(MFA).	PKI / Public Key Cryptography	eavesdropping attacks	It provides confidentiality of the message. creating digital signatures. useful for communicating over insecure networks like the Internet					
Rainbow Attack	Avoid rainbow table cracking by simply making password extremely long.	Keystroke Dynamics	Shoulder surfing, keyloggers, phishing, etc.	Even with the password the attacker cannot access the system.	High rejections occur due to different typing speed of users. It is difficult to identify even the legitimate user.	No	Yes	Medium	Medium
Phishing attacks	To put his/her personal information into a website, look up into the URL bar. anything else is a fake.	Click Pattern	Shoulder surfing, phishing, key loggers	Difficult to compromise even the password is known.	More rejections due to different mental levels of users.	No	Yes	Medium	Medium

Social Engineering Attack	To protect from social engineering question the attacker find out if he is legit. Better safe than sorry.	Graphical Passwords	Shoulder surfing	Alternative for text-based passwords. Graphical objects are displayed and the user needs to select it	Proper sketch should be drawn by the user on the touch sensitive screens. Processing time is longer. It depends on the ability of the user to draw sketches	Yes	Yes	Medium	Slow
Shoulder Surfing Attack	When typing password make sure there is no one behind attempting to peak. Make sure that not to keep any sticky notes lying around that have password or password hints on them.	One-Time Password	Replay attacks, keyloggers, shoulder surfing attacks, etc.	Avoididentity theft. It protects the online transactions An OTP captured by an attacker may be of no use to him.	It requires some additional technology such as SMS. An OTP may be of random challenge-response type.	Yes	Yes	High	Medium
Guessing Attack	never use a password anything that someone may be able to guess.	Biometrics	Shoulder surfing, pishing, key loggers etc	Rreal and unique signature and cannot be stolen , cannot be forgotten, neither can they be given to another person..	Costly and difficult to implement. Not a completely matured method and it can be easily compromised and is time consuming sometimes the number of false results,	Yes	No	High	Slow
SQL Injection Attacks	:Patches for Operating Systems, softwares, and antivirus are to be regularly updated. A proper validation of input data Access Control permission on the database must be strictly defined.	Authentication Panel	Brute force, dictionary and video recording attacks.	Vulnerabilities can be rectifiedby updating weak components regularly,it is fast.	Proper location should be selected by the user from the given panel. It depends on the accuracy of the user to select the location.	No	yes	High	Medium
Offline cracking	Safe in blocking automated guessing applications because after entering wrong password it will automatically block the system.	Zero-Knowledge Proofs	Brute force, dictionary and video recording attacks.	Secret that is known only to user.	If the secret is revealed to the verifier, he may share it with someone else	No	Yes	Low	Medium

Password Resetting	Full disk encryption which can prevent from accessing the OS and passwords stored on the system.	Virtual Password	phishing,key loggers, password file compromise attacks.	This Novel password scheme offers secure user's password in on-line environments	Protection level is medium	Yes	No	Medium	Fast
Reverse brute-force attacks	Establishing a password policy that disallows common passwords.	Moving Balls Based Security Scheme	dictionary attacks, shouldering	It is simple & easy to remember.	user must have to remember the number of columns and the respective balls.	No	Yes	High	Medium
		Digital Signatures	Phishing attacks	. It provides integrity, authentication and non-repudiation aspects of security. It assures the recipient that the document has not been altered in transit.	Compatibility, cost	No	No	High	Medium

VI. Conclusion

Conclusion: Before adopting any password method we should know different password attacking methods and their countermeasures for preventing the password attacks, here different online as well as offline password attack methods, their advantages, disadvantages ,their countermeasures, which authentication method resists to which attacks, hardware requirement ,processing time, protection levelare discussed which will be use full for designing the authentication methods .Also by using the combination of more than one authentication method provides the greater security.

References

1. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A Survey of Password Attacks and Comparative Analysis
2. on Methods for Secure Authentication", World Applied Sciences Journal, vol. 19, pp. 439-444, Jan. 2012.
3. Jesudoss A. et.al / Indian Journal of Computer Science and Engineering (IJCSE)A survey on authentication attacks and countermeasures in a distributed environment ISSN : 0976-5166 Vol. 5 No.2 Apr-May 2014 75
4. How to Start Research in Computer Networks: Seven Steps on the Road to SuccessBy Prof. Ahmed Helmy Department of Electrical EngineeringUniversity of Southern California www.cleophon.com - Computer, internet & technology blog. Article Source: http://EzineArticles.com/?expert=Robin_George_InchananiyilPassword Attack Methods And Prevention
5. http://en.wikipedia.org/wiki/Dictionary_attack Wikipedia:
6. web Blogs How a cheap graphics card could crack your password in under a second
7. http://www.thc.org
8. (http://www.hammerofgod.com/download.htm)
9. http://www.sqlsecurity.com/DesktopDefault.aspx?tabid=26
10. Jan 30, 2006Roger Grimes | Windows IT Pro
11. (http://www.antsight.com/zsl/rainbowcrack
12. ScoopLM (http://www.securityfriday.com/tools/ScoopLM.html) and KerbCrack
13. (http://ntsecurity.nu/toolbox/kerbcrack), a sniffer and cracker for cracking Kerberos
14. Prevent Hacking with Password-Cracking Countermeasures By Kevin Beaver from Hacking For Dummies, 4th Edition
15. www.google.com
16. http://www.amfastech.com/2013/03/best-counter-measures-for-password.html
17. Best Counter Measures for the Password Attacks || How to Prevent from being Hacked? http://windowsitpro.com/security/prevent-password-cracking

18. http:// www.windowsitpro.com, InstantDoc ID 49232.

19. Table 1 in Chapter 3 of the "Microsoft Windows 2000 Security Hardening Guide" (http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/03osinstl.mspx).

20. http://www.dummies.com/how-to/content/how-to-crack-ios-passwords.html

21. References:By Kevin Beaver from Hacking For Dummies, 4th Edition

22. http://security.stackexchange.com/postedited Sep 19 '14 at 7:09

23. http://www.wikepedia.com

24. http://www.dummie.com/how-to-crack/

AUTHOR(S) PROFILE

Author Name: Mrs. Savita Kamalakarrao Kulkarni, received the M.Sc. degree in Computer Science from Department of Computer Science & Information Technology ,Dr.Babasaheb Ambedkar Marathwada University, Aurangabad in 2004. During 2004 to 2010 she worked as a Assistant Professors at Shri Madhavrao Patil Mahavidyalaya ,Murum(SMP College),District Osmanabad. Now she is working as a Assistant Professor at VSS College (Vindyachal Shikshan Sanstha's), District Jalna since Jan 2011 up to date. Her interest of area is computer networking, cloud computing.